



Panduan Pengguna ONTAP

FSx untuk ONTAP



FSx untuk ONTAP: Panduan Pengguna ONTAP

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Apa itu Amazon FSx untuk NetApp ONTAP?	1
Fitur FSx untuk ONTAP	2
Keamanan dan perlindungan data	3
Alat-alat pemantauan	3
Harga FSx untuk ONTAP	4
FSx untuk ONTAP di AWS re:Post	4
Apakah Anda FSx pengguna Amazon pertama kali?	4
Cara kerjanya	5
Sistem berkas	5
Penyimpanan mesin virtual	5
volume	6
Tingkatan penyimpanan	6
Tingkatan data	7
Efisiensi penyimpanan	7
Mengakses data Anda	7
Mengelola FSx sumber daya ONTAP	7
Mulai menggunakan	9
Menyiapkan	9
Mendaftar untuk Akun AWS	9
Buat pengguna dengan akses administratif	10
Langkah berikutnya	11
Buat sistem file FSx untuk ONTAP	11
Membuat SVM yang bergabung dengan Microsoft Active Directory-	15
Memasang sistem file Anda	16
Membersihkan sumber daya	17
Wilayah AWS	19
Mengakses data Anda	23
Klien yang didukung	24
Menggunakan protokol penyimpanan blok	25
Mengakses data dari dalam AWS Cloud	26
Mengakses data dari VPC yang sama	26
Mengakses data dari VPC yang berbeda	26
Mengakses data dari lokal	30
Mengakses NFS, SMB, ONTAP CLI, dan API dari lokal	31

Mengakses titik akhir antar-cluster dari lokal	32
Konfigurasi perutean untuk mengakses sistem file Multi-AZ dari luar VPC Anda	33
Konfigurasi perutean untuk mengakses sistem file Multi-AZ dari lokal	34
Pemasangan pada klien Linux	35
Menggunakan /etc/fstab untuk me-mount secara otomatis saat reboot instance	36
Pemasangan pada klien Windows	38
Prasyarat	38
Memasang pada klien macOS	40
Penyediaan iSCSI untuk Linux	42
Sebelum Anda mulai	43
Instal dan konfigurasi iSCSI di host Linux	44
Konfigurasi iSCSI pada sistem file untuk FSx ONTAP	46
Pasang iSCSI LUN di klien Linux Anda	48
Penyediaan iSCSI untuk Windows	54
Konfigurasi iSCSI pada klien Windows	56
Konfigurasi iSCSI pada sistem file untuk FSx ONTAP	57
Pasang iSCSI LUN pada klien Windows	58
Memvalidasi konfigurasi iSCSI Anda	62
NVMePenyediaan/TCP untuk Linux	63
Sebelum Anda mulai	64
Instal dan konfigurasi NVMe pada host Linux	65
Konfigurasi NVMe pada FSx sistem file untuk ONTAP	65
Pasang NVMe perangkat di klien Linux Anda	68
Mengakses data melalui titik akses S3	73
Wilayah AWS dengan jalur akses Amazon S3 untuk FSx ONTAP	75
Aturan penamaan, batasan, dan batasan	75
Merujuk titik akses	76
Kompatibilitas titik akses	78
Mengelola akses	82
Membuat titik akses	85
Mengelola titik akses	91
Menggunakan titik akses	94
Memecahkan masalah titik akses	97
Mengakses data dari layanan lain AWS	100
Menggunakan Amazon WorkSpaces	100
Menggunakan Amazon ECS	106

Menggunakan Amazon EVS	109
Menggunakan VMware Cloud	109
Opsi ketersediaan, daya tahan, dan penerapan	110
Memilih jenis penyebaran sistem file	110
Jenis penyebaran AZ tunggal	110
Jenis penyebaran multi-AZ	111
Memilih pembuatan sistem file	113
Proses failover FSx untuk ONTAP	114
Menguji failover pada sebuah sistem file	115
Sumber daya jaringan	115
Subnet	115
Antarmuka jaringan elastis sistem file	115
Performa	118
Mengukur kinerja	118
Latensi	118
Throughput dan IOPS	118
SMB Multichannel dan dukungan NFS nconnect	118
Detail performa	119
Dampak jenis penerapan pada kinerja	121
Dampak kapasitas penyimpanan terhadap performa	123
Dampak kapasitas throughput terhadap performa	124
Contoh: kapasitas penyimpanan dan kapasitas throughput	130
Mengelola sumber daya	132
Mengelola kapasitas penyimpanan	132
Tingkatan penyimpanan	133
Memilih kapasitas penyimpanan sistem file	134
Kapasitas penyimpanan sistem file dan IOPS	138
Kapasitas penyimpanan volume	164
Mengelola sistem file	190
Sumber daya sistem file	190
Membuat sistem file	193
Memperbarui sistem file	207
Mengelola pasangan HA	210
Mengelola NVMe cache	219
Mengelola jenis jaringan	219
Memantau detail sistem file	221

Menghapus sistem file	223
Mengelola SVMs	223
Jumlah maksimum SVMs per sistem file	224
Menciptakan SVMs	225
Memperbarui SVMs	229
Mengelola konfigurasi SVM Microsoft Active Directory	232
Mengaudoit akses file	233
Menyiapkan kelompok kerja	244
Memantau detail SVM	251
Menghapus SVMs	252
Mengelola volume	253
Gaya volume	255
Tipe volume	256
Gaya keamanan volume	257
Membuat volume	258
Memperbarui volume	263
Memindahkan volume	267
Volume pemantauan	271
Menghapus volume	273
Membuat iSCSI LUN	275
Langkah selanjutnya	277
Memperbarui jendela pemeliharaan	277
Mengelola kapasitas throughput	279
Kapan harus mengubah kapasitas throughput	280
Bagaimana permintaan bersamaan ditangani	280
Memperbarui kapasitas throughput	281
Memantau perubahan kapasitas throughput pada konsol	282
Mengelola saham SMB	284
Mengelola dengan NetApp aplikasi	287
Mendaftar untuk NetApp akun	287
Menggunakan NetApp Console	288
Menggunakan CLI NetApp ONTAP	289
Menggunakan ONTAP REST API	293
Pemberian tag pada sumber daya	293
Dasar-dasar tag	294
Pemberian tag pada sumber daya Anda	295

Menyalin tag ke cadangan	296
Batasan tag	297
Izin dan penandaan	297
Melindungi data Anda	299
Mencadangkan volume	299
Cara kerja backup	300
Persyaratan penyimpanan	301
Pencadangan harian otomatis	301
Pencadangan yang diprakarsai pengguna	302
Menyalin tag ke cadangan	303
Menggunakan AWS Backup	303
Memulihkan cadangan	304
Kinerja Backup	306
Mencadangkan volume SnapLock	307
Membuat backup yang diinisiasi pengguna	307
Memulihkan cadangan	308
Memulihkan subset data	312
Memantau kemajuan pemulihan volume	313
Menghapus cadangan	315
Menggunakan snapshot volume	316
Kebijakan snapshot	317
Memulihkan file dari snapshot	318
Melihat snapshot umum	319
Memperbarui ruang cadangan snapshot	320
Menonaktifkan snapshot otomatis	321
Menghapus snapshot	323
Menghapus snapshot	323
Cadangan snapshot	325
Melindungi data dengan Autonomous Ransomware Protection	326
Bagaimana ARP bekerja	326
Apa yang dicari ARP	327
Bagaimana menanggapi dugaan serangan dengan ARP	327
Mengaktifkan ARP	328
Menanggapi peringatan ARP	329
Memahami peringatan EMS untuk ARP	331
Melindungi data dengan SnapLock	332

Cara kerja SnapLock	333
Memahami SnapLock Kepatuhan	338
Memahami SnapLock Perusahaan	339
Memahami periode SnapLock retensi	340
Mengkomit file ke WORM	343
Mereplikasi data Anda dengan FlexCache	348
Cara kerja FlexCache	348
FlexCachemenulis mode	349
FlexCacheikhtisar pembuatan volume	349
MembuatFlexCache	350
Menggunakan SnapMirror untuk replikasi terjadwal	356
Menggunakan NetApp Console untuk menjadwalkan replikasi	356
Menggunakan ONTAP CLI untuk menjadwalkan replikasi	357
Pelaporan penagihan dan penggunaan	358
FSx untuk laporan penagihan ONTAP	358
FSx untuk laporan penggunaan ONTAP	361
Memantau sistem file	366
Pemantauan CloudWatch dengan	367
Mengakses metrik CloudWatch	368
Pemantauan di FSx konsol Amazon	370
Metrik sistem file	381
Metrik sistem file generasi kedua	402
Metrik volume	422
Memantau acara EMS	430
Ikhtisar acara EMS	431
Melihat acara EMS	431
Penerusan acara EMS ke server Syslog	438
Pemantauan dengan Wawasan Infrastruktur Data	440
Pemantauan dengan Panen dan Grafana	441
Memulai Harvest dan Grafana	441
Dasbor Harvest yang Didukung	441
Dasbor yang tidak didukung Harvest	443
CloudFormation template	443
Jenis EC2 instans Amazon	444
Prosedur penyebaran	444
Masuk ke Grafana	448

Pemecahan Masalah Panen dan Grafana	448
Pemantauan AWS CloudTrail dengan	451
FSx Informasi Amazon di CloudTrail	452
Memahami Entri File FSx Log Amazon	453
Bekerja dengan Direktori Aktif	455
Prasyarat Direktori Aktif yang dikelola sendiri	456
Persyaratan Direktori Aktif yang dikelola sendiri	456
Persyaratan konfigurasi jaringan	457
Persyaratan akun layanan Direktori Aktif	458
Praktik terbaik Direktori Aktif yang dikelola sendiri	460
Mendelegasikan izin ke akun layanan Amazon FSx Anda	460
Tetap perbarui konfigurasi AD	461
Batasi lalu lintas dalam VPC dengan grup keamanan	462
Membuat aturan grup keamanan keluar	462
Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager	462
Cara kerja bergabung SVMs ke Active Directory	471
Informasi Direktori Aktif diperlukan	472
Mengelola konfigurasi SVM Active Directory	473
Bergabung SVMs dengan Active Directory	474
Memperbarui konfigurasi Active Directory	477
Memperbarui konfigurasi Active Directory dengan CLI NetApp	479
Migrasi ke Amazon FSx	485
Migrasi menggunakan SnapMirror	485
Sebelum Anda mulai	487
Buat volume tujuan	488
Rekam sumber dan tujuan antar cluster LIFs	490
Membangun cluster peering antara sumber dan tujuan	490
Buat hubungan peering SVM	491
Ciptakan SnapMirror hubungan	492
Transfer data ke sistem file ONTAP Anda FSx	493
Memotong ke Amazon FSx	494
Migrasi file dengan AWS DataSync	495
Prasyarat	496
DataSync langkah dasar migrasi	496
Keamanan	498
Perlindungan data	499

Enkripsi data FSx untuk ONTAP	500
Enkripsi saat diam	500
Mengenkripsi data dalam perjalanan	502
Manajemen identitas dan akses	524
Audiens	524
Mengautentikasi dengan identitas	525
Mengelola akses menggunakan kebijakan	526
FSx untuk ONTAP dan IAM	528
Contoh kebijakan berbasis identitas	533
Menyelesaikan masalah IAM	536
Menggunakan Peran Terkait Layanan	538
Menggunakan tag dengan Amazon FSx	543
AWS kebijakan terkelola	550
Amazon FSx ServiceRolePolicy	551
Amazon FSx DeleteServiceLinkedRoleAccess	551
Amazon FSx FullAccess	551
Amazon FSx ConsoleFullAccess	552
Amazon FSx ConsoleReadOnlyAccess	553
Amazon FSx ReadOnlyAccess	554
Pembaruan kebijakan	554
Kontrol Akses Sistem File dengan Amazon VPC	567
Grup keamanan Amazon VPC	568
Validasi Kepatuhan	571
Titik akhir VPC antarmuka	571
Pertimbangan untuk titik akhir VPC FSx antarmuka Amazon	572
Membuat titik akhir VPC antarmuka untuk Amazon API FSx	572
Membuat kebijakan titik akhir VPC untuk Amazon FSx	573
Ketahanan	573
Pencadangan dan pemulihan	574
Snapshot	574
Zona Ketersediaan	574
Keamanan Infrastruktur	575
Menggunakan perangkat lunak antivirus	575
ONTAP peran dan pengguna	576
Peran administrator sistem file dan pengguna	576
Peran administrator SVM dan pengguna	577

Mengautentikasi ONTAP pengguna dengan Active Directory	580
Membuat ONTAP pengguna baru untuk sistem file dan administrasi SVM	581
Membuat ONTAP pengguna	581
Membuat peran SVM	584
Mengkonfigurasi otentikasi Active Directory untuk pengguna ONTAP	586
Mengkonfigurasi otentikasi kunci publik	588
Memperbarui persyaratan kata sandi	589
Gagal memperbarui kata sandi fsxadmin akun	590
Kuota	592
Kuota yang dapat Anda tingkatkan	592
Kuota sumber daya untuk setiap sistem file	594
Pemecahan masalah	601
Sistem file yang salah konfigurasi	601
Berbagi VPC dinonaktifkan	601
Tidak dapat membuat sistem file Multi-AZ	602
SSD tier lebih dari 90% penuh	602
Anda tidak dapat mengakses sistem file Anda	603
Tag tabel rute tidak ada	603
Terlalu banyak rute	604
Rute tidak ada ke server	604
ENI yang dimodifikasi atau dihapus	604
ENI yang dihapus	605
Tidak ada aturan masuk	605
Aturan keluar yang tidak ada	605
Subnet instance komputasi tidak menggunakan tabel rute apa pun yang terkait dengan sistem file Anda	605
Tidak dapat memperbarui tabel rute Multi-AZ	606
Tidak dapat mengakses iSCSI	606
Subnet VPC yang tidak dibagikan	606
NFS, SMB, ONTAP CLI, dan API tidak dapat diakses dari VPC yang berbeda dan lokal	607
SVM salah konfigurasi	607
SVM Anda memiliki volume offline	607
SVM Anda memiliki volume offline dengan iSCSI LUN atau namespace NVMe/TCP	607
Kunci AWS Secrets Manager rahasia atau KMS tidak dikonfigurasi dengan benar	608
Memecahkan masalah penurunan SSD	608
Penurunan SSD dijeda - pemanfaatan tinggi	609

Penurunan SSD dijeda - FlexClone	609
Pengalihan volume gagal selama penurunan	610
Penurunan SSD terlalu lama	610
Tidak dapat bergabung dengan SVM ke Active Directory	611
Nama NetBIOS SVM sama dengan domain rumah	612
SVM bergabung ke Active Directory lain	612
Nama SVM NetBIOS sudah digunakan	613
Amazon tidak FSx dapat mengakses kredensial akun layanan Direktori Aktif Anda di AWS Secrets Manager	613
FSx tidak dapat menjangkau pengontrol domain Active Directory	615
Konfigurasi port atau izin akun layanan tidak memadai	615
Kredensial akun layanan tidak valid	616
Amazon tidak FSx dapat terhubung ke pengontrol domain Direktori Aktif karena kredensial akun layanan tidak mencukupi	616
Tidak dapat menjangkau server DNS Active Directory atau pengontrol domain	617
Nama domain Direktori Aktif tidak valid	619
Akun layanan tidak dapat mengakses grup administrator Direktori Aktif	620
OU yang ditentukan tidak valid	620
Tidak dapat menghapus SVM atau volume	621
Mengidentifikasi penghapusan yang gagal	622
Penghapusan SVM: Tabel rute tidak dapat diakses	622
Penghapusan SVM: Hubungan teman sebaya	623
SVM atau penghapusan volume: SnapMirror	624
Penghapusan SVM: LIF berkemampuan Kerberos	625
Penghapusan SVM: Alasan lain	627
Penghapusan volume: hubungan FlexCache	629
Volume salah konfigurasi	630
Volume lebih dari 98% penuh	630
Volume penyimpanan blok sedang offline	630
Volume FlexCache asal offline	631
Volume offline dengan SnapMirror hubungan	631
Volume penyimpanan blok dibatasi	631
Volume FlexCache asal terbatas	632
Volume terbatas dengan SnapMirror hubungan	632
Volume memiliki penyimpanan yang tidak mencukupi	633
Tentukan bagaimana kapasitas penyimpanan volume Anda digunakan	633

Meningkatkan kapasitas penyimpanan volume	633
Menggunakan autosizing volume	634
Penyimpanan utama sistem file Anda penuh	634
Menghapus snapshot	634
Meningkatkan kapasitas file maksimum volume	635
Pencadangan volume gagal	635
Memulihkan volume yang dihapus	636
Memecahkan masalah jaringan	636
Anda ingin menangkap jejak paket	636
Kesalahan I/O dan kegagalan klaim kembali kunci NFS	639
Kesalahan I/O selama kegagalan	639
NFSv4 alternatif	642
Riwayat dokumen	643
.....	dclxviii

Apa itu Amazon FSx untuk NetApp ONTAP?

Amazon FSx untuk NetApp ONTAP adalah layanan yang dikelola sepenuhnya yang menyediakan penyimpanan file yang sangat andal, terukur, berkinerja tinggi, dan kaya fitur yang dibangun di atas NetApp sistem file ONTAP yang populer. FSx untuk ONTAP menggabungkan fitur yang sudah dikenal, kinerja, kemampuan, dan operasi API sistem NetApp file dengan kelincahan, skalabilitas, dan kesederhanaan yang dikelola sepenuhnya. Layanan AWS

FSx untuk ONTAP menyediakan penyimpanan file bersama yang kaya fitur, cepat, dan fleksibel yang dapat diakses secara luas dari Linux, Windows, dan instance komputasi macOS yang berjalan di dalam atau di tempat. AWS FSx untuk ONTAP menawarkan penyimpanan solid state drive (SSD) berkinerja tinggi dengan latensi submilidetik. Dengan FSx ONTAP, Anda dapat mencapai tingkat kinerja SSD untuk beban kerja Anda sambil membayar penyimpanan SSD hanya untuk sebagian kecil dari data Anda.

Mengelola data Anda dengan FSx ONTAP lebih mudah karena Anda dapat memotret, mengkloning, dan mereplikasi file Anda dengan mengklik tombol. Selain itu, FSx untuk ONTAP secara otomatis meningkatkan data Anda ke penyimpanan elastis berbiaya lebih rendah, sehingga mengurangi kebutuhan Anda untuk menyediakan atau mengelola kapasitas.

FSx untuk ONTAP juga menyediakan penyimpanan yang sangat tersedia dan tahan lama dengan cadangan yang dikelola sepenuhnya dan dukungan untuk pemulihan bencana lintas wilayah. Untuk membuatnya lebih mudah untuk melindungi dan mengamankan data Anda, FSx untuk ONTAP mendukung keamanan data populer dan aplikasi antivirus.

Bagi pelanggan yang menggunakan NetApp ONTAP lokal, FSx ONTAP adalah solusi ideal untuk memigrasi, mencadangkan, atau mem-burst aplikasi berbasis file Anda dari lokal ke lokasi AWS tanpa perlu mengubah kode aplikasi atau cara Anda mengelola data.

Sebagai layanan yang dikelola sepenuhnya, FSx ONTAP memudahkan peluncuran dan skala penyimpanan file bersama yang andal, berkinerja tinggi, dan aman di cloud. Dengan FSx untuk ONTAP, Anda tidak perlu lagi khawatir tentang:

- Menyiapkan dan menyediakan server file dan volume penyimpanan
- Mereplikasi data
- Menginstal dan menambal perangkat lunak server file
- Mendeteksi dan mengatasi kegagalan perangkat keras

- Mengelola failover dan failback
- Melakukan backup secara manual

FSx untuk ONTAP juga menyediakan integrasi yang kaya dengan AWS layanan lain, seperti AWS Identity and Access Management (IAM) WorkSpaces, Amazon, AWS Key Management Service (AWS KMS), dan. AWS CloudTrail

Topik

- [Fitur FSx untuk ONTAP](#)
- [Keamanan dan perlindungan data](#)
- [Alat-alat pemantauan](#)
- [Harga FSx untuk ONTAP](#)
- [FSx untuk ONTAP di AWS re:Post](#)
- [Apakah Anda FSx pengguna Amazon pertama kali?](#)

Fitur FSx untuk ONTAP

Dengan FSx untuk ONTAP, Anda mendapatkan solusi penyimpanan file yang dikelola sepenuhnya dengan:

- Support untuk dataset skala petabyte dalam satu namespace
- Hingga puluhan gigabyte per detik (GBps) [throughput per sistem file](#)
- [Akses multi-protokol ke data](#) menggunakan Network File System (NFS), Server Message Block (SMB), Internet Small Computer Systems Interface (iSCSI), dan protokol Non-Volatile Memory Express () NVMe
- Opsi penyebaran [Multi-AZ dan Single-AZ yang sangat tersedia dan](#) tahan lama
- Tingkat data otomatis yang mengurangi biaya penyimpanan dengan secara otomatis mentransisikan data yang jarang diakses ke tingkat penyimpanan berbiaya lebih rendah berdasarkan pola akses Anda
- Kompresi data, deduplikasi, dan pemadatan untuk mengurangi konsumsi penyimpanan Anda
- Support untuk dua [opsi tipe jaringan](#), IPv4 -only dan dual-stack (yang mendukung keduanya IPv4 dan IPv6), untuk mengakses dan mengelola sistem file Anda
- Dukungan untuk NetApp fitur [SnapMirrorreplikasi](#)

- Support untuk NetApp solusi FlexCache caching lokal
- Support untuk akses dan manajemen menggunakan native AWS atau NetApp tools dan operasi API
 - Konsol Manajemen AWS, AWS Command Line Interface (AWS CLI), dan SDKs
 - [NetApp ONTAP CLI, REST API, dan Konsol NetApp](#)

Keamanan dan perlindungan data

Model tanggung jawab bersama digunakan dalam kaitannya [Keamanan di Amazon FSx untuk NetApp ONTAP](#) dengan. Amazon FSx menyediakan berbagai tingkat keamanan dan [kepatuhan](#) untuk memfasilitasi perlindungan data Anda.

FSx untuk ONTAP mendukung perlindungan data, keamanan, dan fitur kontrol akses berikut:

- [Mengkripsi data saat istirahat](#) untuk data sistem file dan backup menggunakan AWS KMS keys
- Mengenkripsi data dalam perjalanan menggunakan:
 - [SMB Kerberos](#)
 - [IPSEC](#)
 - [Enkripsi berbasis Nitro](#)
- Pemindaian [antivirus](#) sesuai permintaan
- Otentikasi dan otorisasi menggunakan [Microsoft Active Directory](#)
- [Audit akses file](#)
- [NetAppSnapLock](#) WORM dengan mode Kepatuhan dan retensi Perusahaan

Untuk informasi selengkapnya, lihat [Perlindungan data di Amazon FSx untuk NetApp ONTAP](#) dan [Melindungi data Anda](#).

Selain itu, Amazon FSx melindungi data Anda dengan cadangan sistem file yang sangat tahan lama. Amazon FSx melakukan pencadangan harian otomatis, dan Anda dapat mengambil cadangan tambahan kapan saja. Untuk informasi selengkapnya, lihat [Melindungi data Anda](#).

Alat-alat pemantauan

Alat pemantauan meliputi [CloudWatch](#), [acara ONTAP EMS CloudTrail](#), [Wawasan Infrastruktur NetApp Data](#), dan [NetAppHarvest](#).

Harga FSx untuk ONTAP

Anda ditagih untuk sistem file berdasarkan kategori berikut:

- Kapasitas penyimpanan SSD (per gigabyte-bulan, atau GB-bulan)
- SSD IOPS yang Anda berikan di atas tiga IOPS/GB (per IOPS bulan)
- Kapasitas throughput (per megabyte per detik [] MBps -bulan)
- Konsumsi penyimpanan kolam kapasitas (per GB-bulan)
- Permintaan kolam kapasitas (per baca dan tulis)
- Konsumsi penyimpanan cadangan (per GB-bulan)

Untuk informasi selengkapnya tentang harga dan biaya yang terkait dengan layanan, lihat [Amazon FSx untuk harga NetApp ONTAP](#).

FSx untuk ONTAP di AWS re:Post

Jika Anda mengalami masalah saat menggunakan Amazon FSx, gunakan [AWS re:Post](#) untuk mendapatkan jawaban atas pertanyaan ONTAP Anda FSx .

Apakah Anda FSx pengguna Amazon pertama kali?

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

1. Jika Anda baru mengenal AWS, lihat [Menyiapkan FSx untuk ONTAP](#) untuk menyiapkan Akun AWS.
2. Jika Anda siap membuat sistem FSx file Amazon pertama Anda, ikuti instruksi di [Memulai dengan Amazon FSx untuk NetApp ONTAP](#).
3. Untuk informasi tentang kinerja, lihat [Amazon FSx untuk kinerja NetApp ONTAP](#).
4. Untuk detail FSx keamanan Amazon, lihat [Keamanan di Amazon FSx untuk NetApp ONTAP](#).
5. Untuk informasi tentang Amazon FSx API, lihat [Referensi Amazon FSx API](#).

Cara kerja Amazon FSx untuk NetApp ONTAP

Topik ini memperkenalkan fitur utama Amazon FSx untuk sistem file NetApp ONTAP dan cara kerjanya, dengan tautan ke bagian dengan deskripsi mendalam, detail implementasi penting, dan prosedur konfigurasi. step-by-step

Topik

- [FSx untuk sistem file ONTAP](#)
- [Penyimpanan mesin virtual](#)
- [volume](#)
- [Tingkatan penyimpanan](#)
- [Efisiensi penyimpanan](#)
- [Mengakses data yang disimpan FSx untuk sistem file ONTAP](#)
- [Mengelola FSx sumber daya ONTAP](#)

FSx untuk sistem file ONTAP

Sistem file adalah yang utama FSx untuk sumber daya ONTAP, analog dengan kluster NetApp ONTAP lokal. Anda menentukan kapasitas penyimpanan solid state drive (SSD) dan kapasitas throughput untuk sistem file Anda, dan pilih Amazon Virtual Private Cloud (VPC) tempat sistem file Anda dibuat. Untuk informasi selengkapnya, lihat [Mengelola FSx untuk sistem file ONTAP](#).

Sistem file Anda dapat memiliki satu hingga 12 pasangan ketersediaan tinggi (HA) tergantung pada konfigurasinya. Pasangan HA terdiri dari dua server file dalam konfigurasi siaga aktif. Generasi pertama FSx untuk sistem file ONTAP dan sistem file Multi-AZ generasi kedua mendukung satu pasangan HA. Sistem file Single-AZ generasi kedua mendukung hingga 12 pasang HA. Untuk informasi selengkapnya, lihat [Mengelola pasangan ketersediaan tinggi \(HA\)](#).

Penyimpanan mesin virtual

Storage Virtual Machine (SVM) adalah file server terisolasi dengan endpoint administratif dan akses data sendiri untuk mengelola dan mengakses data. Saat Anda mengakses data dalam sistem file ONTAP Anda, klien dan workstation Anda berinteraksi dengan SVM menggunakan alamat IP titik akhir SVM. FSx Untuk informasi selengkapnya, lihat [Mengelola SVMs](#).

Anda dapat bergabung SVMs ke Microsoft Active Directory untuk otentikasi dan otorisasi akses file. Untuk informasi selengkapnya, lihat [Bekerja dengan Microsoft Active Directory FSx untuk ONTAP](#).

volume

FSx untuk volume ONTAP adalah sumber daya virtual yang Anda gunakan untuk mengatur dan mengelompokkan data Anda. Volume adalah wadah logis yang di-host SVMs, dan data yang disimpan di dalamnya menghabiskan kapasitas penyimpanan fisik pada sistem file Anda.

Saat Anda membuat volume, Anda mengatur ukurannya, yang menentukan jumlah data fisik yang dapat Anda simpan di dalamnya, terlepas dari tingkat penyimpanan mana data disimpan. Anda juga mengatur jenis volume, baik RW (read-writable) atau DP (perlindungan data). Volume DP adalah read-only dan dapat digunakan sebagai tujuan dalam hubungan atau NetApp SnapMirror . SnapVault

FSx untuk volume ONTAP disediakan tipis, artinya mereka hanya mengkonsumsi kapasitas penyimpanan untuk data yang disimpan di dalamnya. Dengan volume yang disediakan tipis, kapasitas penyimpanan tidak dicadangkan terlebih dahulu. Sebaliknya, penyimpanan dialokasikan secara dinamis, seperti yang diperlukan. Ruang kosong dilepaskan kembali ke sistem file ketika data dalam volume atau LUN dihapus. Misalnya, Anda dapat membuat tiga volume 10 TiB pada sistem file yang dikonfigurasi dengan kapasitas penyimpanan gratis 10 TiB, selama jumlah total data yang disimpan dalam tiga volume tidak melebihi 10 TiB setiap saat. Jumlah data yang disimpan secara fisik pada volume dihitung terhadap konsumsi kapasitas penyimpanan Anda secara keseluruhan. Untuk informasi selengkapnya, lihat [Mengelola FSx volume ONTAP](#).

Tingkatan penyimpanan

Sistem file FSx untuk ONTAP memiliki dua tingkatan penyimpanan: penyimpanan primer dan penyimpanan kolam kapasitas. Penyimpanan primer disediakan, dapat diskalakan, penyimpanan SSD berkinerja tinggi yang dibuat khusus untuk bagian aktif kumpulan data Anda. Penyimpanan kolam kapasitas adalah tingkat penyimpanan yang sepenuhnya elastis yang dapat menskalakan hingga ukuran petabyte dan dioptimalkan biaya untuk data yang jarang diakses. Data yang Anda tulis ke volume Anda menghabiskan kapasitas pada tingkatan penyimpanan Anda. Untuk informasi selengkapnya, lihat [FSx untuk tingkatan penyimpanan ONTAP](#). Anda dapat meningkatkan kapasitas penyimpanan SSD dari sistem file Anda seiring dengan bertambahnya kebutuhan penyimpanan Anda. Pada sistem file generasi kedua, Anda juga dapat mengurangi kapasitas penyimpanan SSD ketika persyaratan penyimpanan berkinerja tinggi Anda berubah, memungkinkan Anda mengoptimalkan biaya penyimpanan. Untuk informasi selengkapnya, lihat [Kapasitas penyimpanan sistem file dan IOPS](#).

Tingkatan data

Tingkatan data adalah proses dimana Amazon FSx untuk NetApp ONTAP secara otomatis memindahkan data antara SSD dan tingkatan penyimpanan kumpulan kapasitas. Setiap volume memiliki kebijakan tiering yang mengontrol apakah data dipindahkan ke tingkat kapasitas ketika menjadi tidak aktif (dingin). Periode pendinginan kebijakan Tiering volume menentukan kapan data menjadi tidak aktif (dingin). Untuk informasi selengkapnya, lihat [Tingkat data volume](#).

Efisiensi penyimpanan

Amazon FSx untuk NetApp ONTAP mendukung fitur efisiensi penyimpanan tingkat blok ONTAP —pemadatan, kompresi, dan deduplikasi— untuk mengurangi kapasitas penyimpanan yang dikonsumsi data Anda. Fitur efisiensi penyimpanan dapat mengurangi jejak data Anda dalam penyimpanan SSD, penyimpanan kolam kapasitas, dan cadangan. Penghematan kapasitas penyimpanan tipikal untuk beban kerja berbagi file tujuan umum tanpa mengorbankan kinerja adalah 65% dari kompresi, deduplikasi, dan pemadatan, baik pada SSD maupun tingkatan penyimpanan kolam kapasitas. Untuk informasi selengkapnya, lihat [Efisiensi penyimpanan](#).

Mengakses data yang disimpan FSx untuk sistem file ONTAP

Anda dapat mengakses data Anda FSx untuk volume ONTAP dari beberapa klien Linux, Windows, atau macOS secara bersamaan melalui protokol NFS (v3, v4, v4.1, v4.2) dan SMB. Anda juga dapat mengakses data menggunakan protokol blok Non-Volatile Memory Express (NVMe) dan Internet Small Computer Systems Interface (iSCSI). Untuk informasi selengkapnya, lihat [Mengakses data FSx ONTAP Anda](#).

Mengelola FSx sumber daya ONTAP

Ada beberapa cara agar Anda dapat berinteraksi dengan sistem file FSx ONTAP Anda dan mengelola sumber dayanya. Anda dapat mengelola sumber daya ONTAP menggunakan keduanya AWS dan alat manajemen NetApp ONTAP: FSx

- AWS alat manajemen
 - The Konsol Manajemen AWS
 - AWS Command Line Interface (AWS CLI)
 - FSx API Amazon dan SDKs

- AWS CloudFormation
- NetApp alat manajemen:
 - NetApp Konsol
 - CLI NetApp ONTAP
 - API REST NetApp ONTAP

Lihat informasi yang lebih lengkap di [Mengelola sumber daya](#).

Memulai dengan Amazon FSx untuk NetApp ONTAP

Pelajari cara mulai menggunakan Amazon FSx untuk NetApp ONTAP. Latihan memulai ini mencakup langkah-langkah berikut.

1. Mendaftar untuk Akun AWS dan membuat pengguna administratif di akun.
2. Buat Amazon FSx untuk sistem file NetApp ONTAP menggunakan FSx konsol Amazon.
3. Pasang sistem file Anda dari instans Amazon EC2 Linux.
4. Bersihkan sumber daya yang Anda buat.

Topik

- [Menyiapkan FSx untuk ONTAP](#)
- [Buat Amazon FSx untuk sistem file NetApp ONTAP](#)
- [Memasang sistem file Anda dari instans Amazon EC2 Linux](#)
- [Membersihkan sumber daya](#)

Menyiapkan FSx untuk ONTAP

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

1. [Mendaftar untuk Akun AWS](#)
2. [Buat pengguna dengan akses administratif](#)

Topik

- [Mendaftar untuk Akun AWS](#)
- [Buat pengguna dengan akses administratif](#)
- [Langkah berikutnya](#)

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

AWS mengirim 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.com/ke/> 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 [Konsol Manajemen AWS](#) sebagai 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 berikutnya

Untuk mulai menggunakan FSx ONTAP, lihat petunjuk [Memulai dengan Amazon FSx untuk NetApp ONTAP](#) untuk membuat FSx sumber daya Amazon Anda.

Buat Amazon FSx untuk sistem file NetApp ONTAP

FSx Konsol Amazon memiliki dua opsi untuk membuat sistem file — opsi Buat cepat dan opsi buat Standar. Untuk membuat sistem file Amazon FSx untuk NetApp ONTAP dengan cepat dan mudah dengan konfigurasi yang direkomendasikan layanan, gunakan opsi Buat cepat.

Opsi Quick create mengkonfigurasi sistem file ini untuk memungkinkan akses data dari instance Linux melalui protokol Network File System (NFS). Setelah sistem file dibuat, Anda dapat membuat tambahan SVMs dan volume sesuai kebutuhan, termasuk SVM yang digabungkan ke Active Directory untuk memungkinkan akses dari klien Windows dan macOS melalui protokol Server Message Block (SMB). Anda juga dapat menambahkan pasangan ketersediaan tinggi (HA) tambahan tergantung pada jenis penerapan yang Anda pilih dan berapa banyak pasangan HA yang Anda tambahkan saat pembuatan.

 Note

FSx untuk sistem file ONTAP yang dibuat dengan opsi Buat cepat menggunakan jenis **IPv4** Jaringan. Untuk membuat sistem file dengan tipe Jaringan Dual-stack (yang mendukung keduanya IPv4 dan IPv6), gunakan opsi Buat Standar.

Untuk informasi tentang menggunakan opsi Buat Standar untuk membuat sistem file dengan konfigurasi yang disesuaikan, dan untuk menggunakan API AWS CLI dan, lihat [Membuat sistem file](#).

Untuk membuat sistem file Anda

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 Amazon FSx untuk NetApp ONTAP, lalu pilih Berikutnya. Halaman Create ONTAP file system muncul.
4. Untuk metode Creation, pilih Quick create.
5. Di bagian Konfigurasi cepat, untuk Nama sistem file - opsional, masukkan nama untuk sistem file Anda. Lebih mudah untuk menemukan dan mengelola sistem file Anda ketika Anda memainkannya. Anda dapat menggunakan maksimal 256 huruf Unicode, spasi putih, dan angka, ditambah karakter khusus ini: + - (tanda hubung) =. _ (garis bawah):/
6. Untuk Jenis Deployment Pilih Multi-AZ atau Single-AZ.
 - Sistem file multi-AZ mereplikasi data Anda dan mendukung failover di beberapa Availability Zone secara bersamaan. Wilayah AWS
 - Sistem file single-AZ mereplikasi data Anda dan menawarkan failover otomatis dalam satu Availability Zone.

Untuk informasi selengkapnya, lihat [Opsi ketersediaan, daya tahan, dan penerapan](#).

 Note

Generasi terbaru FSx untuk sistem file ONTAP yang tersedia untuk Anda Wilayah AWS dipilih secara default. Anda dapat menentukan generasi sistem file Anda (tersedia Wilayah AWS) dengan opsi Buat Standar. Untuk informasi selengkapnya, lihat [Membuat sistem file](#).

7. Untuk kapasitas penyimpanan SSD, tentukan kapasitas penyimpanan sistem file Anda, dalam gibibytes (GiB). Masukkan bilangan bulat apa pun dalam kisaran 1.024—1.048.576. Untuk informasi selengkapnya, lihat [Untuk membuat sistem file \(konsol\)](#).

Anda dapat meningkatkan jumlah kapasitas penyimpanan sesuai kebutuhan setiap saat setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat [Mengelola kapasitas penyimpanan](#).

8. Untuk kapasitas Throughput, Amazon FSx secara otomatis menyediakan kapasitas throughput yang direkomendasikan berdasarkan penyimpanan SSD Anda. Anda juga dapat memilih throughput sistem file Anda (hingga 73.728 MBps tergantung pada jenis penerapan dan jumlah pasangan HA).
9. Untuk Virtual Private Cloud (VPC), pilih Amazon VPC yang ingin Anda kaitkan dengan sistem file Anda.
10. (Hanya multi-AZ) Rentang alamat IP titik akhir menentukan rentang alamat IP di mana titik akhir untuk mengakses sistem file Anda dibuat.

Pilih opsi Buat cepat untuk rentang alamat IP titik akhir:

- Rentang IPv4 alamat yang tidak terisi dari VPC Anda — Pilih opsi ini agar Amazon FSx menggunakan 64 alamat IP terakhir dari rentang CIDR utama VPC sebagai rentang alamat titik akhir IPv4 untuk sistem file. Perhatikan bahwa rentang ini dibagi di beberapa sistem file jika Anda memilih opsi ini beberapa kali.

 Note

- Setiap sistem file yang Anda buat menggunakan dua alamat IP dari rentang ini—satu untuk cluster, dan satu untuk SVM pertama. Alamat IP pertama dan terakhir juga dicadangkan. Untuk setiap SVM tambahan, sistem file mengkonsumsi alamat IP lain. Misalnya, sistem file yang menampung 10 SVMs menggunakan 11 alamat IP. Sistem file tambahan bekerja dengan cara yang sama. Mereka menggunakan

dua alamat IP awal, ditambah satu untuk setiap SVM tambahan. Jumlah maksimum sistem file yang menggunakan rentang alamat IP yang sama, masing-masing dengan SVM tunggal, adalah 31.

- Opsi ini berwarna abu-abu jika salah satu dari 64 alamat IP terakhir dalam rentang CIDR utama VPC digunakan oleh subnet.
- Rentang IPv4 alamat mengambang di luar VPC Anda - Pilih opsi ini agar Amazon FSx menggunakan rentang alamat 198.19.x.0/24 yang belum digunakan oleh sistem file lain dengan VPC dan tabel rute yang sama.

Anda juga dapat menentukan rentang alamat IP Anda sendiri di opsi Buat standar. Rentang alamat IP yang Anda pilih dapat berada di dalam atau di luar rentang IPv4 alamat VPC, asalkan tidak tumpang tindih dengan subnet apa pun, dan selama itu belum digunakan oleh sistem file lain dengan VPC dan tabel rute yang sama. Sebaiknya gunakan rentang yang ada di dalam rentang alamat IP VPC.

 Note

Pastikan bahwa semua tabel rute yang Anda gunakan terkait dengan sistem file Multi-AZ Anda. Melakukannya membantu mencegah tidak tersedianya selama failover. Untuk informasi tentang mengaitkan tabel rute VPC Amazon Anda dengan sistem file Anda, lihat [Memperbarui sistem file](#)

11. Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur efisiensi penyimpanan ONTAP (kompresi, deduplikasi, dan pemadatan) atau Dinonaktifkan untuk mematikannya.
12. Pilih Berikutnya, dan tinjau konfigurasi sistem file pada halaman Create ONTAP file system. Perhatikan pengaturan sistem file mana yang dapat Anda modifikasi setelah sistem file dibuat.
13. Pilih Buat sistem file.

Quick create membuat sistem file dengan satu SVM (bernama `fsx`) dan satu volume (bernama `vol1`). Volume memiliki jalur persimpangan `/vol1` dan kebijakan tingkatan kumpulan kapasitas Auto (yang secara otomatis akan memberi peringkat data apa pun yang belum diakses selama 31 hari ke penyimpanan kolam berkapasitas lebih rendah). Kebijakan snapshot default ditetapkan ke volume default. Data sistem file dienkripsi saat istirahat menggunakan kunci terkelola AWS KMS layanan default Anda.

Membuat SVM yang bergabung dengan Microsoft Active Directory-

Setelah membuat sistem file, Anda dapat membuat tambahan SVMs bergabung ke Microsoft Active Directory untuk mengaktifkan akses SMB dari klien Windows dan macOS. FSx untuk ONTAP terintegrasi dengan AWS Secrets Manager untuk mengelola domain Microsoft Active Directory Anda dengan aman, bergabung dengan kredensial akun layanan.

Untuk membuat SVM yang bergabung dengan Microsoft Active Directory-

1. Di FSx konsol Amazon, pilih Storage virtual machines dari panel navigasi kiri.
2. Pilih Buat mesin virtual penyimpanan.
3. Untuk sistem File, pilih sistem file yang Anda buat.
4. Untuk nama mesin virtual Storage, masukkan nama untuk SVM Anda.
5. Untuk konfigurasi Microsoft Active Directory, pilih Bergabung dengan Microsoft Active Directory.
6. Untuk kredensial akun layanan bergabung dengan Domain, pilih Dikelola di Secrets Manager (default) untuk menggunakan Secrets Manager untuk pengelolaan kredensial yang aman.

Note

Menggunakan Secrets Manager menghilangkan kebutuhan untuk menyimpan kredensial plaintext dan menyediakan manajemen kredensial terpusat. Untuk informasi selengkapnya, lihat [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).

7. Untuk Rahasia, pilih rahasia yang ada dari Secrets Manager yang berisi kredensial akun layanan bergabung domain Anda, atau pilih Buat rahasia baru untuk membuatnya.
8. Lengkapi kolom konfigurasi Microsoft Active Directory yang tersisa sesuai kebutuhan untuk lingkungan Anda.
9. Pilih Buat mesin virtual penyimpanan.

SVM Anda akan dibuat dan digabungkan ke Microsoft Active Directory menggunakan kredensial yang disimpan di Secrets Manager. Anda sekarang dapat membuat share dan volume SMB di SVM ini untuk akses klien Windows dan macOS.

Memasang sistem file Anda dari instans Amazon EC2 Linux

Anda dapat memasang sistem file dari instans Amazon Elastic Compute Cloud (Amazon EC2). Prosedur ini menggunakan instance yang menjalankan Amazon Linux 2.

Untuk me-mount sistem file Anda dari Amazon EC2

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Buat atau pilih EC2 instans Amazon yang menjalankan Amazon Linux 2 yang berada di cloud pribadi virtual (VPC) yang sama dengan sistem file Anda. Untuk informasi selengkapnya tentang meluncurkan instance, lihat [Langkah 1: Meluncurkan instance](#) di Panduan EC2 Pengguna Amazon.
3. Connect ke instans Amazon EC2 Linux Anda. Untuk informasi selengkapnya, lihat [Connect ke instans Linux Anda](#) di Panduan EC2 Pengguna Amazon.
4. Buka terminal di EC2 instans Amazon Anda menggunakan shell aman (SSH), dan masuk dengan kredensi yang sesuai.
5. Buat direktori di EC2 instans Amazon Anda untuk digunakan sebagai titik pemasangan volume dengan perintah berikut. Dalam contoh berikut, ganti *mount-point* dengan informasi Anda sendiri.

```
$ sudo mkdir /mount-point
```

6. Pasang Amazon Anda FSx untuk sistem file NetApp ONTAP ke direktori yang Anda buat. Gunakan mount perintah yang mirip dengan contoh berikut. Dalam contoh berikut, ganti nilai placeholder berikut dengan informasi Anda sendiri.
 - *nfs_version*— Versi NFS yang Anda gunakan; FSx untuk ONTAP mendukung versi 3, 4.0, 4.1, dan 4.2.
 - *nfs-dns-name*— Nama DNS NFS dari mesin virtual penyimpanan (SVM) di mana volume yang Anda pasang ada. Anda dapat menemukan nama DNS NFS di FSx konsol Amazon dengan memilih mesin virtual Penyimpanan, lalu memilih SVM tempat volume yang Anda pasang ada. Nama DNS NFS ditemukan di panel Endpoints.
 - *volume-junction-path*— Jalur persimpangan volume yang Anda pasang. Anda dapat menemukan jalur persimpangan volume di FSx konsol Amazon pada panel Ringkasan halaman Detail volume.

- **mount-point**— Nama direktori yang Anda buat pada EC2 instance Anda untuk titik pemasangan volume.

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

Perintah berikut menggunakan nilai contoh.

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

Jika Anda memiliki masalah dengan EC2 instans Amazon Anda (seperti waktu koneksi habis), lihat [Memecahkan masalah EC2 instans di Panduan Pengguna Amazon EC2](#).

Membersihkan sumber daya

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

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. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
3. Di FSx konsol Amazon, hapus semua volume FSx ONTAP Anda yang bukan volume root SVM Anda. Untuk informasi selengkapnya, lihat [Menghapus volume](#).
4. Hapus semua FSx untuk ONTAP SVMs. Untuk informasi selengkapnya, lihat [Menghapus penyimpanan mesin virtual \(SVM\)](#).
5. Di FSx konsol Amazon, hapus sistem file Anda. Ketika Anda menghapus sistem file, semua backup otomatis dihapus secara otomatis. Namun, Anda masih harus menghapus cadangan yang dibuat secara manual. Langkah-langkah berikut menguraikan proses ini.
 - a. Dari dasbor konsol, pilih nama sistem file yang Anda buat untuk latihan ini.
 - b. Untuk Tindakan, pilih Hapus sistem file.

- c. Dalam kotak dialog Hapus sistem file, masukkan ID sistem file yang ingin Anda hapus di kotak ID sistem file.
- d. Pilih Hapus sistem file.
- e. Sementara Amazon FSx menghapus sistem file, statusnya di dasbor berubah menjadi DELETING. Setelah sistem file dihapus, itu tidak lagi muncul di dasbor. Setiap backup otomatis dihapus bersama dengan sistem file.
- f. Sekarang Anda dapat menghapus backup apa pun yang dibuat secara manual untuk sistem file Anda. Dari navigasi sisi kiri, pilih Backup.
- g. Dari dasbor, pilih backup apa pun yang memiliki ID sistem file yang sama dengan sistem file yang Anda hapus, dan pilih Hapus backup. Pastikan untuk menyimpan cadangan akhir, jika Anda membuatnya.
- h. Kotak dialog Hapus backup terbuka. Biarkan kotak centang dipilih untuk cadangan yang ingin Anda hapus, lalu pilih Hapus cadangan. IDs

Sistem FSx file Amazon Anda dan cadangan otomatis terkait sekarang dihapus, bersama dengan cadangan manual apa pun yang Anda pilih untuk dihapus juga.

Ketersediaan oleh Wilayah AWS

Amazon FSx untuk sistem file NetApp ONTAP tersedia di berikut ini Wilayah AWS, dengan dukungan jenis penerapan ditunjukkan untuk setiap wilayah:

Wilayah AWS	Tunggal-AZ 1	Multi-AZ 1	Tunggal-AZ 2	Multi-AZ 2		
Timur AS (N. Virginia)	✓	✓	✓	✓		
AS Timur (Ohio)	✓	✓	✓	✓		
AS Barat (California Utara)	✓	✓	✓	✓		
AS Barat (Oregon)	✓	✓	✓	✓		
AWS GovCloud (AS-Timur)	✓	✓				
AWS GovCloud (AS-Barat)	✓	✓				
Afrika (Cape Town)	✓	✓				
Asia Pacific (Hong Kong)	✓	✓				

Wilayah AWS	Tunggal-AZ 1	Multi-AZ 1	Tunggal-AZ 2	Multi-AZ 2		
Asia Pacific (Tokyo)	✓	✓	✓	✓		
Asia Pasifik (Seoul)	✓	✓	✓	✓		
Asia Pasifik (Osaka)	✓	✓				
Asia Pasifik (Mumbai)	✓	✓	✓	✓		
Asia Pasifik (Hyderabad)	✓	✓				
Asia Pasifik (Singapura)	✓	✓	✓	✓		
Asia Pasifik (Sydney)	✓	✓	✓	✓		
Asia Pasifik (Jakarta)	✓	✓				

Wilayah AWS	Tunggal-AZ 1	Multi-AZ 1	Tunggal-AZ 2	Multi-AZ 2		
Asia Pasifik (Melbourne)	✓	✓				
Asia Pasifik (Malaysia)	✓	✓				
Asia Pasifik (Taipei)	✓	✓				
Asia Pasifik (Thailand)	✓	✓				
Kanada (Pusat)	✓	✓	✓	✓		
Kanada Barat (Calgary)	✓	✓				
Eropa (Frankfurt)	✓	✓	✓	✓		
Eropa (Zürich)	✓	✓	✓	✓		
Eropa (Stockholm)	✓	✓	✓	✓		
Eropa (Milan)	✓	✓				

Wilayah AWS	Tunggal-AZ 1	Multi-AZ 1	Tunggal-AZ 2	Multi-AZ 2		
Eropa (Spanyol)	✓	✓	✓	✓		
Eropa (Irlandia)	✓	✓	✓	✓		
Eropa (London)	✓	✓				
Eropa (Paris)	✓	✓				
Israel (Tel Aviv)	✓	✓				
Meksiko (Tengah)	✓	✓				
Timur Tengah (UEA)	✓	✓				
Timur Tengah (Bahrain)	✓	✓				
Amerika Selatan (Sao Paulo)	✓	✓				

Mengakses data FSx ONTAP Anda

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

Setiap SVM memiliki empat titik akhir yang digunakan untuk mengakses data atau mengelola SVM menggunakan ONTAP NetApp CLI atau REST API:

- **Nfs**— Untuk menghubungkan menggunakan protokol Network File System (NFS)
- **Smb**— Untuk menghubungkan menggunakan protokol Service Message Block (SMB) (Jika SVM Anda bergabung ke Active Directory, atau Anda menggunakan workgroup.)
- **Iscsi**— Untuk menghubungkan menggunakan protokol Internet Small Computer Systems Interface (iSCSI) untuk dukungan penyimpanan blok bersama.
- **Nvme**— Untuk menghubungkan menggunakan Non-Volatile Memory Express (NVMe) over TCP/IP untuk dukungan penyimpanan blok bersama.
- **Management**— Untuk mengelola SVMs menggunakan NetApp ONTAP CLI atau API, atau Konsol NetApp

Note

Protokol iSCSI tersedia di semua sistem file yang memiliki 6 atau [lebih sedikit pasangan pasangan ketersediaan tinggi](#) (HA). NVMe/TCP Protokol ini tersedia pada sistem file generasi kedua yang memiliki 6 atau lebih sedikit pasangan HA.

Topik

- [Klien yang didukung](#)
- [Menggunakan protokol penyimpanan blok](#)
- [Mengakses data dari dalam AWS Cloud](#)
- [Mengakses data dari lokal](#)
- [Konfigurasi perutean untuk mengakses sistem file Multi-AZ dari luar VPC Anda](#)
- [Konfigurasi perutean untuk mengakses sistem file Multi-AZ dari lokal](#)
- [Volume pemasangan pada klien Linux](#)
- [Volume pemasangan pada klien Microsoft Windows](#)

- [Volume pemasangan pada klien macOS](#)
- [Penyediaan iSCSI untuk Linux](#)
- [Penyediaan iSCSI untuk Windows](#)
- [NVMePenyediaan/TCP untuk Linux](#)
- [Mengakses data Anda melalui jalur akses Amazon S3](#)
- [Mengakses data dari layanan lain AWS](#)

Klien yang didukung

FSx untuk sistem file ONTAP mendukung akses data dari berbagai contoh komputasi dan sistem operasi. Ini dilakukan dengan mendukung akses menggunakan protokol Network File System (NFS) (v3, v4.0, v4.1 dan v4.2), semua versi protokol Server Message Block (SMB) (termasuk 2.0, 3.0, dan 3.1.1), dan protokol Internet Small Computer Systems Interface (iSCSI).

Important

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 akan dilampirkan ke antarmuka network elastis sistem file.

Instans AWS komputasi berikut didukung untuk digunakan dengan FSx ONTAP:

- Instans Amazon Elastic Compute Cloud (Amazon EC2) yang menjalankan Linux dengan dukungan NFS atau SMB, Microsoft Windows, dan macOS. Untuk informasi lebih lanjut lihat [Volume pemasangan pada klien Linux](#), [Volume pemasangan pada klien Microsoft Windows](#), dan [Volume pemasangan pada klien macOS](#).
- Amazon Elastic Container Service (Amazon ECS) Container Docker di instans EC2 Amazon Windows dan Linux. Untuk informasi selengkapnya, lihat [Menggunakan Amazon Elastic Container Service dengan FSx untuk ONTAP](#).
- Amazon Elastic Kubernetes Service — Untuk mempelajari lebih lanjut, lihat [Amazon NetApp untuk driver ONTAP CSI di Panduan Pengguna FSx Amazon](#) EKS.
- Red Hat OpenShift Service on AWS (ROSA) — Untuk mempelajari lebih lanjut, lihat [Apa itu OpenShift Layanan Red Hat? AWS](#) dalam OpenShift Layanan Red Hat pada Panduan AWS Pengguna.

- WorkSpaces Contoh Amazon. Untuk informasi selengkapnya, lihat [Menggunakan Amazon WorkSpaces dengan FSx untuk ONTAP](#).
- Instans Amazon AppStream 2.0.
- AWS Lambda — Untuk informasi lebih lanjut, lihat posting AWS blog [Mengaktifkan akses SMB untuk beban kerja tanpa server](#) dengan Amazon FSx.
- Mesin virtual (VMs) berjalan di VMware Cloud di AWS lingkungan. Untuk informasi selengkapnya, lihat [Mengonfigurasi Amazon FSx untuk NetApp ONTAP sebagai Penyimpanan Eksternal](#) dan [VMware Cloud AWS dengan Amazon FSx untuk Panduan Penerapan NetApp ONTAP](#).

Setelah dipasang, FSx untuk sistem file ONTAP muncul sebagai direktori lokal atau huruf drive melalui NFS dan SMB, menyediakan penyimpanan file jaringan bersama yang dikelola sepenuhnya yang dapat diakses secara bersamaan oleh hingga ribuan klien. iSCSI LUNS dapat diakses sebagai perangkat blok saat dipasang melalui iSCSI.

Menggunakan protokol penyimpanan blok

Amazon FSx untuk NetApp ONTAP mendukung Internet Small Computer Systems Interface (iSCSI) dan Non-Volatile Memory Express NVMe () melalui TCP NVMe/TCP) block storage protocols. In Storage Area Network (SAN) environments, storage systems are targets that have storage target devices. For iSCSI, the storage target devices are referred to as logical units (LUNs). For NVMe/TCP, perangkat target penyimpanan disebut sebagai ruang nama.

Anda menggunakan antarmuka logis iSCSI (LIF) SVM untuk terhubung ke keduanya NVMe dan penyimpanan blok iSCSI.

Anda mengonfigurasi penyimpanan dengan membuat LUNs untuk iSCSI dan dengan membuat ruang nama untuk NVMe LUNs dan ruang nama kemudian diakses oleh host menggunakan protokol iSCSI atau TCP.

Untuk informasi selengkapnya tentang mengonfigurasi iSCSI NVMe/TCP dan memblokir penyimpanan, lihat:

- [Penyediaan iSCSI untuk Linux](#)
- [Penyediaan iSCSI untuk Windows](#)
- [NVMePenyediaan/TCP untuk Linux](#)

Mengakses data dari dalam AWS Cloud

Setiap sistem FSx file Amazon dikaitkan dengan Virtual Private Cloud (VPC). Anda dapat mengakses sistem file ONTAP Anda FSx dari mana saja di VPC sistem file, terlepas dari Availability Zone. Anda juga dapat mengakses sistem file Anda dari VPCs yang lain yang dapat berada di AWS akun yang berbeda atau Wilayah AWS. Selain persyaratan yang dijelaskan di bagian berikut FSx untuk mengakses sumber daya ONTAP, 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, lihat [Grup keamanan Amazon VPC](#).

Mengakses data dari dalam VPC yang sama

Saat Anda membuat Amazon FSx untuk sistem file NetApp ONTAP, Anda memilih Amazon VPC di mana ia berada. Semua SVMs dan volume yang terkait dengan Amazon FSx untuk sistem file NetApp ONTAP juga terletak di VPC yang sama. Saat memasang volume, jika sistem file dan klien yang memasang volume terletak di VPC yang sama dan Akun AWS, Anda dapat menggunakan nama DNS SVM dan sambungan volume atau berbagi SMB, tergantung pada klien.

Anda dapat mencapai kinerja optimal jika klien dan volume berada di Availability Zone yang sama dengan subnet sistem file, atau subnet pilihan untuk sistem file multi-AZ. Untuk mengidentifikasi subnet sistem file atau subnet pilihan, di FSx konsol Amazon, pilih Sistem file, lalu pilih sistem file ONTAP yang volumenya Anda pasang, dan subnet atau subnet pilihan (Multi-AZ) ditampilkan di Subnet atau Preferred subnet panel.

Mengakses data dari luar VPC penyebaran

Bagian ini menjelaskan cara mengakses titik akhir sistem file ONTAP dari AWS lokasi di luar VPC penyebaran sistem file. FSx

Mengakses titik akhir manajemen NFS, SMB, dan ONTAP pada sistem file multi-AZ

Endpoint manajemen NFS, SMB, dan ONTAP di FSx Amazon NetApp untuk sistem file Multi-AZ ONTAP menggunakan alamat protokol internet (IP) mengambang sehingga klien yang terhubung dengan mulus bertransisi antara server file pilihan dan siaga selama peristiwa failover. Untuk informasi selengkapnya tentang failover, lihat [Proses failover FSx untuk ONTAP](#).

Alamat IP mengambang ini dibuat dalam tabel rute VPC yang Anda kaitkan dengan sistem file Anda, dan berada dalam sistem file EndpointIPv4AddressRange atau EndpointIPv6AddressRange

yang Anda tentukan selama pembuatan. Rentang alamat IP endpoint menggunakan rentang alamat berikut, tergantung pada bagaimana sistem file dibuat:

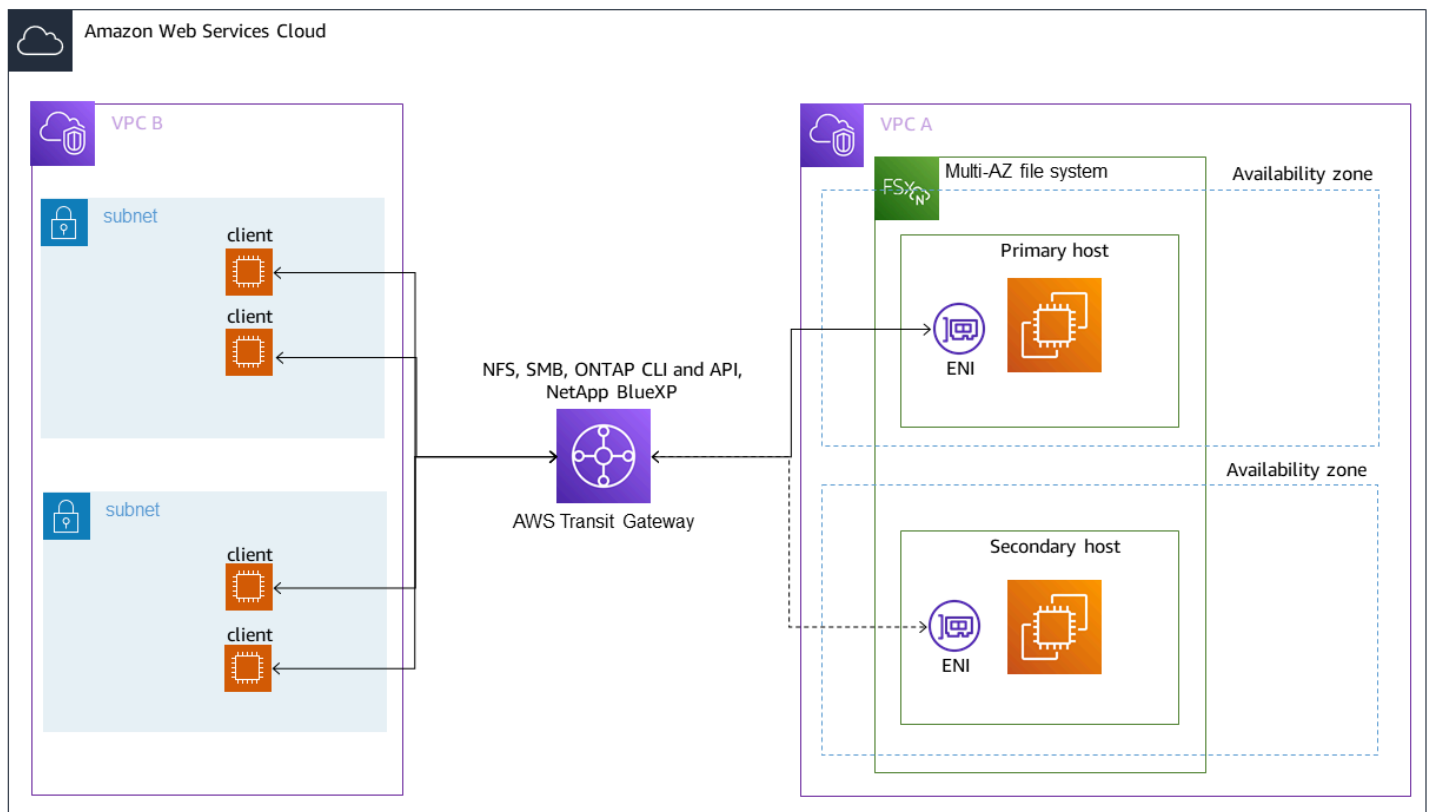
- Sistem file dual-stack multi-AZ yang dibuat dengan konsol Amazon FSx atau Amazon FSx API secara default menggunakan rentang alamat IP /118 yang tersedia yang dipilih oleh Amazon FSx dari salah satu rentang CIDR VPC. Anda dapat memiliki alamat IP titik akhir yang tumpang tindih untuk sistem file yang digunakan dalam VPC/route tabel yang sama, selama mereka tidak tumpang tindih dengan subnet apa pun.
- Sistem file IPv4 multi-AZ saja yang dibuat menggunakan FSx konsol Amazon menggunakan 64 alamat IP terakhir dalam rentang CIDR utama VPC untuk rentang alamat IP titik akhir sistem file secara default.

Sistem file IPv4 multi-AZ saja yang dibuat menggunakan atau AWS CLI Amazon FSx API menggunakan rentang alamat IP dalam blok 198.19.0.0/16 alamat untuk rentang alamat IP titik akhir secara default.

- Untuk salah satu jenis jaringan, Anda juga dapat menentukan rentang alamat IP Anda sendiri saat Anda menggunakan opsi Buat Standar. Rentang alamat IP yang Anda pilih dapat berada di dalam atau di luar rentang alamat IP VPC, asalkan tidak tumpang tindih dengan subnet apa pun, dan selama itu belum digunakan oleh sistem file lain dengan VPC dan tabel rute yang sama. Untuk opsi ini, kami sarankan menggunakan rentang yang ada di dalam rentang alamat IP VPC.

Hanya [AWS Transit Gateway](#) mendukung routing ke alamat IP mengambang, yang juga dikenal sebagai transitive peering. VPC Peering, Direct Connect, dan Site-to-Site VPN tidak mendukung pengintip transitif. Oleh karena itu, Anda diharuskan menggunakan Transit Gateway untuk mengakses antarmuka ini dari jaringan yang berada di luar VPC sistem file Anda.

Diagram berikut menggambarkan penggunaan Transit Gateway untuk NFS, SMB, atau akses manajemen ke sistem file Multi-AZ yang berada di VPC yang berbeda dari klien yang mengaksesnya.



Note

Pastikan bahwa semua tabel rute yang Anda gunakan terkait dengan sistem file Multi-AZ Anda. Melakukannya membantu mencegah tidak tersedianya selama failover. Untuk informasi tentang mengaitkan tabel rute VPC Amazon Anda dengan sistem file Anda, lihat [Memperbarui sistem file](#)

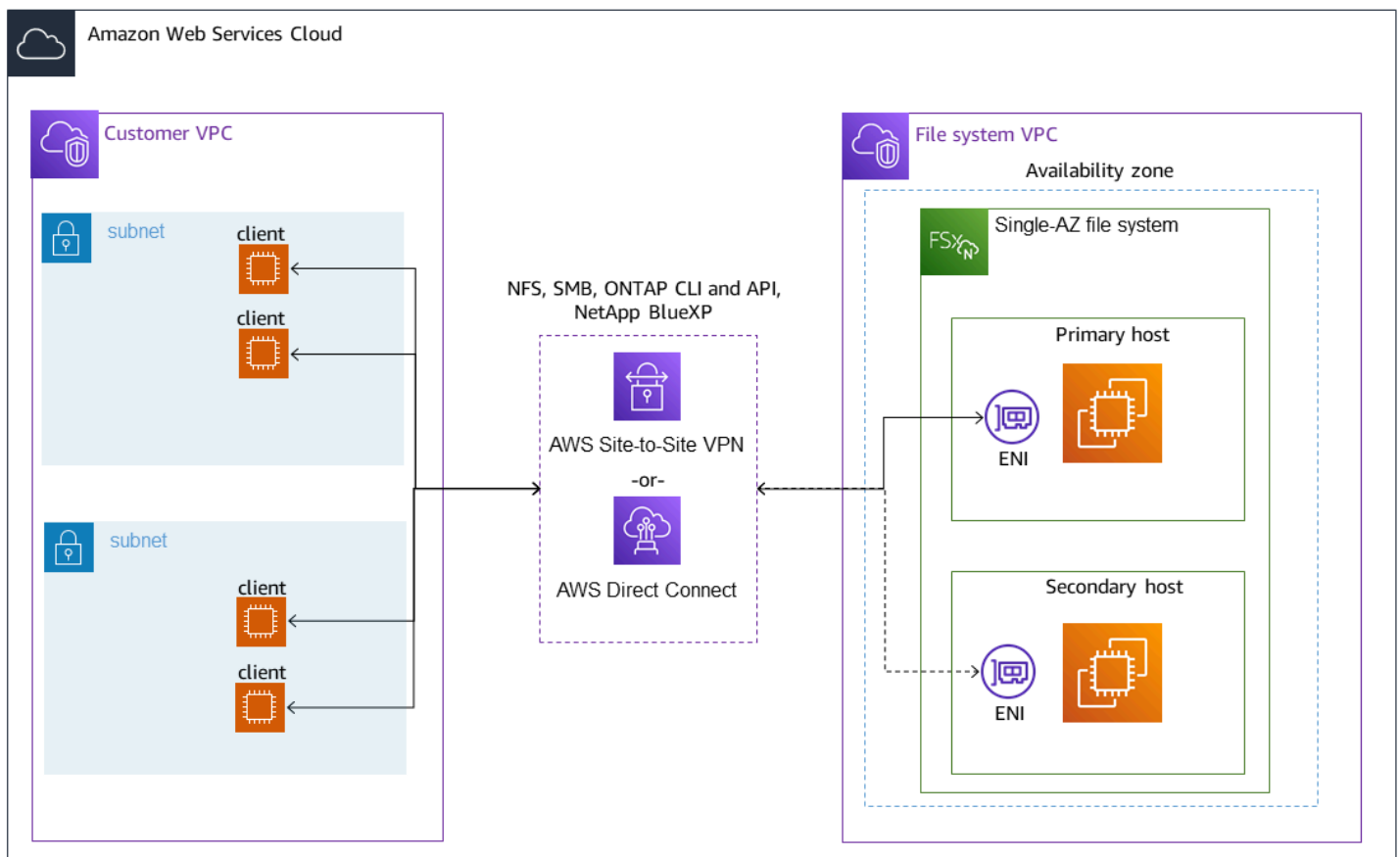
Untuk informasi tentang kapan Anda perlu menggunakan Transit Gateway untuk mengakses sistem file ONTAP Anda FSx, lihat [Kapan Transit Gateway diperlukan?](#)

Amazon FSx mengelola tabel rute VPC untuk sistem file multi-AZ menggunakan otentikasi berbasis tag. Tabel rute ini ditandai dengan **Key: AmazonFSx; Value: ManagedByAmazonFSx**. Saat membuat atau memperbarui FSx untuk sistem file ONTAP Multi-AZ menggunakan CloudFormation kami sarankan Anda menambahkan **Key: AmazonFSx; Value: ManagedByAmazonFSx** tag secara manual.

Mengakses NFS, SMB, atau ONTAP CLI dan API untuk sistem file single-AZ

Titik akhir yang digunakan FSx untuk mengakses sistem file ONTAP Single-AZ melalui NFS atau SMB, dan untuk mengelola sistem file menggunakan ONTAP CLI atau REST API, adalah alamat IP sekunder pada ENI dari server file aktif. Alamat IP sekunder berada dalam rentang CIDR VPC, sehingga klien dapat mengakses data dan port manajemen menggunakan VPC Peering, atau tanpa memerlukan. AWS Direct Connect Site-to-Site VPN AWS Transit Gateway

Diagram berikut menggambarkan penggunaan Site-to-Site VPN atau Direct Connect untuk NFS, SMB, atau akses manajemen ke sistem file Single-AZ yang berada di VPC yang berbeda dari klien yang mengaksesnya.



Kapan Transit Gateway diperlukan?

Apakah Transit Gateway diperlukan untuk sistem file Multi-AZ Anda tergantung pada metode yang Anda gunakan untuk mengakses data sistem file Anda. Sistem file single-AZ tidak memerlukan Transit Gateway. Tabel berikut menjelaskan kapan Anda perlu menggunakan AWS Transit Gateway untuk mengakses sistem file Multi-AZ.

Akses data	Membutuhkan Transit Gateway?
Mengakses FSx melalui NFS, SMB, atau NetApp ONTAP REST API, CLI, atau NetApp Console	Hanya jika: - Mengakses dari jaringan peered (lokal, misalnya), dan - Anda tidak mengakses FSx melalui instance Cache File Global NetApp FlexCache atau Global
Mengakses data melalui iSCSI	Tidak
Mengakses data melalui NVMe	Tidak
Bergabung dengan SVM ke Active Directory	Tidak
SnapMirror	Tidak
FlexCache Caching	Tidak
Cache File Global	Tidak

Mengakses NVMe, iSCSI, dan titik akhir antar-cluster di luar VPC penerapan

Anda dapat menggunakan VPC Peering atau AWS Transit Gateway untuk mengakses sistem file Anda, NVMe iSCSI, dan titik akhir antar-cluster dari luar VPC penyebaran sistem file. Anda dapat menggunakan VPC Peering untuk merutekan, NVMe iSCSI, dan lalu lintas antar-cluster di antaranya. VPCs Koneksi peering VPC adalah koneksi jaringan antara dua VPCs, dan digunakan untuk merutekan lalu lintas di antara mereka menggunakan pribadi IPv4 atau alamat. IPv6 Anda dapat menggunakan VPC peering untuk terhubung VPCs dalam yang sama Wilayah AWS atau di antara yang berbeda. Wilayah AWS Untuk informasi lebih lanjut tentang peering VPC, lihat [Apa itu VPC peering?](#) di Panduan Peering VPC Amazon.

Mengakses data dari lokal

Anda dapat mengakses sistem file ONTAP Anda FSx dari lokal menggunakan [Site-to-Site VPN](#) dan [Direct Connect](#); pedoman kasus penggunaan yang lebih spesifik tersedia di bagian berikut. [Selain persyaratan apa pun yang tercantum di bawah ini untuk mengakses sumber daya ONTAP yang](#)

[berbeda FSx dari lokal, Anda juga perlu memastikan bahwa grup keamanan VPC sistem file Anda memungkinkan data mengalir antara sistem file dan klien; untuk daftar port yang diperlukan, lihat \[grup keamanan VPC Amazon\]\(#\).](#)

Mengakses titik akhir NFS, SMB, dan ONTAP CLI dan REST API dari lokal

Bagian ini menjelaskan cara mengakses port manajemen NFS, SMB, dan ONTAP FSx untuk sistem file ONTAP dari jaringan lokal.

Mengakses sistem file Multi-AZ dari lokal

Amazon FSx mengharuskan Anda menggunakan AWS Transit Gateway atau mengonfigurasi Cache File NetApp Global jarak jauh atau NetApp FlexCache mengakses sistem file multi-AZ dari jaringan lokal. Untuk mendukung failover di seluruh zona ketersediaan untuk sistem file multi-AZ, Amazon FSx menggunakan alamat IP mengambang untuk antarmuka yang digunakan untuk titik akhir manajemen NFS, SMB, dan ONTAP.

Karena titik akhir NFS, SMB, dan manajemen menggunakan alamat IP mengambang, Anda harus menggunakan [AWS Transit Gateway](#) bersama dengan AWS Direct Connect atau Site-to-Site VPN untuk mengakses antarmuka ini dari jaringan lokal. Alamat IP mengambang yang digunakan untuk antarmuka ini berada di dalam `EndpointIPv4AddressRange` atau yang `EndpointIPv6AddressRange` Anda tentukan saat membuat sistem file Multi-AZ Anda. Rentang alamat IP endpoint menggunakan rentang alamat berikut, tergantung pada bagaimana sistem file dibuat:

- Sistem file dual-stack multi-AZ yang dibuat dengan konsol Amazon FSx atau Amazon FSx API secara default menggunakan rentang alamat IP /118 yang tersedia yang dipilih oleh Amazon FSx dari salah satu rentang CIDR VPC. Anda dapat memiliki alamat IP titik akhir yang tumpang tindih untuk sistem file yang digunakan dalam VPC/route tabel yang sama, selama mereka tidak tumpang tindih dengan subnet apa pun.
- Sistem file IPv4 multi-AZ saja yang dibuat menggunakan FSx konsol Amazon menggunakan 64 alamat IP terakhir dalam rentang CIDR utama VPC untuk rentang alamat IP titik akhir sistem file secara default.

Sistem file IPv4 multi-AZ saja yang dibuat menggunakan atau AWS CLI Amazon FSx API menggunakan rentang alamat IP dalam blok `198.19.0.0/16` alamat untuk rentang alamat IP titik akhir secara default.

- Untuk salah satu jenis jaringan, Anda juga dapat menentukan rentang alamat IP Anda sendiri saat Anda menggunakan opsi Buat Standar. Rentang alamat IP yang Anda pilih dapat berada di dalam

atau di luar rentang alamat IP VPC, asalkan tidak tumpang tindih dengan subnet apa pun, dan selama itu belum digunakan oleh sistem file lain dengan VPC dan tabel rute yang sama. Untuk opsi ini, kami sarankan menggunakan rentang yang ada di dalam rentang alamat IP VPC.

Alamat IP mengambang digunakan untuk memungkinkan transisi mulus klien Anda ke sistem file siaga jika failover diperlukan. Untuk informasi selengkapnya, lihat [Proses failover FSx untuk ONTAP](#).

Important

Untuk mengakses sistem file Multi-AZ menggunakan Transit Gateway, setiap lampiran Transit Gateway harus dibuat dalam subnet yang tabel rutanya dikaitkan dengan sistem file Anda.

Untuk informasi selengkapnya, lihat [Konfigurasi perutean untuk mengakses sistem file Multi-AZ dari lokal](#).

Mengakses sistem file Single-AZ dari lokal

Persyaratan yang digunakan AWS Transit Gateway untuk mengakses data dari jaringan lokal tidak ada untuk sistem file Single-AZ. Sistem file single-AZ digunakan dalam satu subnet, dan alamat IP mengambang tidak diperlukan untuk menyediakan failover antar node. Sebaliknya, alamat IP yang Anda akses pada sistem file Single-AZ diimplementasikan sebagai alamat IP sekunder dalam rentang CIDR VPC sistem file, memungkinkan Anda untuk mengakses data Anda dari jaringan lain tanpa memerlukan AWS Transit Gateway.

Mengakses titik akhir antar-cluster dari lokal

FSx untuk titik akhir antar-cluster ONTAP didedikasikan untuk lalu lintas replikasi antara sistem file NetApp ONTAP, termasuk antara penerapan lokal dan untuk ONTAP. NetApp FSx Lalu lintas replikasi mencakup SnapMirror, FlexCache, dan FlexClone hubungan antara mesin virtual penyimpanan (SVMs) dan volume di berbagai sistem file, dan Cache File NetApp Global. Endpoint antar-cluster juga digunakan untuk lalu lintas Active Directory.

Karena titik akhir antar-kluster sistem file menggunakan alamat IP yang berada dalam rentang CIDR dari VPC yang Anda berikan saat Anda membuat FSx untuk sistem file ONTAP, Anda tidak diharuskan menggunakan Gateway Transit untuk merutekan lalu lintas antar kluster antara lokal dan AWS Cloud. Namun, klien lokal tetap harus menggunakan Site-to-Site VPN atau Direct Connect membuat koneksi aman ke VPC Anda.

Untuk informasi selengkapnya, lihat [Konfigurasi perutean untuk mengakses sistem file Multi-AZ dari lokal](#).

Konfigurasi perutean untuk mengakses sistem file Multi-AZ dari luar VPC Anda

Jika Anda memiliki sistem file Multi-AZ dengan `EndpointIPv4AddressRange` atau `EndpointIPv6AddressRange` yang berada di luar rentang alamat IP VPC Anda, Anda perlu mengatur perutean tambahan AWS Transit Gateway untuk mengakses sistem file Anda dari jaringan peered atau lokal.

Important

Untuk mengakses sistem file Multi-AZ menggunakan Transit Gateway, setiap lampiran Transit Gateway harus dibuat dalam subnet yang tabel rutanya dikaitkan dengan sistem file Anda.

Note

Tidak diperlukan konfigurasi Transit Gateway tambahan untuk sistem file Single-AZ atau sistem file Multi-AZ dengan rentang alamat IP titik akhir yang berada dalam rentang alamat IP VPC Anda.

Untuk mengkonfigurasi routing menggunakan AWS Transit Gateway

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Pilih sistem FSx file ONTAP untuk yang Anda konfigurasi akses dari jaringan peered.
3. Di Jaringan & keamanan salin rentang alamat IP titik akhir.
4. Tambahkan rute ke Transit Gateway yang merutekan lalu lintas yang ditujukan untuk rentang alamat IP ini ke VPC sistem file Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan gateway transit di Gateway](#) Transit VPC Amazon.
5. Konfirmasikan bahwa Anda FSx dapat mengakses sistem file ONTAP Anda dari jaringan peered.

Untuk menambahkan tabel rute ke sistem file Anda, lihat [Memperbarui sistem file](#).

 Note

Catatan DNS untuk manajemen, NFS, dan titik akhir SMB hanya dapat diselesaikan dari dalam VPC yang sama dengan sistem file. Untuk memasang volume atau terhubung ke port manajemen dari jaringan lain, Anda perlu menggunakan alamat IP titik akhir. Alamat IP ini tidak berubah seiring waktu.

Konfigurasi perutean untuk mengakses sistem file Multi-AZ dari lokal

Mengkonfigurasi AWS Transit Gateway akses ke sistem file Multi-AZ dari lokal

Jika Anda memiliki sistem file Multi-AZ dengan `EndpointIPv4AddressRange` atau `EndpointIPv6AddressRange` yang berada di luar jangkauan CIDR VPC Anda, Anda perlu mengatur perutean tambahan AWS Transit Gateway untuk mengakses sistem file Anda dari jaringan peered atau lokal.

 Note

Tidak diperlukan konfigurasi Transit Gateway tambahan untuk sistem file Single-AZ atau sistem file Multi-AZ dengan rentang alamat IP titik akhir yang berada dalam rentang alamat IP VPC Anda.

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Pilih sistem FSx file ONTAP untuk yang Anda konfigurasi akses dari jaringan peered.
3. Di Jaringan & keamanan salin Endpoint IPv4 atau rentang IPv6 alamat.
4. Tambahkan rute ke Transit Gateway yang merutekan lalu lintas yang ditujukan untuk rentang alamat IP ini ke VPC sistem file Anda. Untuk informasi selengkapnya, lihat [Bekerja dengan gateway transit di Panduan Pengguna Gateway Transit VPC Amazon](#).
5. Konfirmasikan bahwa Anda FSx dapat mengakses sistem file ONTAP Anda dari jaringan peered.

 Important

Untuk mengakses sistem file Multi-AZ menggunakan Transit Gateway, setiap lampiran Transit Gateway harus dibuat dalam subnet yang tabel rutenya dikaitkan dengan sistem file Anda. Jika Anda memiliki subnet lampiran Transit Gateway yang terpisah, Anda juga harus mengaitkan tabel rute untuk subnet tersebut dengan Amazon FSx sehingga diperbarui dengan alamat titik FSx akhir Amazon.

Untuk menambahkan tabel rute ke sistem file Anda, lihat [Memperbarui sistem file](#).

Volume pemasangan pada klien Linux

Kami merekomendasikan bahwa volume yang ingin Anda pasang dengan klien Linux memiliki pengaturan gaya keamanan UNIX `atoumixed`. Untuk informasi selengkapnya, lihat [Mengelola FSx volume ONTAP](#).

 Note

Secara default, FSx untuk pemasangan ONTAP NFS adalah `mount. hard`. Untuk memastikan failover yang lancar jika terjadi, kami sarankan Anda menggunakan opsi `hard` pemasangan default.

Untuk memasang volume ONTAP pada klien Linux

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Buat atau pilih EC2 instans Amazon yang menjalankan Amazon Linux 2 yang berada di VPC yang sama dengan sistem file.

Untuk informasi selengkapnya tentang meluncurkan instance EC2 Linux, lihat [Langkah 1: Meluncurkan instance](#) di Panduan EC2 Pengguna Amazon.

3. Connect ke instans Amazon EC2 Linux Anda. Untuk informasi selengkapnya, lihat [Connect ke instans Linux Anda](#) di Panduan EC2 Pengguna Amazon.
4. Buka terminal pada EC2 instance Anda menggunakan shell aman (SSH), dan masuk dengan kredensi yang sesuai.
5. Buat direktori pada EC2 instance untuk memasang volume SVM sebagai berikut:


```
sudo mkdir /fsx
```

6. Pasang volume ke direktori yang baru saja Anda buat menggunakan perintah berikut:

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

Contoh berikut menggunakan nilai sampel.

```
sudo mount -t nfs svm-01234567890abcdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /fsx
```

Anda juga dapat menggunakan alamat IP SVM alih-alih nama DNS-nya. Sebaiknya gunakan nama DNS untuk memasang klien ke sistem file generasi kedua karena membantu memastikan bahwa klien Anda seimbang di seluruh pasangan ketersediaan tinggi (HA) sistem file Anda.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

Note

Untuk sistem file generasi kedua, protokol paralel NFS (PNFS) diaktifkan secara default dan digunakan secara default untuk setiap klien yang memasang volume dengan NFS v4.1 atau lebih besar.

Menggunakan /etc/fstab untuk me-mount secara otomatis saat reboot instance

Untuk mengaktifkan ulang volume ONTAP Anda FSx secara otomatis saat instans Amazon EC2 Linux reboot, gunakan file tersebut. /etc/fstab File /etc/fstab berisi informasi tentang sistem file. Perintah `mount -a`, yang berjalan selama start-up instance, memasang sistem file yang terdaftar di /etc/fstab

Note

FSx untuk sistem file ONTAP tidak mendukung pemasangan otomatis menggunakan instance /etc/fstab Amazon EC2 Mac.

Note

Sebelum Anda dapat memperbarui `/etc/fstab` file EC2 instance Anda, pastikan bahwa Anda sudah membuat FSx untuk sistem file ONTAP. Untuk informasi selengkapnya, lihat [Membuat sistem file](#).

Untuk memperbarui berkas `/etc/fstab` pada instance Anda EC2

1. Connect ke EC2 instans Anda:

- Untuk menyambung ke instans Anda dari komputer yang menjalankan macOS atau Linux, tentukan file.pem untuk perintah SSH Anda. Untuk melakukan ini, gunakan `-i` opsi dan jalur ke kunci pribadi Anda.
- Untuk terhubung ke instans Anda dari komputer yang menjalankan Windows, Anda dapat menggunakan MindTerm atau Putty. Untuk menggunakan PuTTY, instal dan konversi file.pem ke file.ppk.

Untuk informasi selengkapnya, lihat topik berikut di Panduan EC2 Pengguna Amazon:

- [Menghubungkan ke instans Linux Anda menggunakan SSH](#)
- [Menghubungkan ke instans Linux Anda dari Windows menggunakan PuTTY](#)

2. Buat direktori lokal yang akan digunakan untuk me-mount volume SVM.

```
sudo mkdir /fsx
```

3. Buka `/etc/fstab` file di editor pilihan Anda.

4. Tambahkan baris berikut ke file `/etc/fstab`. Masukkan karakter tab di antara setiap parameter. Ini akan muncul sebagai satu baris tanpa jeda baris.

```
svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
```

Anda juga dapat menggunakan alamat IP SVM volume. Tiga parameter terakhir menunjukkan opsi NFS (yang kami atur ke default), pembuangan sistem file dan pemeriksaan sistem file (ini biasanya tidak digunakan sehingga kami mengaturnya ke 0).

5. Simpan perubahan pada file.

6. Sekarang pasang file share menggunakan perintah berikut. Lain kali sistem dimulai, folder akan dipasang secara otomatis.

```
sudo mount /fsx
sudo mount svm-dns-name:volume-junction-path
```

EC2 Instance Anda sekarang dikonfigurasi untuk me-mount volume ONTAP setiap kali dimulai ulang.

Volume pemasangan pada klien Microsoft Windows

Bagian ini menjelaskan cara mengakses data dalam sistem file ONTAP Anda FSx dengan klien yang menjalankan sistem operasi Microsoft Windows. Tinjau persyaratan berikut, terlepas dari jenis klien yang Anda gunakan.

Prosedur ini mengasumsikan bahwa klien dan sistem file terletak di Akun AWS VPC yang sama dan. Jika klien berada di lokasi atau di VPC yang berbeda,, atau Akun AWS Wilayah AWS, prosedur ini juga mengasumsikan bahwa Anda telah menyiapkan AWS Transit Gateway atau koneksi jaringan khusus menggunakan AWS Direct Connect atau menggunakan terowongan pribadi yang aman. AWS Virtual Private Network Untuk informasi selengkapnya, lihat [Mengakses data dari luar VPC penyebaran](#).

Kami menyarankan Anda melampirkan volume ke klien Windows Anda menggunakan protokol SMB.

Prasyarat

Untuk mengakses volume penyimpanan ONTAP menggunakan klien Microsoft Windows, Anda harus memenuhi prasyarat berikut:

- SVM volume yang Anda lampirkan harus digabungkan ke Active Directory organisasi Anda, atau Anda harus menggunakan workgroup. Untuk informasi selengkapnya tentang menggabungkan SVM Anda ke Active Directory, lihat [Mengelola FSx mesin virtual penyimpanan ONTAP](#). Untuk informasi selengkapnya tentang penggunaan kelompok kerja, lihat [Menyiapkan server SMB di workgroup](#).
- Volume yang Anda lampirkan harus memiliki pengaturan gaya keamanan. NTFS Untuk informasi selengkapnya, lihat [Gaya keamanan volume](#).

Untuk me-mount volume pada klien Windows menggunakan SMB dan Active Directory

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Buat atau pilih EC2 instans Amazon yang menjalankan Microsoft Windows yang berada di VPC yang sama dengan sistem file, dan bergabung ke Microsoft Active Directory yang sama dengan SVM volume.

Untuk informasi selengkapnya tentang meluncurkan instance, lihat [Langkah 1: Meluncurkan instance](#) di Panduan EC2 Pengguna Amazon.

Untuk informasi selengkapnya tentang menggabungkan SVM ke Active Directory, lihat [Mengelola FSx mesin virtual penyimpanan ONTAP](#).

3. Connect ke instans Amazon EC2 Windows Anda. Untuk informasi selengkapnya, lihat [Menyambungkan ke instans Windows Anda](#) di Panduan EC2 Pengguna Amazon.
4. Buka prompt perintah.
5. Jalankan perintah berikut. Ganti yang berikut ini:
 - Ganti Z : dengan huruf drive yang tersedia.
 - Ganti DNS_NAME dengan nama DNS atau alamat IP titik akhir SMB untuk SVM volume.
 - Ganti SHARE_NAME dengan nama saham SMB. C\$ adalah pangsa SMB default di root namespace SVM, tetapi Anda tidak boleh memasangnya karena itu memperlihatkan penyimpanan ke volume root dan dapat menyebabkan gangguan keamanan dan layanan. Anda harus memberikan nama berbagi SMB untuk dipasang, bukan. C\$ Untuk informasi selengkapnya tentang membuat saham SMB, lihat [Mengelola saham SMB](#).

```
net use Z: \\DNS_NAME\SHARE_NAME
```

Contoh berikut menggunakan nilai sampel.

```
net use Z: \\corp.example.com\group_share
```

Anda juga dapat menggunakan alamat IP SVM alih-alih nama DNS-nya. Sebaiknya gunakan nama DNS untuk memasang klien ke sistem file generasi kedua karena membantu memastikan bahwa klien Anda seimbang di seluruh pasangan ketersediaan tinggi (HA) sistem file Anda.

```
net use Z: \\198.51.100.5\group_share
```

Volume pemasangan pada klien macOS

Bagian ini menjelaskan cara mengakses data dalam sistem file ONTAP Anda FSx dengan klien yang menjalankan sistem operasi macOS. Tinjau persyaratan berikut, terlepas dari jenis klien yang Anda gunakan.

Prosedur ini mengasumsikan bahwa klien dan sistem file terletak di Akun AWS VPC yang sama dan. Jika klien berada di lokasi, atau di VPC yang berbeda, atau Wilayah AWS, Anda telah menyiapkan Akun AWS atau koneksi jaringan khusus menggunakan AWS Transit Gateway AWS Direct Connect atau menggunakan terowongan pribadi yang aman. AWS Virtual Private Network Untuk informasi selengkapnya, lihat [Mengakses data dari luar VPC penyebaran](#).

Kami menyarankan Anda melampirkan volume ke klien Mac Anda menggunakan protokol SMB.

Untuk memasang volume ONTAP pada klien macOS menggunakan SMB

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Buat atau pilih instans Amazon EC2 Mac yang menjalankan macOS yang ada di VPC yang sama dengan sistem file.

Untuk informasi selengkapnya tentang meluncurkan instance, lihat [Langkah 1: Meluncurkan instance](#) di Panduan EC2 Pengguna Amazon.

3. Connect ke instans Amazon EC2 Mac Anda. Untuk informasi selengkapnya, lihat [Connect ke instans Linux Anda](#) di Panduan EC2 Pengguna Amazon.
4. Buka terminal pada EC2 instance Anda menggunakan shell aman (SSH), dan masuk dengan kredensi yang sesuai.
5. Buat direktori pada EC2 instance untuk memasang volume sebagai berikut:

```
sudo mkdir /fsx
```

6. Pasang volume menggunakan perintah berikut.

```
sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
```

Contoh berikut menggunakan nilai sampel.

```
sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-east-1.amazonaws.com:/C$ /fsx
```

Anda juga dapat menggunakan alamat IP SVM alih-alih nama DNS-nya. Sebaiknya gunakan nama DNS untuk memasang klien ke sistem file generasi kedua karena membantu memastikan bahwa klien Anda seimbang di seluruh pasangan ketersediaan tinggi (HA) sistem file Anda.

```
sudo mount -t smbfs 198.51.100.10:/C$ /fsx
```

C\$ adalah berbagi SMB default yang dapat Anda pasang untuk melihat root namespace SVM. Jika Anda telah membuat pembagian Blok Pesan Server (SMB) apa pun di SVM Anda, berikan nama berbagi SMB sebagai gantinya. C\$ Untuk informasi selengkapnya tentang membuat saham SMB, lihat [Mengelola saham SMB](#).

Untuk memasang volume ONTAP pada klien macOS menggunakan NFS

1. Buka EC2 konsol Amazon di <https://console.aws.amazon.com/ec2/>.
2. Buat atau pilih EC2 instans Amazon yang menjalankan Amazon Linux 2 yang berada di VPC yang sama dengan sistem file.

Untuk informasi selengkapnya tentang meluncurkan instance EC2 Linux, lihat [Langkah 1: Meluncurkan instance](#) di Panduan EC2 Pengguna Amazon.

3. Connect ke instans Amazon EC2 Linux Anda. Untuk informasi selengkapnya, lihat [Connect ke instans Linux Anda](#) di Panduan EC2 Pengguna Amazon.
4. Pasang volume ONTAP Anda FSx pada EC2 instance Linux dengan menggunakan skrip data pengguna selama peluncuran instance, atau dengan menjalankan perintah berikut:

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-point
```

Contoh berikut menggunakan nilai sampel.

```
sudo mount -t nfs -o nfsvers=4.1  
svm-01234567890abcdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /  
fsxontap
```

Anda juga dapat menggunakan alamat IP SVM alih-alih nama DNS-nya. Sebaiknya gunakan nama DNS untuk memasang klien ke sistem file generasi kedua karena membantu memastikan bahwa klien Anda seimbang di seluruh pasangan HA sistem file Anda.

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. Pasang volume ke direktori yang baru saja Anda buat menggunakan perintah berikut.

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

Contoh berikut menggunakan nilai sampel.

```
sudo mount -t nfs svm-01234567890abcdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /fsx
```

Anda juga dapat menggunakan alamat IP SVM alih-alih nama DNS-nya. Sebaiknya gunakan nama DNS untuk memasang klien ke sistem file generasi kedua karena membantu memastikan bahwa klien Anda seimbang di seluruh pasangan ketersediaan tinggi (HA) sistem file Anda.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

Penyediaan iSCSI untuk Linux

FSx untuk ONTAP mendukung protokol iSCSI. Anda perlu menyediakan iSCSI pada kedua klien Linux dan sistem file Anda untuk menggunakan protokol iSCSI untuk mengangkut data antara klien dan sistem file Anda. Protokol iSCSI tersedia di semua sistem file yang memiliki 6 atau [lebih sedikit pasangan ketersediaan tinggi](#) (HA).

Ada tiga langkah utama untuk memproses konfigurasi iSCSI di FSx NetApp Amazon Anda untuk ONTAP, yang tercakup dalam prosedur berikut:

1. Instal dan konfigurasi klien iSCSI di host Linux.
2. Konfigurasi iSCSI pada SVM sistem file.
 - Buat grup inisiator iSCSI.
 - Petakan grup inisiator ke LUN.
3. Pasang iSCSI LUN pada klien Linux.

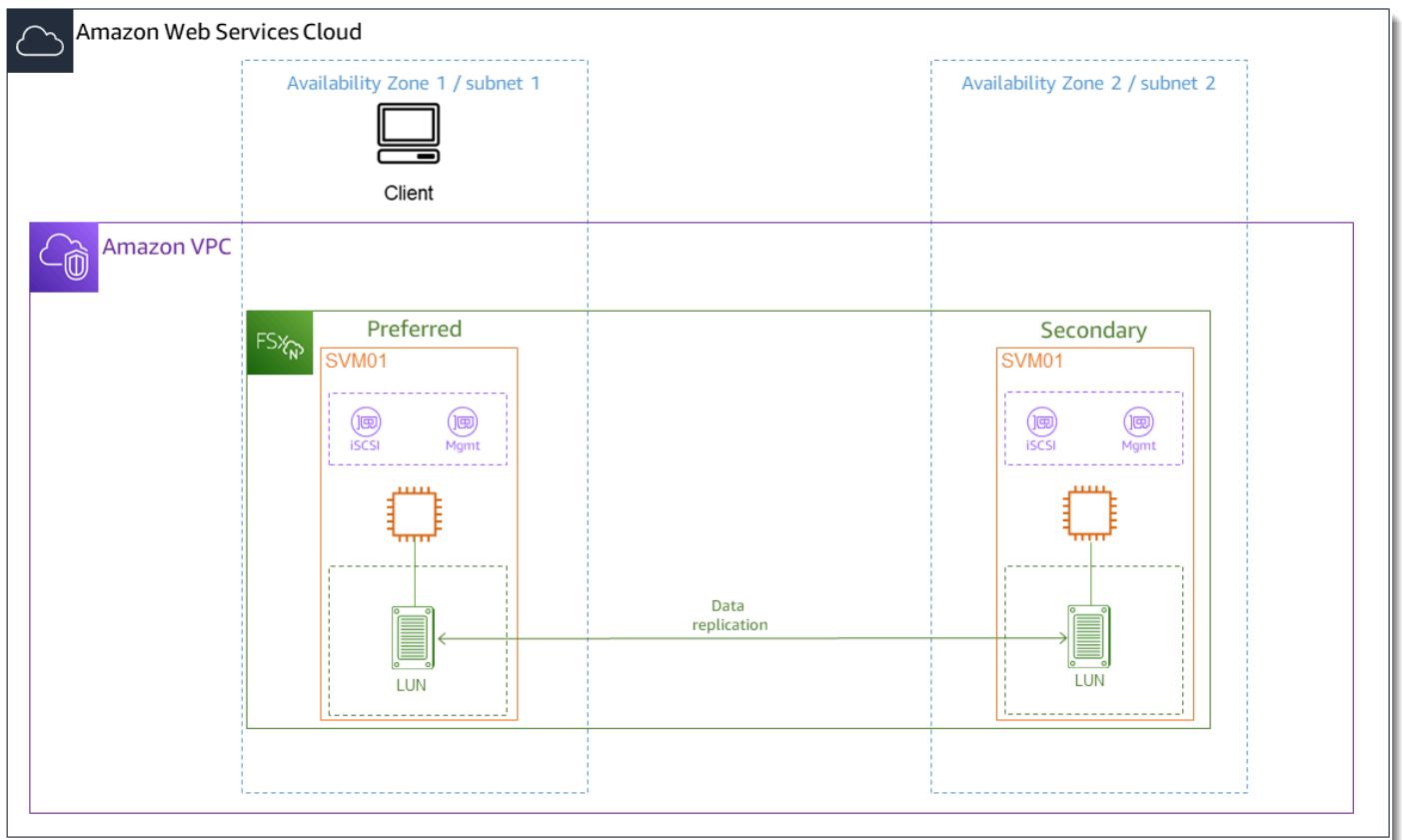
Sebelum Anda mulai

Sebelum Anda memulai proses mengkonfigurasi sistem file Anda untuk iSCSI, Anda harus menyelesaikan item berikut.

- Buat sistem file FSx untuk ONTAP. Untuk informasi selengkapnya, lihat [Membuat sistem file](#).
- Buat iSCSI LUN pada sistem file. Untuk informasi selengkapnya, lihat [Membuat iSCSI LUN](#).
- Buat EC2 instance yang menjalankan Amazon Linux 2 Amazon Machine Image (AMI) di VPC yang sama dengan sistem file. Ini adalah host Linux tempat Anda akan mengkonfigurasi iSCSI dan mengakses data file Anda.

Di luar cakupan prosedur ini, jika host berada di VPC lain, Anda dapat menggunakan peering VPC atau AWS Transit Gateway untuk memberikan VPCs akses lain ke titik akhir iSCSI volume. Untuk informasi selengkapnya, lihat [Mengakses data dari luar VPC penyebaran](#).

- Konfigurasi grup keamanan VPC host Linux untuk memungkinkan lalu lintas masuk dan keluar seperti yang dijelaskan dalam [Kontrol Akses Sistem File dengan Amazon VPC](#)
- Dapatkan kredensi untuk ONTAP pengguna dengan fsxadmin hak istimewa yang akan Anda gunakan untuk mengakses ONTAP CLI. Untuk informasi selengkapnya, lihat [ONTAPperan dan pengguna](#).
- Host Linux yang akan Anda konfigurasi untuk iSCSI dan gunakan untuk mengakses FSx sistem file for ONTAP terletak di VPC yang sama dan. Akun AWS
- Sebaiknya EC2 instans berada di zona ketersediaan yang sama dengan subnet pilihan sistem file Anda, seperti yang ditunjukkan pada grafik berikut.



Jika EC2 instans Anda menjalankan AMI Linux yang berbeda dari Amazon Linux 2, beberapa utilitas yang digunakan dalam prosedur dan contoh ini mungkin sudah diinstal, dan Anda mungkin menggunakan perintah yang berbeda untuk menginstal paket yang diperlukan. Selain menginstal paket, perintah yang digunakan di bagian ini berlaku untuk EC2 Linux lainnya AMIs.

Topik

- [Instal dan konfigurasi iSCSI di host Linux](#)
- [Konfigurasi iSCSI pada sistem file untuk FSx ONTAP](#)
- [Pasang iSCSI LUN di klien Linux Anda](#)

Instal dan konfigurasi iSCSI di host Linux

Untuk menginstal klien iSCSI

1. Konfirmasikan `device-mapper-multipath` itu `iscsi-initiator-utils` dan diinstal pada perangkat Linux Anda. Connect ke instance Linux Anda menggunakan klien SSH. Untuk informasi selengkapnya, lihat [Connect ke instans Linux menggunakan SSH](#).

2. Instal multipath dan klien iSCSI menggunakan perintah berikut. Instalasi multipath diperlukan jika Anda ingin secara otomatis failover antara server file Anda.

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. Untuk memfasilitasi respons yang lebih cepat ketika secara otomatis gagal di antara server file saat menggunakan multipath, atur nilai batas waktu penggantian dalam `/etc/iscsi/iscsid.conf` file ke nilai 5 alih-alih menggunakan nilai default. 120

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. Mulai layanan iSCSI.

```
~$ sudo service iscsid start
```

Perhatikan bahwa tergantung pada versi Linux Anda, Anda mungkin harus menggunakan perintah ini sebagai gantinya:

```
~$ sudo systemctl start iscsid
```

5. Konfirmasikan bahwa layanan sedang berjalan menggunakan perintah berikut.

```
~$ sudo systemctl status iscsid.service
```

Sistem merespons dengan output berikut:

```
iscsid.service - Open-iSCSI
   Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor preset: disabled)
   Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
     Docs: man:iscsid(8)
           man:iscsiadm(8)
   Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
   CGroup: /system.slice/iscsid.service
           ##14659 /usr/sbin/iscsid
           ##14660 /usr/sbin/iscsid
```

Untuk mengkonfigurasi iSCSI pada klien Linux Anda

1. Untuk mengaktifkan klien Anda untuk secara otomatis failover antara server file Anda, Anda harus mengkonfigurasi multipath. Gunakan perintah berikut ini.

```
~$ sudo mpathconf --enable --with_multipathd y
```

2. Tentukan nama inisiator host Linux Anda menggunakan perintah berikut. Lokasi nama inisiator tergantung pada utilitas iSCSI Anda. Jika Anda menggunakan `iscsi-initiator-utils`, nama inisiator terletak di file `/etc/iscsi/initiatorname.iscsi`.

```
~$ sudo cat /etc/iscsi/initiatorname.iscsi
```

Sistem merespons dengan nama inisiator.

```
InitiatorName=iqn.1994-05.com.redhat:abcdef12345
```

Konfigurasikan iSCSI pada sistem file untuk FSx ONTAP

1. Hubungkan ke CLI NetApp ONTAP pada FSx sistem file for ONTAP tempat Anda membuat iSCSI LUN menggunakan perintah berikut. Untuk informasi selengkapnya, lihat [Menggunakan CLI NetApp ONTAP](#).

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. Buat grup inisiator (`igroup`) menggunakan perintah NetApp ONTAP CLI. [lun igroup create](#) Grup inisiator memetakan ke LUNs iSCSI dan mengontrol inisiator (klien) mana yang dapat diakses. LUNs Ganti `host_initiator_name` dengan nama inisiator dari host Linux Anda yang Anda ambil dalam prosedur sebelumnya.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -  
initiator host_initiator_name -protocol iscsi -ostype linux
```

Jika Anda ingin membuat LUNs dipetakan ke `igroup` ini tersedia untuk beberapa host, Anda dapat menentukan beberapa nama inisiator yang dipisahkan dengan koma. Untuk informasi selengkapnya, lihat [lun igroup create](#) di Pusat Dokumentasi NetApp ONTAP.

3. Konfirmasikan bahwa `igroup` ada menggunakan [lun igroup show](#) perintah:

```
::> lun igroup show
```

Sistem merespons dengan output berikut:

Vserver	Igroup	Protocol	OS Type	Initiators
<i>svm_name</i>	<i>igroup_name</i>	iscsi	linux	iqn.1994-05.com.redhat:abcdef12345

- Langkah ini mengasumsikan bahwa Anda telah membuat iSCSI LUN. Jika belum, lihat step-by-step instruksi [Membuat iSCSI LUN](#) untuk melakukannya.

Buat pemetaan dari LUN yang Anda buat ke igroup yang Anda buat, menggunakan [lun mapping create](#), menentukan atribut berikut:

- *svm_name*— Nama mesin virtual penyimpanan yang menyediakan target iSCSI. Tuan rumah menggunakan nilai ini untuk mencapai LUN.
- *vol_name*— Nama volume hosting LUN.
- *lun_name*— Nama yang Anda tetapkan ke LUN.
- *igroup_name*— Nama grup inisiator.
- *lun_id*— Bilangan bulat ID LUN khusus untuk pemetaan, bukan untuk LUN itu sendiri. Ini digunakan oleh inisiator di igroup sebagai Logical Unit Number menggunakan nilai ini untuk inisiator saat mengakses penyimpanan.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -  
igroup igroup_name -lun-id lun_id
```

- Gunakan [lun show -path](#) perintah untuk mengonfirmasi LUN dibuat, online, dan dipetakan.

```
::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
```

Sistem merespons dengan output berikut:

Vserver	Path	serial-hex	state	mapped
<i>svm_name</i>	/vol/ <i>vol_name</i> / <i>lun_name</i>	6c5742314e5d52766e796150	online	mapped

Simpan `serial_hex` nilainya (dalam contoh ini `6c5742314e5d52766e796150`), Anda akan menggunakannya di langkah selanjutnya untuk membuat nama ramah untuk perangkat blok.

- Gunakan `network interface show -vserver` perintah untuk mengambil alamat `iscsi_1` dan `iscsi_2` antarmuka untuk SVM di mana Anda telah membuat iSCSI LUN Anda.

```
::> network interface show -vserver svm_name
```

Sistem merespons dengan output berikut:

Logical Current Is	Status	Network	Current
Vserver Interface Port Home	Admin/Oper	Address/Mask	Node
-----	-----	-----	-----

<i>svm_name</i>			
iscsi_1	up/up	172.31.0.143/20	
FSxId0123456789abcdef8-01 e0e	true		
iscsi_2	up/up	172.31.21.81/20	
FSxId0123456789abcdef8-02 e0e	true		
nfs_smb_management_1			
	up/up	198.19.250.177/20	
FSxId0123456789abcdef8-01 e0e	true		
3 entries were displayed.			

Dalam contoh ini, alamat IP `iscsi_1` adalah `172.31.0.143` dan `iscsi_2` is `172.31.21.81`.

Pasang iSCSI LUN di klien Linux Anda

Proses pemasangan iSCSI LUN pada klien Linux Anda melibatkan tiga langkah:

- Menemukan node iSCSI target
- Mempartisi iSCSI LUN
- Memasang iSCSI LUN pada klien

Ini tercakup dalam prosedur berikut.

Untuk menemukan node iSCSI target

1. Pada klien Linux Anda, gunakan perintah berikut untuk menemukan node iSCSI target `iscsi_1` menggunakan alamat IP. `iscsi_1_IP`

```
~$ sudo iscsiadm --mode discovery --op update --type sendtargets --  
portal iscsi_1_IP
```

```
172.31.0.143:3260,1029  
iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3  
172.31.21.81:3260,1028  
iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

Dalam contoh ini,

`iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3` sesuai dengan untuk iSCSI LUN di zona ketersediaan yang disukai. `target_initiator`

2. (Opsional) Untuk mendorong throughput yang lebih tinggi daripada klien EC2 tunggal Amazon maksimum 5 Gbps (~625) MBps ke iSCSI LUN Anda, ikuti prosedur yang dijelaskan dalam [bandwidth jaringan EC2 instans Amazon di Panduan Pengguna Amazon](#) Elastic Compute Cloud untuk Instans Linux guna membuat sesi tambahan untuk throughput yang lebih besar.

Perintah berikut menetapkan 8 sesi per inisiator per node ONTAP di setiap zona ketersediaan, memungkinkan klien untuk mendorong hingga 40 Gbps (5.000 MBps) throughput agregat ke iSCSI LUN.

```
~$ sudo iscsiadm --mode node -T target_initiator --op update -n  
node.session.nr_sessions -v 8
```

3. Masuk ke inisiator target. LUNs iSCSI Anda disajikan sebagai disk yang tersedia.

```
~$ sudo iscsiadm --mode node -T target_initiator --login
```

```
Logging in to [iface: default, target:  
iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:  
172.31.14.66,3260] (multiple)  
Login to [iface: default, target:  
iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:  
172.31.14.66,3260] successful.
```

Output di atas terpotong; Anda akan melihat satu `Logging in` dan satu `Login successful` respons untuk setiap sesi pada setiap server file. Dalam kasus 4 sesi per node, akan ada 8 `Logging in` dan 8 `Login successful` tanggapan.

- Gunakan perintah berikut untuk memverifikasi bahwa `dm-multipath` telah mengidentifikasi dan menggabungkan sesi iSCSI dengan menampilkan LUN tunggal dengan beberapa kebijakan. Harus ada jumlah perangkat yang sama yang terdaftar sebagai `active` dan yang terdaftar sebagai `enabled`.

```
~$ sudo multipath -ll
```

Dalam output, nama disk diformat sebagai `dm-xyz`, di mana `xyz` adalah bilangan bulat. Jika tidak ada disk multipath lainnya, nilai ini adalah `dm-0`

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
hwhandler='0' wp=rw
|+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda      8:0   active ready running
| |- 1:0:0:1 sdc      8:32  active ready running
| |- 3:0:0:1 sdg      8:96  active ready running
| `-- 4:0:0:1 sdh      8:112 active ready running
`+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb      8:16  active ready running
  |- 7:0:0:1 sdf      8:80  active ready running
  |- 6:0:0:1 sde      8:64  active ready running
  `-- 5:0:0:1 sdd      8:48  active ready running
```

Perangkat blok Anda sekarang terhubung ke klien Linux Anda. Itu terletak di bawah jalan `setapak/dev/dm-xyz`. Anda tidak boleh menggunakan jalur ini untuk tujuan administratif; sebagai gantinya, gunakan tautan simbolis yang berada di bawah jalur `dev/mapper/wwid`, di mana `wwid` adalah pengenalan unik untuk LUN Anda yang konsisten di seluruh perangkat. Pada langkah berikutnya, Anda akan memberikan nama yang ramah `wwid` sehingga Anda dapat membedakannya dari disk multipathed lainnya.

Untuk menetapkan perangkat blok nama yang ramah

1. Untuk memberikan nama yang ramah pada perangkat Anda, buat alias dalam `/etc/multipath.conf` file. Untuk melakukan ini, tambahkan entri berikut ke file menggunakan editor teks pilihan Anda, ganti placeholder berikut:
 - Ganti `serial_hex` dengan nilai yang Anda simpan dalam [Konfigurasi iSCSI pada sistem file untuk FSx ONTAP](#) prosedur.
 - Tambahkan awalan `3600a0980` ke `serial_hex` nilai seperti yang ditunjukkan pada contoh. Ini adalah pembukaan unik untuk distribusi ONTAP yang NetApp digunakan Amazon FSx untuk NetApp ONTAP.
 - Ganti `device_name` dengan nama ramah yang ingin Anda gunakan untuk perangkat Anda.

```

multipaths {
    multipath {
        wwid 3600a0980serial_hex
        alias device_name
    }
}

```

Sebagai alternatif, Anda dapat menyalin dan menyimpan skrip berikut sebagai file bash, seperti `multipath_alias.sh`. Anda dapat menjalankan skrip dengan hak istimewa `sudo`, mengganti `serial_hex` (tanpa awalan `3600a0980`) dan `device_name` dengan nomor seri masing-masing dan nama ramah yang diinginkan. Skrip ini mencari `multipaths` bagian yang tidak dikomentari dalam file `/etc/multipath.conf`. Jika ada, itu menambahkan `multipath` entri ke bagian itu; jika tidak, itu akan membuat `multipaths` bagian baru dengan `multipath` entri untuk perangkat blok Anda.

```

#!/bin/bash
SN=serial_hex
ALIAS=device_name
CONF=/etc/multipath.conf
grep -q '^multipaths {' $CONF
UNCOMMENTED=$?
if [ $UNCOMMENTED -eq 0 ]
then
    sed -i '/^multipaths {/a\\tmultipath {\\n\\t\\twwid 3600a0980"${SN}"\\n\\t\\talias "${ALIAS}"\\n\\t}\\n' $CONF
else

```



```
printf "multipaths {\n\tmultipath {\n\t\ttwwid 3600a0980$SN\n\t\talias
$ALIAS\n\t}\n}" >> $CONF
fi
```

2. Mulai ulang multipathd layanan /etc/multipathd.conf agar perubahan diterapkan.

```
~$ systemctl restart multipathd.service
```

Untuk mempartisi LUN

Langkah selanjutnya adalah memformat dan mempartisi LUN Anda menggunakan `fdisk`.

1. Gunakan perintah berikut untuk memverifikasi bahwa jalur ke Anda `device_name` ada.

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. Partisi disk menggunakan `fdisk`. Anda akan memasukkan prompt interaktif. Masukkan opsi dalam urutan yang ditampilkan. Anda dapat membuat beberapa partisi dengan menggunakan nilai yang lebih kecil dari sektor terakhir (20971519 dalam contoh ini).

Note

Last sector Nilainya akan bervariasi tergantung pada ukuran iSCSI LUN Anda (10GB dalam contoh ini).

```
~$ sudo fdisk /dev/mapper/device_name
```

Prompt `fdisk` interaktif dimulai.

```
Welcome to fdisk (util-linux 2.30.2).
```

```
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.
```

```
Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.
```

```

Command (m for help): n
Partition type
  p primary (0 primary, 0 extended, 4 free)
  e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
20971519): 20971519

Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.

```

Setelah masuk `w`, partisi baru Anda `/dev/mapper/partition_name` menjadi tersedia. *partition_name* Memiliki formatnya `<device_name><partition_number>`. 1 digunakan sebagai nomor partisi yang digunakan dalam `fdisk` perintah pada langkah sebelumnya.

3. Buat sistem file Anda menggunakan `/dev/mapper/partition_name` sebagai jalur.

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

Sistem merespons dengan output berikut:

```

mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:

```

```
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Untuk me-mount LUN pada klien Linux

1. Buat direktori *directory_path* sebagai titik pemasangan untuk sistem file Anda.

```
~$ sudo mkdir /directory_path/mount_point
```

2. Pasang sistem file menggunakan perintah berikut.

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. (Opsional) Jika Anda ingin memberikan kepemilikan pengguna tertentu dari direktori mount, ganti *username* dengan nama pengguna pemilik.

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (Opsional) Verifikasi bahwa Anda dapat membaca dari dan menulis data ke sistem file.

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

Anda telah berhasil membuat dan memasang iSCSI LUN pada klien Linux Anda.

Penyediaan iSCSI untuk Windows

FSx untuk ONTAP mendukung protokol iSCSI. Anda perlu menyediakan iSCSI pada klien Windows dan SVM dan volume untuk menggunakan protokol iSCSI untuk mengangkut data antara klien dan sistem file Anda. Protokol iSCSI tersedia di semua sistem file yang memiliki 6 atau [lebih sedikit pasangan ketersediaan tinggi](#) (HA).

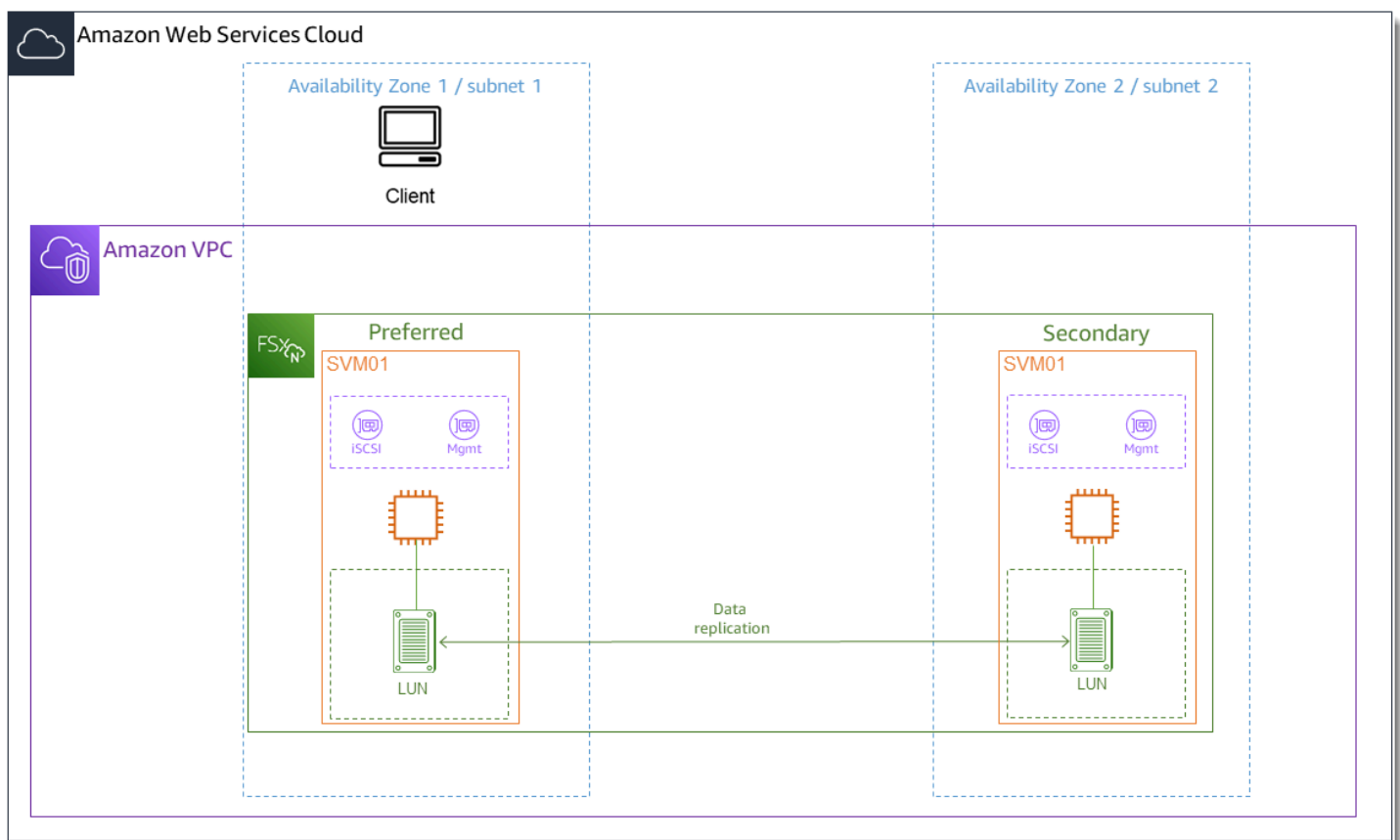
Contoh yang disajikan dalam prosedur ini menunjukkan bagaimana menyediakan protokol iSCSI pada klien FSx dan untuk sistem file ONTAP, dan menggunakan pengaturan berikut:

- iSCSI LUN yang dipasang ke host Windows sudah dibuat. Untuk informasi selengkapnya, lihat [Membuat iSCSI LUN](#).
- Host Microsoft Windows yang memasang iSCSI LUN adalah instance EC2 Amazon yang menjalankan Microsoft Windows Server 2019 Amazon Machine Image (AMI). Ini memiliki grup keamanan VPC yang dikonfigurasi untuk memungkinkan lalu lintas masuk dan keluar seperti yang dijelaskan dalam. [Kontrol Akses Sistem File dengan Amazon VPC](#)

Anda mungkin menggunakan Microsoft Windows AMI yang berbeda dalam pengaturan Anda.

- Klien dan sistem file terletak di VPC yang sama dan. Akun AWS Jika klien berada di VPC lain, Anda dapat menggunakan VPC peering atau AWS Transit Gateway untuk memberikan akses lain ke endpoint iSCSI VPCs . Untuk informasi selengkapnya, lihat [Mengakses data dari luar VPC penyebaran](#).

Sebaiknya EC2 instans berada di zona ketersediaan yang sama dengan subnet pilihan sistem file Anda, seperti yang ditunjukkan pada grafik berikut.



Topik

- [Konfigurasi iSCSI pada klien Windows](#)
- [Konfigurasi iSCSI pada sistem file untuk FSx ONTAP](#)
- [Pasang iSCSI LUN pada klien Windows](#)
- [Memvalidasi konfigurasi iSCSI Anda](#)

Konfigurasi iSCSI pada klien Windows

1. Gunakan Windows Remote Desktop untuk terhubung ke klien Windows tempat Anda ingin memasang iSCSI LUN. Untuk informasi selengkapnya, lihat [Connect ke instans Windows menggunakan RDP di Panduan Pengguna](#) Amazon Elastic Compute Cloud.
2. Buka Windows PowerShell sebagai Administrator. Gunakan perintah berikut untuk mengaktifkan iSCSI pada instance Windows Anda dan konfigurasi layanan iSCSI untuk memulai secara otomatis.

```
PS C:\> Start-Service MSiSCSI
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. Ambil nama inisiator instance Windows Anda. Anda akan menggunakan nilai ini dalam mengonfigurasi iSCSI pada sistem file ONTAP FSx Anda menggunakan CLI ONTAP. NetApp

```
PS C:\> (Get-InitiatorPort).NodeAddress
```

Sistem merespons dengan port inisiator:

```
iqn.1991-05.com.microsoft:ec2amaz-abc123d
```

4. Untuk mengaktifkan klien Anda untuk secara otomatis failover antara server file Anda, Anda perlu instal Multipath-I/O (MPIO) pada instance Windows Anda. Gunakan perintah berikut ini.

```
PS C:\> Install-WindowsFeature Multipath-I/O
```

5. Mulai ulang instance Windows Anda setelah Multipath-I/O instalasi selesai. Biarkan instance Windows Anda tetap terbuka untuk melakukan langkah-langkah pemasangan iSCSI LUN di bagian berikut.

Konfigurasi iSCSI pada sistem file untuk FSx ONTAP

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Menggunakan ONTAP CLI [lun igroup create](#), buat grup inisiator, atau. igroup Grup inisiator memetakan ke LUNs iSCSI dan mengontrol inisiator (klien) mana yang dapat diakses. LUNs Ganti *host_initiator_name* dengan nama inisiator dari host Windows Anda yang Anda ambil dalam prosedur sebelumnya.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype windows
```

Io membuat LUNs dipetakan ke ini igroup tersedia untuk beberapa host, Anda dapat menentukan beberapa nama inisiator yang dipisahkan koma menggunakan [lun igroup create](#) ONTAP Perintah CLI.

3. Konfirmasikan bahwa berhasil igroup dibuat menggunakan [lun igroup show](#) ONTAP Perintah CLI:

```
::> lun igroup show
```

Sistem merespons dengan output berikut:

Vserver	Igroup	Protocol	OS Type	Initiators
svm_name	igroup_name	iscsi	windows	iqn.1994-05.com.windows:abcdef12345

Dengan yang igroup dibuat, Anda siap untuk membuat LUNs dan memetakannya keigroup.

4. Langkah ini mengasumsikan bahwa Anda telah membuat iSCSI LUN. Jika belum, lihat step-by-step instruksi [Membuat iSCSI LUN](#) untuk melakukannya.

Buat pemetaan LUN dari LUN ke yang baru. igroup

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Konfirmasikan bahwa LUN dibuat, online, dan dipetakan dengan perintah berikut:

```
::> lun show -path /vol/vol_name/lun_name
```

Vserver	Path	State	Mapped	Type	Size
<i>svm_name</i>	/vol/ <i>vol_name</i> / <i>lun_name</i>	online	mapped	windows	10GB

Anda sekarang siap untuk menambahkan target iSCSI pada instance Windows Anda.

6. Ambil alamat IP *iscsi_1* dan *iscsi_2* antarmuka untuk SVM Anda menggunakan perintah berikut:

```
::> network interface show -vserver svm_name
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is Home
<i>svm_name</i>	<i>iscsi_1</i>	up/up	172.31.0.143/20	FSxId0123456789abcdef8-01	e0e	true
	<i>iscsi_2</i>	up/up	172.31.21.81/20	FSxId0123456789abcdef8-02	e0e	true
	<i>nfs_smb_management_1</i>	up/up	198.19.250.177/20	FSxId0123456789abcdef8-01	e0e	true

3 entries were displayed.

Dalam contoh ini, alamat IP *iscsi_1* adalah 172.31.0.143 dan *iscsi_2* is 172.31.21.81.

Pasang iSCSI LUN pada klien Windows

1. Pada instance Windows Anda, buka PowerShell terminal sebagai Administrator.
2. Anda akan membuat .ps1 skrip yang melakukan hal berikut:
 - Terhubung ke setiap antarmuka iSCSI sistem file Anda.
 - Menambahkan dan mengkonfigurasi MPIO untuk iSCSI.

- Menetapkan 8 sesi untuk setiap koneksi iSCSI, yang memungkinkan klien untuk mendorong hingga 40 Gbps (MBps5.000) throughput agregat ke iSCSI LUN. Memiliki 8 sesi memastikan satu klien dapat mendorong kapasitas throughput 4.000 penuh untuk tingkat tertinggi untuk kapasitas MBps throughput FSx ONTAP. Anda dapat secara opsional mengubah jumlah sesi ke jumlah sesi yang lebih tinggi atau lebih rendah (setiap sesi menyediakan hingga 625 MBps throughput) dengan memodifikasi variabel. RecommendedConnectionCount Untuk informasi selengkapnya, lihat [Bandwidth jaringan EC2 instans Amazon](#) di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Windows.

Salin kumpulan perintah berikut ke dalam file untuk membuat .ps1 skrip.

- Ganti iscsi_1 dan iscsi_2 dengan alamat IP yang Anda ambil pada langkah sebelumnya.
- Ganti ec2_ip dengan alamat IP instance Windows Anda.

```
Write-Host "Starting iSCSI connection setup..."
$TargetPortalAddresses = @("iscsi_1","iscsi_2"); $LocaliSCSIAddress = "ec2_ip"
$RecommendedConnectionCount = 8

Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
    New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

$currentMPIOSettings = Get-MPIOSetting
if ($currentMPIOSettings.PathVerificationState -ne 'Enabled') {
    Write-Host "Setting MPIO path verification state to Enabled"; Set-
MPIOSetting -NewPathVerificationState Enabled
} else { Write-Host "MPIO path verification state already Enabled" }

$portalConnectionCounts = @{}
foreach ($TargetPortalAddress in $TargetPortalAddresses)
{ $portalConnectionCounts[$TargetPortalAddress] = 0 }

$sessions = Get-IscsiSession
if ($sessions) {
    foreach ($session in $sessions) {
        if ($session.IsConnected) {
```



```

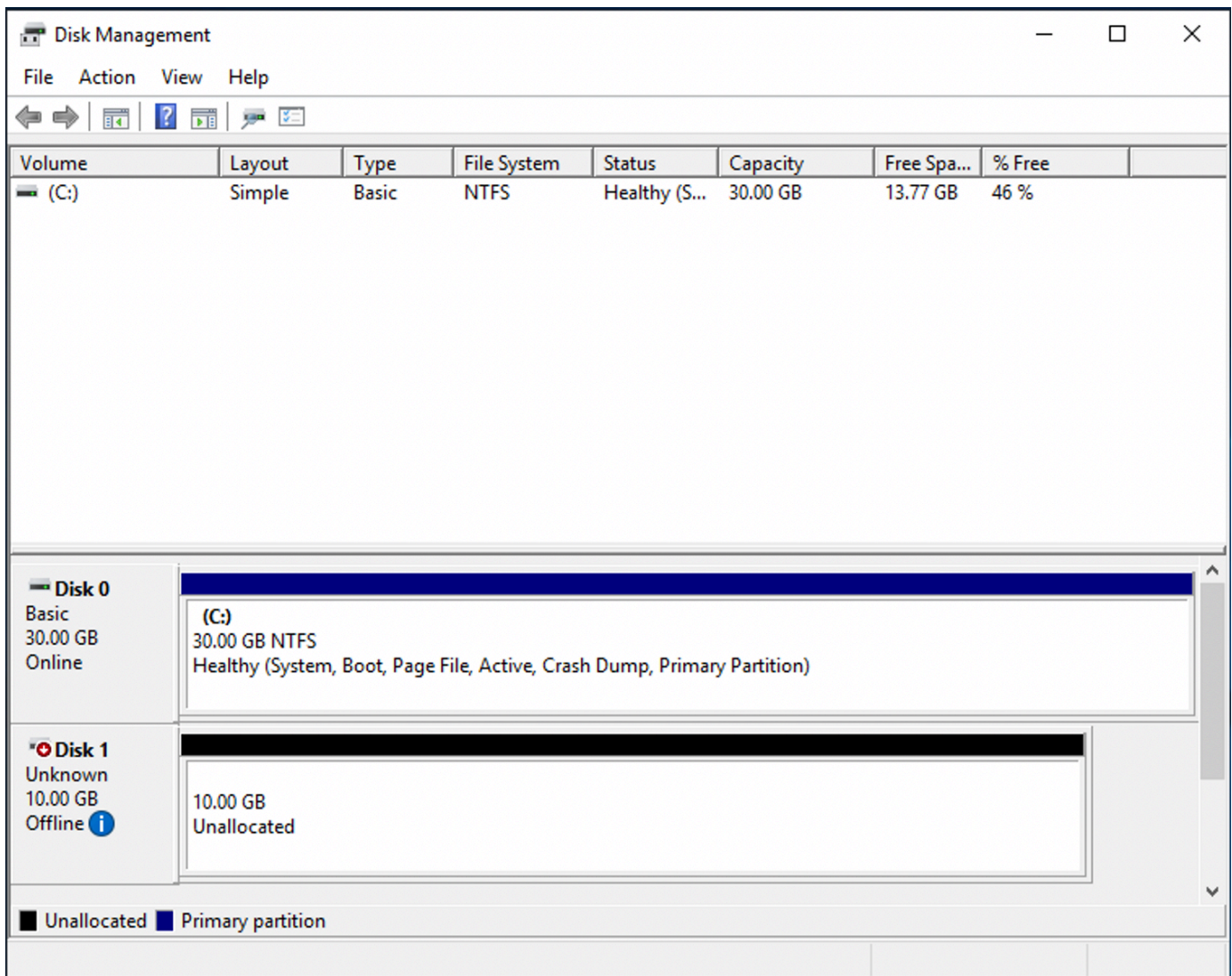
        $targetPortal = (Get-IscsiTargetPortal -iSCSISession
$session).TargetPortalAddress
        if ($portalConnectionCounts.ContainsKey($targetPortal))
{ $portalConnectionCounts[$targetPortal]++ }
    }
}

foreach ($TargetPortalAddress in $TargetPortalAddresses) {
    $existingCount = $portalConnectionCounts[$TargetPortalAddress];
    $remainingConnections = $RecommendedConnectionCount - $existingCount
    Write-Host "Portal $TargetPortalAddress has $existingCount
existing connections, $remainingConnections remaining (max recommended:
$RecommendedConnectionCount)"
    if ($remainingConnections -gt 0) {
        Write-Host "Creating $remainingConnections connections for portal
$TargetPortalAddress"
        1..$remainingConnections | ForEach-Object {
            Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
-IsPersistent $true
        }
    } else { Write-Host "Maximum connections (8) reached for portal
$TargetPortalAddress" }
}

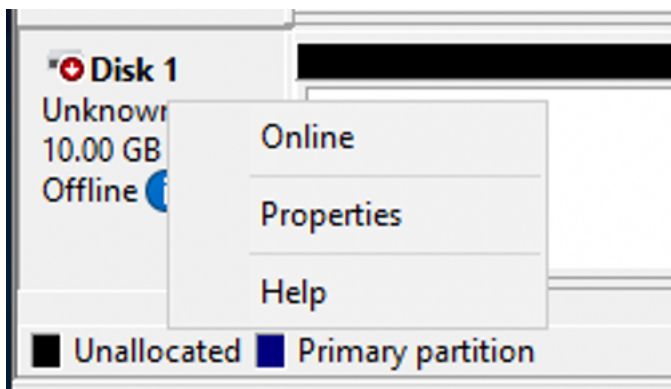
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR

```

3. Luncurkan aplikasi Manajemen Disk Windows. Buka kotak dialog Windows Run, dan masukkan `diskmgmt.msc` dan tekan Enter. Aplikasi Manajemen Disk terbuka.



4. Temukan disk yang tidak terisi ini adalah iSCSI LUN. Dalam contoh, Disk 1 adalah disk iSCSI. Ini offline.



Bawa volume online dengan menempatkan kursor di atas Disk 1 dan klik kanan lalu pilih Online.

Note

Anda dapat mengubah kebijakan jaringan area penyimpanan (SAN) sehingga volume baru secara otomatis dibawa online. Untuk informasi selengkapnya, lihat [kebijakan SAN](#) di Referensi Perintah Microsoft Windows Server.

5. Untuk menginisialisasi disk, letakkan kursor di atas Disk 1 klik kanan, dan pilih Inisialisasi. Dialog Inisialisasi muncul. Pilih OK inisialisasi disk.
6. Format disk seperti biasanya. Setelah pemformatan selesai, drive iSCSI muncul sebagai drive yang dapat digunakan pada klien Windows.

Memvalidasi konfigurasi iSCSI Anda

Kami telah menyediakan skrip untuk memeriksa apakah pengaturan iSCSI Anda dikonfigurasi dengan benar. Script memeriksa parameter seperti jumlah sesi, distribusi node, dan status Multipath I/O (MPIO). Tugas berikut menjelaskan cara menginstal dan menggunakan skrip.

Untuk memvalidasi konfigurasi iSCSI Anda

1. Buka PowerShell jendela Windows.
2. Unduh skrip menggunakan perintah berikut.

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

3. Perluas file zip menggunakan perintah berikut.

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

4. Jalankan skrip menggunakan perintah berikut.

```
PS C:\> ./CheckiSCSI.ps1
```

5. Tinjau output untuk memahami status konfigurasi Anda saat ini. Contoh berikut menunjukkan konfigurasi iSCSI yang sukses.

```
PS C:\> ./CheckiSCSI.ps1
```

```
This script checks the iSCSI configuration on the local instance.  
It will provide information about the number of connected sessions, connected file  
servers, and MPIO status.
```

```
MPIO is installed on this server.
```

```
MPIO Load Balance Policy is set to Round Robin (RR).  
Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'  
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'  
has 16 total sessions (16 active, 0 non-active)  
spread across 2 node(s).  
MPIO: Yes
```

NVMePenyediaan/TCP untuk Linux

FSx untuk ONTAP mendukung Non-Volatile Memory Express melalui TCP (NVMe/TCP) block storage protocol. With NVMe/TCP, Anda menggunakan ONTAP CLI untuk menyediakan ruang nama dan subsistem dan kemudian memetakan ruang nama ke subsistem, mirip dengan cara LUNs disediakan dan dipetakan ke grup inisiator (igroups) untuk iSCSI. Protokol NVMe /TCP tersedia pada sistem file generasi kedua yang memiliki 6 atau lebih sedikit pasangan [ketersediaan tinggi](#) (HA).

Note

FSx untuk sistem file ONTAP menggunakan titik akhir iSCSI SVM untuk protokol penyimpanan blok iSCSI dan /TCP. NVMe

Ada tiga langkah utama untuk memproses NVMe konfigurasi/TCP di Amazon Anda FSx untuk NetApp ONTAP, yang tercakup dalam prosedur berikut:

1. Instal dan konfigurasi NVMe klien di host Linux.
2. Konfigurasi NVMe pada SVM sistem file.
 - Buat NVMe namespace.
 - Buat NVMe subsistem.
 - Petakan namespace ke subsistem.

- Tambahkan NQN klien ke subsistem.
3. Pasang NVMe perangkat di klien Linux.

Sebelum Anda mulai

Sebelum Anda memulai proses mengkonfigurasi sistem file Anda NVMe untuk/TCP, Anda harus menyelesaikan item berikut.

- Buat sistem file FSx untuk ONTAP. Untuk informasi selengkapnya, lihat [Membuat sistem file](#).
- Buat EC2 instance yang menjalankan Red Hat Enterprise Linux (RHEL) 9.3 di VPC yang sama dengan sistem file. Ini adalah host Linux tempat Anda akan mengkonfigurasi NVMe dan mengakses data file Anda menggunakan NVMe /TCP untuk Linux.

Di luar cakupan prosedur ini, jika host berada di VPC lain, Anda dapat menggunakan peering VPC atau AWS Transit Gateway untuk memberikan VPCs akses lain ke titik akhir iSCSI volume. Untuk informasi selengkapnya, lihat [Mengakses data dari luar VPC penyebaran](#).

- Konfigurasi grup keamanan VPC host Linux untuk memungkinkan lalu lintas masuk dan keluar seperti yang dijelaskan dalam. [Kontrol Akses Sistem File dengan Amazon VPC](#)
- Dapatkan kredensi untuk ONTAP pengguna dengan fsxadmin hak istimewa yang akan Anda gunakan untuk mengakses ONTAP CLI. Untuk informasi selengkapnya, lihat [ONTAPperan dan pengguna](#).
- Host Linux yang akan Anda konfigurasi NVMe dan gunakan untuk mengakses sistem file FSx for ONTAP terletak di Akun AWS VPC yang sama dan.
- Kami menyarankan agar EC2 instans berada di zona ketersediaan yang sama dengan subnet pilihan sistem file Anda.

Jika EC2 instans Anda menjalankan AMI Linux yang berbeda dari RHEL 9.3, beberapa utilitas yang digunakan dalam prosedur dan contoh ini mungkin sudah diinstal, dan Anda mungkin menggunakan perintah yang berbeda untuk menginstal paket yang diperlukan. Selain menginstal paket, perintah yang digunakan di bagian ini berlaku untuk EC2 Linux lainnya AMIs.

Topik

- [Instal dan konfigurasi NVMe pada host Linux](#)
- [Konfigurasi NVMe pada FSx sistem file untuk ONTAP](#)
- [Pasang NVMe perangkat di klien Linux Anda](#)

Instal dan konfigurasi NVMe pada host Linux

Untuk menginstal NVMe klien

1. Connect ke instance Linux Anda menggunakan klien SSH. Untuk informasi selengkapnya, lihat [Connect ke instans Linux Anda dari Linux atau macOS menggunakan SSH](#).
2. Instal `nvme-cli` menggunakan perintah berikut:

```
~$ sudo yum install -y nvme-cli
```

3. Muat `nvme-tcp` modul ke host:

```
$ sudo modprobe nvme-tcp
```

4. Dapatkan Nama NVMe Berkualitas (NQN) host Linux dengan menggunakan perintah berikut:

```
$ cat /etc/nvme/hostnqn  
nqn.2014-08.org.nvmexpress:uuid:9ed5b327-b9fc-4cf5-97b3-1b5d986345d1
```

Rekam respons untuk digunakan di langkah selanjutnya.

Konfigurasi NVMe pada FSx sistem file untuk ONTAP

Untuk mengkonfigurasi NVMe pada sistem file

Hubungkan ke CLI NetApp ONTAP FSx pada sistem file for ONTAP tempat Anda berencana untuk membuat NVMe perangkat.

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Buat volume baru pada SVM yang Anda gunakan untuk mengakses NVMe antarmuka.

```
::> vol create -vserver fsx -volume nvme_vol1 -aggregate aggr1 -size 1t
```

```
[Job 597] Job succeeded: Successful
```

3. Buat NVMe namespace ns_1 menggunakan perintah [vserver nvme namespace create](#) NetApp ONTAP CLI. Namespace memetakan ke inisiator (klien) dan mengontrol inisiator (klien) mana yang memiliki akses ke perangkat. NVMe

```
::> vserver nvme namespace create -vserver fsx -path /vol/nvme_vol1/ns_1 -size 100g
      -ostype linux
Created a namespace of size 100GB (107374182400).
```

4. Buat NVMe subsystem menggunakan perintah [vserver nvme subsystem create](#) NetApp ONTAP CLI.

```
~$ vserver nvme subsystem create -vserver fsx -subsystem sub_1 -ostype linux
```

5. Petakan namespace ke subsystem yang baru saja Anda buat.

```
::> vserver nvme subsystem map add -vserver fsx -subsystem sub_1 -path /vol/
      nvme_vol1/ns_1
```

6. Tambahkan klien ke subsystem menggunakan NQN yang Anda ambil sebelumnya.

```
::> vserver nvme subsystem host add -subsystem sub_1 -host-nqn
      nqn.2014-08.org.nvmeexpress:uuid:ec21b083-1860-d690-1f29-44528e4f4e0e -vserver fsx
```

Jika Anda ingin membuat perangkat yang dipetakan ke subsystem ini tersedia untuk beberapa host, Anda dapat menentukan beberapa nama inisiator dalam daftar yang dipisahkan koma. Untuk informasi selengkapnya, lihat [vserver nvme subsystem host add](#) di ONTAP Docs. NetApp

7. Konfirmasikan bahwa namespace ada menggunakan perintah: [vserver nvme namespace show](#)

```
::> vserver nvme namespace show -vserver fsx -instance
Vserver Name: fsx
      Namespace Path: /vol/nvme_vol1/ns_1
      Size: 100GB
      Size Used: 90.59GB
      OS Type: linux
      Comment:
      Block Size: 4KB
      State: online
      Space Reservation: false
      Space Reservations Honored: false
```

```

        Is Read Only: false
        Creation Time: 5/20/2024 17:03:08
        Namespace UUID: c51793c0-8840-4a77-903a-c869186e74e3
        Vdisk ID: 80d42c6f00000000187cca9
        Restore Inaccessible: false
        Inconsistent Filesystem: false
        Inconsistent Blocks: false
        NVFail: false
Node Hosting the Namespace: FsxId062e9bb6e05143fcb-01
        Volume Name: nvme_vol1
        Qtree Name:
        Mapped Subsystem: sub_1
        Subsystem UUID: db526ec7-16ca-11ef-a612-d320bd5b74a9
        Namespace ID: 00000001h
        ANA Group ID: 00000001h
        Vserver UUID: 656d410a-1460-11ef-a612-d320bd5b74a9
        Vserver ID: 3
        Volume MSID: 2161388655
        Volume DSID: 1029
        Aggregate: aggr1
        Aggregate UUID: cfa8e6ee-145f-11ef-a612-d320bd5b74a9
Namespace Container State: online
        Autodelete Enabled: false
        Application UUID: -
        Application: -
        Has Metadata Provisioned: true

1 entries were displayed.

```

8. Gunakan [network interface show -vserver](#) perintah untuk mengambil alamat antarmuka penyimpanan blok untuk SVM tempat Anda membuat perangkat. NVMe

```

::> network interface show -vserver svm_name -data-protocol nvme-tcp

```

	Logical	Status	Network	Current
	Current Is			
Vserver	Interface	Admin/Oper	Address/Mask	Node
	Port Home			
<i>svm_name</i>	iscsi_1	up/up	172.31.16.19/20	
FsxId0123456789abcdef8-01	e0e	true		


```

            iscsi_2                up/up      172.31.26.134/20
FSxId0123456789abcdef8-02  e0e      true
2 entries were displayed.

```

Note

`iscsi_1`LIF digunakan untuk iSCSI dan /TCP. NVMe

Dalam contoh ini, alamat IP `iscsi_1` adalah 172.31.16.19 dan `iscsi_2` adalah 172.31.26.134.

Pasang NVMe perangkat di klien Linux Anda

Proses pemasangan NVMe perangkat pada klien Linux Anda melibatkan tiga langkah:

1. Menemukan node NVMe
2. Membagi perangkat NVMe
3. Memasang NVMe perangkat pada klien

Ini tercakup dalam prosedur berikut.

Untuk menemukan NVMe node target

1. Pada klien Linux Anda, gunakan perintah berikut untuk menemukan NVMe node target. Ganti *iscsi_1_IP* dengan `iscsi_1` alamat IP, dan *client_IP* alamat IP klien.

Note

`iscsi_1` dan `iscsi_2` LIFs digunakan untuk NVMe iSCSI dan penyimpanan.

```
~$ sudo nvme discover -t tcp -w client_IP -a iscsi_1_IP
```

```

Discovery Log Number of Records 4, Generation counter 11
=====Discovery Log Entry 0=====
trtype:  tcp
adrfam:  ipv4

```

```

subtype: current discovery subsystem
treql:    not specified
portid: 0
trsvcid: 8009
subnqn: nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr: 172.31.26.134
eflags: explicit discovery connections, duplicate discovery information
sectype: none
=====Discovery Log Entry 1=====
trtype: tcp
adrfam: ipv4
subtype: current discovery subsystem
treql:    not specified
portid: 1
trsvcid: 8009
subnqn: nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
traddr: 172.31.16.19
eflags: explicit discovery connections, duplicate discovery information
sectype: none

```

2. (Optional) Untuk mendorong throughput yang lebih tinggi daripada klien EC2 tunggal Amazon maksimum 5 Gbps (~625 MBps) ke NVMe perangkat file Anda, ikuti prosedur yang dijelaskan dalam bandwidth [jaringan EC2 instans Amazon](#) di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux untuk membuat sesi tambahan.
3. Masuk ke inisiator target dengan batas waktu kehilangan pengontrol setidaknya 1800 detik, sekali lagi menggunakan `iscsi_1` alamat IP untuk `iscsi_1_IP` dan alamat IP klien untuk `client_IP` NVMe Perangkat Anda disajikan sebagai disk yang tersedia.

```
~$ sudo nvme connect-all -t tcp -w client_IP -a iscsi_1 -l 1800
```

4. Gunakan perintah berikut untuk memverifikasi bahwa NVMe tumpukan telah mengidentifikasi dan menggabungkan beberapa sesi dan mengkonfigurasi multipathing. Perintah kembali Y jika konfigurasi berhasil.

```
~$ cat /sys/module/nvme_core/parameters/multipath
Y
```

5. Gunakan perintah berikut untuk memverifikasi bahwa pengaturan NVMe -of model diatur ke NetApp ONTAP Controller dan load balancing iopolicy diatur round-robin untuk masing-masing ONTAP ruang nama untuk mendistribusikan I/O pada semua jalur yang tersedia

```
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/model
Amazon Elastic Block Store
NetApp ONTAP Controller
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/iopolicy
numa
round-robin
```

6. Gunakan perintah berikut untuk memverifikasi bahwa ruang nama dibuat dan ditemukan dengan benar di host:

```
~$ sudo nvme list
```

Node	Generic Namespace	Usage	SN	Model	FW
Rev					

/dev/nvme0n1	/dev/ng0n1	vol05955547c003f0580	Amazon Elastic		
Block Store	0x1	25.77 GB / 25.77 GB	512 B + 0 B		
1.0					
/dev/nvme2n1	/dev/ng2n1	1WB12JWY/XLKAAAAAAC	NetApp ONTAP		
Controller	0x1	107.37 GB / 107.37 GB	4 KiB + 0 B		
FFFFFFFF					

Perangkat baru dalam output adalah /dev/nvme2n1. Skema penamaan ini mungkin berbeda tergantung pada instalasi Linux Anda.

7. Verifikasi bahwa status pengontrol setiap jalur aktif dan memiliki status multipathing Asymmetric Namespace Access (ANA) yang benar:

```
~$ nvme list-subsys /dev/nvme2n1
nvme-subsys2 -
  NQN=nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:subsystem.rhel
    hostnqn=nqn.2014-08.org.nvmeexpress:uuid:ec2a70bf-3ab2-6cb0-f997-8730057ceb24
      iopolicy=round-robin
\
+- nvme2 tcp
traddr=172.31.26.134,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
live non-optimized
```

```
+ - nvme3 tcp
traddr=172.31.16.19,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
live optimized
```

Dalam contoh ini, NVMe tumpukan telah secara otomatis menemukan LIF alternatif sistem file Anda `scsi_2`, `172.31.26.134`.

8. Verifikasi bahwa NetApp plug-in menampilkan nilai yang benar untuk masing-masing ONTAP perangkat namespace:

```
~$ sudo nvme netapp ontapdevices -o column
Device          Vserver          Namespace Path
              NSID  UUID                               Size
-----
-----
-----
/dev/nvme2n1     fsx              /vol/nvme_vol1/ns_1
                1      0441c609-3db1-4b0b-aa83-790d0d448ece  107.37GB
```

Untuk mempartisi perangkat

1. Gunakan perintah berikut untuk memverifikasi bahwa jalur ke device_name `nvme2n1` Anda ada.

```
~$ ls /dev/mapper/nvme2n1
/dev/nvme2n1
```

2. Partisi disk menggunakan `fdisk`. Anda akan memasukkan prompt interaktif. Masukkan opsi dalam urutan yang ditampilkan. Anda dapat membuat beberapa partisi dengan menggunakan nilai yang lebih kecil dari sektor terakhir (20971519 dalam contoh ini).

Note

Last sector Nilainya akan bervariasi tergantung pada ukuran NVMe perangkat Anda (100 GiB dalam contoh ini).

```
~$ sudo fdisk /dev/mapper/nvme2n1
```

Prompt `fdisk` interaktif dimulai.

```
Welcome to fdisk (util-linux 2.37.4).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.
```

```
Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.
```

```
Command (m for help): n
Partition type
  p primary (0 primary, 0 extended, 4 free)
  e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (256-26214399, default 256):
Last sector, +sectors or +size{K,M,G,T,P} (256-26214399, default
26214399): 20971519
```

```
Created a new partition 1 of type 'Linux' and of size 100 GiB.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

Setelah masukw, partisi baru Anda /dev/nvme2n1 menjadi tersedia. *partition_name* Memiliki formatnya *<device_name><partition_number>*. 1 digunakan sebagai nomor partisi dalam fdisk perintah pada langkah sebelumnya.

3. Buat sistem file Anda menggunakan /dev/nvme2n1 sebagai jalur.

```
~$ sudo mkfs.ext4 /dev/nvme2n1
```

Sistem merespons dengan output berikut:

```
mke2fs 1.46.5 (30-Dec-2021)
Found a dos partition table in /dev/nvme2n1
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 372fb2fd-ae0e-4e74-ac06-3eb3eabd55fb
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872
```

```
Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

Untuk me-mount NVMe perangkat pada klien Linux

1. Buat direktori *directory_path* sebagai titik pemasangan untuk sistem file Anda pada instance Linux.

```
~$ sudo mkdir /directory_path/mount_point
```

2. Pasang sistem file menggunakan perintah berikut.

```
~$ sudo mount -t ext4 /dev/nvme2n1 /directory_path/mount_point
```

3. (Opsional) Jika Anda ingin memberikan kepemilikan pengguna tertentu dari direktori mount, ganti *username* dengan nama pengguna pemilik.

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (Opsional) Verifikasi bahwa Anda dapat membaca dari dan menulis data ke sistem file.

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

Anda telah berhasil membuat dan memasang NVMe perangkat di klien Linux Anda.

Mengakses data Anda melalui jalur akses Amazon S3

Anda juga dapat menggunakan titik akses S3 untuk mengakses data file yang disimpan di sistem FSx file Amazon seolah-olah berada di S3, memungkinkan Anda untuk menggunakannya dengan aplikasi dan layanan yang bekerja dengan S3 tanpa perubahan aplikasi atau memindahkan data dari penyimpanan file. Titik akses Amazon S3 adalah titik akhir S3 yang terpasang ke bucket S3 atau untuk ONTAP dan FSx untuk volume OpenZFS. FSx Jalur akses Amazon S3 menyederhanakan pengelolaan akses data untuk aplikasi atau AWS layanan apa pun yang berfungsi dengan S3.

Dengan titik akses S3, pelanggan dengan kumpulan data bersama, termasuk data lake, arsip media, dan konten buatan pengguna, dapat dengan mudah mengontrol dan menskalakan akses data untuk ratusan aplikasi, tim, atau individu dengan membuat titik akses individual dengan nama dan izin yang disesuaikan untuk masing-masing.

Titik akses S3 yang dilampirkan ke Amazon FSx untuk volume NetApp ONTAP mendukung akses baca dan tulis ke data file Anda menggunakan operasi objek S3 (misalnya, `GetObjectPutObject`, dan `ListObjectsV2`) terhadap titik akhir Amazon S3.

Setiap titik akses S3 yang dilampirkan ke sistem file FSx untuk ONTAP memiliki kebijakan titik akses AWS Identity and Access Management (IAM) dan pengguna sistem file UNIX atau Windows terkait yang digunakan untuk mengotorisasi semua permintaan yang dibuat melalui jalur akses. Untuk setiap permintaan, S3 pertama-tama mengevaluasi semua kebijakan yang relevan, termasuk kebijakan pengguna, titik akses, Titik Akhir VPC S3, dan kebijakan kontrol layanan, untuk mengotorisasi permintaan tersebut. Setelah permintaan disahkan oleh S3, permintaan tersebut kemudian diotorisasi oleh sistem file, yang mengevaluasi apakah pengguna sistem file yang terkait dengan titik akses S3 memiliki izin untuk mengakses data pada sistem file. Anda dapat mengonfigurasi titik akses untuk menerima permintaan hanya dari virtual private cloud (VPC) untuk membatasi akses data Amazon S3 ke jaringan pribadi. Amazon S3 memberlakukan Blokir akses publik secara default untuk semua titik akses yang dilampirkan ke volume FSx untuk ONTAP, dan Anda tidak dapat mengubah atau menonaktifkan setelan ini.

Anda menggunakan FSx konsol Amazon, CLI, dan API untuk [membuat titik akses S3 dan melampirkannya](#) ke volume untuk ONTAP. FSx Titik akses memungkinkan Anda untuk mengakses data file Anda menggunakan API S3, meskipun data Anda terus berada di sistem file ONTAP Anda FSx dan Anda dapat terus menggunakan protokol NFS dan SMB untuk mengakses data Anda di samping S3 API.

Jalur akses Amazon S3 FSx untuk sistem pengisian ONTAP memberikan latensi dalam rentang puluhan milidetik, konsisten dengan akses bucket S3. Throughput dan permintaan per detik yang dapat Anda arahkan ke sistem FSx file Amazon melalui S3 API bergantung pada throughput yang disediakan sistem file. Untuk informasi selengkapnya tentang kemampuan kinerja sistem file, lihat [Amazon FSx untuk kinerja NetApp ONTAP](#)

Topik

- [Wilayah AWS dengan jalur akses Amazon S3 untuk FSx ONTAP](#)
- [Aturan, batasan, dan batasan penamaan titik akses](#)
- [Mereferensikan titik akses dengan ARNs, alias titik akses, atau virtual-hosted-style URIs](#)

- [Kompatibilitas titik akses](#)
- [Mengelola akses titik akses](#)
- [Membuat titik akses](#)
- [Mengelola titik akses Amazon S3](#)
- [Menggunakan titik akses](#)
- [Memecahkan masalah titik akses S3](#)

Wilayah AWS dengan jalur akses Amazon S3 untuk FSx ONTAP

Jalur akses Amazon S3 FSx untuk ONTAP didukung sebagai berikut Wilayah AWS: Afrika (Cape Town), Asia Pasifik (Hong Kong, Hyderabad, Jakarta, Melbourne, Mumbai, Osaka, Seoul, Singapura, Sydney, Tokyo), Kanada (Tengah), Kanada Barat (Calgary), Eropa (Frankfurt, Irlandia, London, Milan, Paris, Spanyol, Stockholm, Zurich), Israel (Tel Aviv), Timur Tengah (Bahrain, UEA), Amerika Selatan (Sao Paulo), AS Timur (Virginia N., Ohio), dan AS Barat (California N., Oregon).

Aturan, batasan, dan batasan penamaan titik akses

Saat membuat titik akses S3 Anda memilih nama untuk itu. Topik berikut memberikan informasi tentang aturan dan batasan dan batasan penamaan jalur akses S3.

Topik

- [Aturan penamaan titik akses](#)
- [Pembatasan dan batasan titik akses](#)

Aturan penamaan titik akses

Saat Anda membuat titik akses S3, Anda memilih namanya. Nama titik akses tidak harus unik di seluruh Akun AWS atau Wilayah AWS. Hal yang sama Akun AWS dapat membuat titik akses dengan nama yang sama di berbeda Wilayah AWS atau dua yang berbeda Akun AWS dapat menggunakan nama titik akses yang sama. Namun, dalam satu Wilayah AWS Akun AWS mungkin tidak memiliki dua titik akses bernama identik.

Nama titik akses S3 tidak dapat diakhiri dengan akhiran `-ext-s3alias`, yang dicadangkan untuk alias titik akses. Untuk daftar lengkap aturan penamaan titik akses, lihat [Aturan penamaan untuk titik akses Amazon S3](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Pembatasan dan batasan titik akses

Titik akses S3 yang dilampirkan FSx untuk volume ONTAP memiliki batasan berikut, yang tidak berlaku untuk titik akses yang terpasang pada bucket S3:

- Anda hanya dapat membuat titik akses S3 Wilayah AWS sama dengan volume ONTAP FSx untuk yang Anda lampirkan.
- Hal yang sama Akun AWS harus memiliki sistem file FSx untuk ONTAP dan titik akses S3. Anda hanya dapat membuat titik akses S3 yang dilampirkan FSx untuk volume ONTAP yang Anda miliki. Anda tidak dapat membuat titik akses S3 yang dilampirkan ke volume yang dimiliki oleh orang lain Akun AWS.
- Anda hanya dapat membuat dan melampirkan jalur akses S3 FSx untuk sistem file ONTAP yang menjalankan NetApp ONTAP versi 9.17.1 dan yang lebih baru.

Untuk daftar lengkap semua batasan dan batasan jalur akses, lihat [Pembatasan dan batasan untuk titik akses](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Mereferensikan titik akses dengan ARNs, alias titik akses, atau virtual-hosted-style URIs

Setelah Anda membuat titik akses yang dilampirkan ke volume ONTAP FSx untuk, Anda dapat mengakses data Anda melalui API AWS CLI dan S3, serta layanan AWS dan aplikasi pihak ketiga yang kompatibel dengan S3. Saat merujuk ke titik akses dalam aplikasi Layanan AWS atau, Anda dapat menggunakan Nama Sumber Daya Amazon (ARN), alias titik akses, atau URI gaya host virtual.

Topik

- [Titik akses ARNs](#)
- [Alias titik akses](#)
- [URI bergaya host virtual](#)

Titik akses ARNs

Titik akses memiliki Nama Sumber Daya Amazon (ARNs). Access point ARNs mirip dengan bucket S3 ARNs, tetapi mereka secara eksplisit diketik dan menyandikan titik akses Wilayah AWS dan Akun AWS ID pemilik jalur akses. Untuk informasi selengkapnya ARNs, lihat [Mengidentifikasi AWS sumber](#)

[daya dengan Amazon Resource Names \(ARNs\)](#) di Panduan AWS Identity and Access Management Pengguna.

Titik akses ARNs memiliki format berikut:

```
arn:aws::s3:region:account-id:accesspoint/resource
```

arn:aws:s3:us-west-2:777777777777:accesspoint/*test* mewakili titik akses bernama *test*, dimiliki oleh akun 777777777777 di Wilayah. *us-west-2*

ARNs untuk objek dan file yang diakses melalui jalur akses gunakan format berikut:

```
arn:aws::s3:region:account-id:accesspoint/access-point-name/object/resource
```

arn:aws:s3:us-west-2:111122223333:accesspoint/*test*/object/*lions.jpg* mewakili file *lions.jpg*, diakses melalui titik akses bernama *test*, dimiliki oleh akun 111122223333 di Wilayah. *us-west-2*

Untuk informasi selengkapnya tentang titik [akses ARNs, lihat Titik akses ARNs](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Alias titik akses

Saat Anda membuat titik akses, Amazon S3 secara otomatis menghasilkan alias titik akses yang dapat Anda gunakan di mana saja Anda dapat menggunakan nama bucket S3 untuk mengakses data.

Alias titik akses tidak dapat diubah. Untuk titik akses yang dilampirkan ke volume FSx untuk ONTAP, alias titik akses terdiri dari bagian-bagian berikut:

```
access point prefix-metadata-ext-s3alias
```

Berikut ini menunjukkan alias ARN dan titik akses untuk titik akses S3 yang dilampirkan ke volume FSx untuk ONTAP, dikembalikan sebagai bagian dari respons terhadap perintah CLI. `describe-s3-access-point-attachments` FSx Titik akses dalam contoh ini diberi nama `my-ontap-ap`.

```
...
  "S3AccessPoint": {
```

```
"ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-ontap-ap",  
"Alias": "my-ontap-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias",  
...
```

Note

-ext-s3alias Akhirnya dicadangkan untuk alias titik akses S3 yang dilampirkan ke volume FSx untuk ONTAP, dan tidak dapat digunakan untuk nama titik akses.

Anda dapat menggunakan alias titik akses alih-alih ARN titik akses Amazon S3 di beberapa operasi pesawat data S3. Untuk daftar operasi yang didukung, lihat [Kompatibilitas titik akses](#).

Untuk set lengkap batasan alias titik akses, lihat [Batasan alias titik akses](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

URI bergaya host virtual

Titik akses hanya mendukung virtual-host-style pengalamatan. Dalam URI gaya host virtual, nama titik akses Akun AWS, dan Wilayah AWS merupakan bagian dari nama domain di URL. Untuk melihat URI S3 untuk titik akses yang dilampirkan ke volume FSx untuk ONTAP, di halaman detail titik akses di bawah detail titik akses S3, pilih nama titik akses yang tercantum untuk titik akses S3. Ini membawa Anda ke halaman detail titik akses di konsol Amazon S3. Anda dapat menemukan URI S3 di bawah Properties.

Untuk informasi selengkapnya, lihat [URI bergaya Virtual-host di Panduan](#) Pengguna Layanan Penyimpanan Sederhana Amazon.

Kompatibilitas titik akses

Anda dapat menggunakan titik akses untuk mengakses data yang disimpan pada volume FSx untuk ONTAP menggunakan Amazon APIs S3 berikut untuk akses data. Semua operasi yang tercantum di bawah ini dapat menerima alias titik akses ARNs atau titik akses.

Tabel berikut adalah sebagian daftar operasi Amazon S3 dan jika kompatibel dengan titik akses. Tabel menunjukkan operasi mana yang didukung oleh titik akses menggunakan volume FSx untuk ONTAP sebagai sumber data.

Operasi S3	Titik akses yang dilampirkan ke volume FSx untuk ONTAP
AbortMultipartUpload	Didukung
CompleteMultipartUpload	Didukung
CopyObject (Hanya salinan wilayah yang sama)	Didukung, jika sumber dan tujuan berada dalam titik akses yang sama
CreateMultipartUpload	Didukung
DeleteObject	Didukung
DeleteObjects	Didukung
DeleteObjectTagging	Didukung
GetBucketAcl	Tidak didukung
GetBucketCors	Tidak didukung
GetBucketLocation	Didukung
GetBucketNotificationConfiguration	Tidak didukung
GetBucketPolicy	Tidak didukung
GetObject	Didukung
GetObjectAcl	Tidak didukung
GetObjectAttributes	Didukung
GetObjectLegalHold	Tidak didukung
GetObjectRetention	Tidak didukung
GetObjectTagging	Didukung

Operasi S3	Titik akses yang dilampirkan ke volume FSx untuk ONTAP
HeadBucket	Didukung
HeadObject	Didukung
ListMultipartUploads	Didukung
ListObjects	Didukung
ListObjectsV2	Didukung
ListObjectVersions	Tidak didukung
ListParts	Didukung
Presign	Tidak didukung
PutObject	Didukung
PutObjectAcl	Tidak didukung
PutObjectLegalHold	Tidak didukung
PutObjectRetention	Tidak didukung
PutObjectTagging	Didukung
RestoreObject	Tidak didukung
UploadPart	Didukung
UploadPartCopy (Hanya salinan wilayah yang sama)	Didukung, jika sumber dan tujuan berada dalam titik akses yang sama

Batasan untuk menggunakan operasi Amazon S3 adalah sebagai berikut:

- Ukuran objek maksimum adalah 5 GB untuk diunggah, tetapi Anda dapat mengunduh objek yang lebih besar dari itu

- FSX_ONTAP adalah satu-satunya kelas penyimpanan yang didukung
- SSE-FSX adalah satu-satunya mode enkripsi sisi server yang didukung
- Fitur Amazon S3 berikut tidak didukung: daftar kontrol akses (ACLs) selain `bucket-owner-full-control`, Requester Pays, Object Versioning, Object Lock, Object Lifecycle, Static Website Hosting (misalnya, pengalihan situs web), otentikasi multi-faktor (MFA), dan penulisan bersyarat

Untuk contoh menggunakan titik akses untuk melakukan operasi akses data pada data file, lihat [Menggunakan titik akses](#).

Objek ETag

Tag entitas adalah hash dari objek. ETag Merefleksikan perubahan hanya pada isi objek, bukan metadatanya. ETag Ini bukan MD5 intisari dari data objek.

Objek Checksum

Anda dapat menggunakan nilai checksum untuk memverifikasi integritas data yang Anda unggah. Saat Anda mengunggah data dan menentukan algoritma checksum, AWS SDK menggunakan algoritma checksum yang Anda pilih untuk menghitung nilai checksum sebelum transmisi data. Amazon S3 kemudian secara independen menghitung checksum data Anda dan memvalidasinya terhadap nilai checksum yang disediakan. Objek diterima hanya setelah mengonfirmasi integritas data dipertahankan selama transit ke Amazon S3. Tidak seperti checksum untuk objek di bucket Tujuan Umum Amazon S3, nilai checksum tidak disimpan dalam volume NetApp untuk ONTAP sebagai FSx metadata objek dan objek itu sendiri. Ini berarti bahwa nilai checksum tidak dikembalikan dalam respons dan tidak digunakan untuk memverifikasi integritas objek saat diunduh.

Enkripsi sisi server dengan Amazon FSx (SSE-FSX)

Semua sistem FSx file Amazon memiliki enkripsi yang dikonfigurasi secara default dan dienkripsi saat istirahat dengan kunci yang dikelola menggunakan AWS Key Management Service Data secara otomatis dienkripsi dan didekripsi pada sistem file karena data sedang ditulis dan dibaca dari sistem file. Proses ini ditangani secara transparan oleh Amazon. FSx

Pengunggahan multibagian

Unggahan multibagian memungkinkan Anda untuk mengunggah satu objek sebagai kumpulan bagian. Setiap bagian merupakan bagian data objek yang saling berkaitan. Anda dapat mengunggah bagian objek ini secara independen, dan dalam urutan apa pun. Unggahan multipart memiliki pertimbangan berikut saat menggunakan jalur akses S3 dengan FSx untuk ONTAP:

- Bagian yang terkait dengan unggahan multibagian yang sedang berlangsung (yaitu unggahan tidak lengkap) tidak disertakan untuk pencadangan volume ONTAP. FSx
- Penyimpanan yang digunakan terkait dengan bagian unggahan multibagian yang sedang berlangsung (yaitu unggahan tidak lengkap) tidak tercermin dalam CloudWatch metrik kapasitas StorageUsed penyimpanan volume tujuan tetapi tercermin dalam metrik kapasitas StorageUsed penyimpanan sistem file induk. CloudWatch
- Setelah operasi upload multipart selesai, metadata bagian terkait tidak lagi disimpan dengan objek. Ini berarti Anda tidak dapat mengambil bagian objek metadata menggunakan `GetObjectAttributes` atau mengunduh satu bagian objek dengan nomor bagian objek yang sedang dibaca.

Daftar Kontrol Akses (ACL)

Daftar kontrol akses Amazon S3 (ACLs) memungkinkan Anda mengelola akses ke bucket dan objek. Titik akses S3 FSx hanya mendukung nilai `bucket-owner-full-control` ACL. Menggunakan nilai ACL lainnya akan menghasilkan `InvalidArgument` pengecualian.

Mengelola akses titik akses

Anda dapat mengonfigurasi setiap titik akses S3 dengan izin dan kontrol jaringan yang berbeda yang diterapkan S3 untuk setiap permintaan yang dibuat menggunakan jalur akses tersebut. Kebijakan sumber daya dukungan titik akses S3 AWS Identity and Access Management (IAM) yang dapat Anda gunakan untuk mengontrol penggunaan titik akses menurut sumber daya, pengguna, atau kondisi lainnya. Untuk aplikasi atau pengguna untuk mengakses file melalui titik akses, baik titik akses dan volume yang mendasarinya harus mengizinkan permintaan. Untuk informasi selengkapnya, lihat [Kebijakan jalur akses IAM](#).

Jalur akses Amazon S3 FSx untuk ONTAP menggunakan model otorisasi lapisan ganda yang menggabungkan izin AWS IAM dengan izin tingkat sistem file. Pendekatan ini memastikan bahwa permintaan akses data diotorisasi dengan benar pada tingkat AWS layanan dan tingkat sistem file yang mendasarinya.

Agar aplikasi atau pengguna berhasil mengakses data melalui titik akses, kebijakan jalur akses S3 dan yang mendasari FSx volume ONTAP harus mengizinkan permintaan tersebut.

Topik

- [Identitas dan otorisasi pengguna sistem file](#)

- [Otorisasi permintaan API S3](#)
- [Blokir Akses Publik S3](#)
- [Kebijakan jalur akses IAM](#)

Identitas dan otorisasi pengguna sistem file

Saat Anda membuat jalur akses S3 untuk volume ONTAP, Anda menentukan identitas sistem file yang akan digunakan untuk mengotorisasi semua permintaan sistem file yang dibuat melalui titik akses tersebut. FSx Identitas sistem file ini menentukan tingkat akses apa yang diberikan ke file dan direktori yang mendasari berdasarkan model izin sistem file. Pengguna sistem file adalah akun pengguna pada sistem FSx file Amazon yang mendasarinya. Jika pengguna sistem file memiliki akses hanya-baca, maka hanya permintaan baca yang dibuat menggunakan titik akses yang diotorisasi, dan permintaan tulis diblokir. Jika pengguna sistem file memiliki akses baca-tulis, maka permintaan baca dan tulis ke volume terlampir yang dibuat menggunakan titik akses diotorisasi.

Identitas sistem file dapat menjadi salah satu dari dua jenis:

- **Identitas UNIX** — Gunakan identitas UNIX (nama pengguna) saat mengakses volume dengan gaya keamanan UNIX
- **Windows Identity** — Gunakan identitas Windows (domain dan nama pengguna) saat mengakses volume dengan gaya keamanan NTFS.

Saat Anda menentukan identitas UNIX atau Windows, semua operasi API S3 yang dilakukan melalui titik akses diotorisasi menggunakan izin pengguna tersebut pada sistem file.

Identitas sistem file yang Anda kaitkan dengan titik akses menentukan tingkat akses ke file dan direktori. Misalnya, jika Anda mengaitkan titik akses dengan identitas UNIX root (UID 0), yang biasanya memiliki izin akses file penuh pada sistem file, maka semua operasi file akan diotorisasi. Sebaliknya, jika Anda mengaitkan titik akses dengan identitas pengguna terbatas, operasi file akan terbatas pada apa yang dapat diakses pengguna berdasarkan model izin sistem file.

Anda harus menggunakan jenis identitas sistem file UNIX untuk volume dengan gaya keamanan UNIX dan tipe identitas Windows untuk volume dengan gaya keamanan NTFS. Penyelarasan ini memastikan bahwa model otorisasi cocok dengan konfigurasi keamanan volume.

Untuk volume gaya keamanan UNIX, sistem file menggunakan mode-bit atau NFSv4 ACLs untuk mengontrol akses. Untuk volume gaya keamanan NTFS, sistem file menggunakan Windows ACLs untuk mengontrol akses.

Important

Melampirkan titik akses S3 ke volume FSx untuk ONTAP tidak mengubah perilaku volume saat volume diakses langsung melalui NFS atau SMB. Semua operasi yang ada terhadap volume akan terus bekerja seperti sebelumnya. Pembatasan yang Anda sertakan dalam kebijakan jalur akses S3 hanya berlaku untuk permintaan yang dibuat menggunakan jalur akses.

Otorisasi permintaan API S3

Saat Anda membuat permintaan API S3 melalui titik akses yang dilampirkan ke volume NetApp ONTAP FSx untuk, Amazon S3 mengevaluasi izin IAM dari prinsipal panggilan terhadap kebijakan sumber daya IAM titik akses. Penelepon utama IAM harus memiliki izin yang diperlukan yang diberikan melalui kebijakan berbasis identitas mereka, dan kebijakan sumber daya jalur akses juga harus mengizinkan tindakan yang diminta.

Amazon S3 mengevaluasi semua kebijakan yang relevan—termasuk kebijakan pengguna, kebijakan titik akses, kebijakan titik akhir VPC, dan kebijakan kontrol layanan—untuk menentukan apakah akan mengizinkan permintaan tersebut.

Anda juga dapat mengonfigurasi titik akses S3 untuk hanya menerima permintaan dari virtual private cloud (VPC) tertentu untuk membatasi akses data. Untuk informasi selengkapnya, lihat [Membuat titik akses terbatas pada cloud privat virtual](#).

Blokir Akses Publik S3

Titik akses Amazon S3 yang dilampirkan ke volume ONTAP secara otomatis dikonfigurasi dengan akses publik blok diaktifkan, yang tidak dapat Anda ubah. FSx

Kebijakan jalur akses IAM

Kebijakan sumber daya dukungan jalur akses Amazon S3 AWS Identity and Access Management (IAM) yang memungkinkan Anda mengontrol penggunaan titik akses berdasarkan sumber daya, pengguna, atau kondisi lainnya. Agar aplikasi atau pengguna dapat mengakses objek melalui titik akses, baik titik akses dan sumber data yang mendasarinya harus mengizinkan permintaan tersebut.

`s3:PutAccessPointPolicy` izin diperlukan untuk membuat kebijakan jalur akses opsional.

Setelah Anda melampirkan jalur akses S3 ke FSx volume Amazon, semua operasi yang ada terhadap volume akan terus berfungsi seperti sebelumnya. Pembatasan yang Anda sertakan dalam kebijakan titik akses hanya berlaku untuk permintaan yang dibuat melalui titik akses tersebut. Untuk informasi selengkapnya, lihat [Mengonfigurasi kebijakan IAM untuk menggunakan titik akses](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Anda dapat mengonfigurasi kebijakan titik akses saat membuat titik akses yang dilampirkan ke volume FSx untuk ONTAP menggunakan FSx konsol Amazon. Untuk menambahkan, memodifikasi, atau menghapus kebijakan titik akses pada titik akses S3 yang ada, Anda dapat menggunakan konsol S3, CLI, atau API.

Membuat titik akses

Anda dapat membuat dan mengelola jalur akses S3 yang dilampirkan ke FSx volume Amazon menggunakan FSx konsol Amazon, CLI, API, dan didukung. SDKs

Note

Karena Anda mungkin ingin mempublikasikan nama jalur akses S3 Anda sehingga pengguna lain dapat menggunakan titik akses, hindari memasukkan informasi sensitif dalam nama jalur akses S3. Nama titik akses diterbitkan dalam basis data yang dapat diakses publik yang dikenal sebagai Sistem Nama Domain (DNS). Untuk informasi selengkapnya tentang nama titik akses, lihat [Aturan penamaan titik akses](#).

Izin yang diperlukan

Izin berikut diperlukan untuk membuat titik akses S3 yang dilampirkan ke volume Amazon FSx :

- `fsx:CreateAndAttachS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`

`s3:PutAccessPointPolicy` izin diperlukan untuk membuat kebijakan Access Point opsional menggunakan konsol Amazon FSx atau S3. Untuk informasi selengkapnya, lihat [Kebijakan jalur akses IAM](#).

Untuk membuat titik akses, lihat topik berikut ini.

Topik

- [Membuat titik akses](#)
- [Membuat titik akses terbatas pada cloud privat virtual](#)

Membuat titik akses

Important

Untuk melampirkan titik akses S3 ke volume ONTAP FSx untuk, volume harus dipasang (memiliki jalur persimpangan). Lihat [dokumentasi ONTAP](#) untuk detail selengkapnya.

Volume FSx untuk ONTAP harus sudah ada di akun Anda saat membuat titik akses S3 untuk volume Anda.

Untuk membuat titik akses S3 yang dilampirkan ke volume FSx untuk ONTAP, Anda menentukan properti berikut:

- Nama titik akses. Untuk informasi tentang aturan penamaan titik akses, lihat [Aturan penamaan titik akses](#).
- Identitas pengguna sistem file yang digunakan untuk mengotorisasi permintaan akses file yang dibuat menggunakan titik akses. Tentukan UNIX atau Windows nama pengguna POSIX yang ingin Anda sertakan. Untuk informasi selengkapnya, lihat [Identitas dan otorisasi pengguna sistem file](#).
- Konfigurasi jaringan titik akses menentukan apakah titik akses dapat diakses dari internet atau jika akses dibatasi ke virtual private cloud (VPC) tertentu. Untuk informasi selengkapnya, lihat [Membuat titik akses terbatas pada cloud privat virtual](#).

Untuk membuat titik akses S3 yang dilampirkan ke FSx volume (FSx konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di bilah navigasi di bagian atas halaman, pilih Wilayah AWS di mana Anda ingin membuat titik akses. Titik akses harus dibuat di Wilayah yang sama dengan volume terkait.
3. Di panel navigasi kiri, pilih Volume.
4. Pada halaman Volume, pilih volume ONTAP FSx untuk yang ingin Anda lampirkan titik akses.
5. Tampilkan halaman Create S3 access point dengan memilih Create S3 access point dari menu Actions.

6. Untuk nama titik akses, masukkan nama untuk titik akses. Untuk informasi selengkapnya tentang pedoman dan batasan untuk nama titik akses, lihat [Aturan penamaan titik akses](#).

Rincian sumber data diisi dengan informasi volume yang Anda pilih di Langkah 3.

7. Identitas pengguna sistem file digunakan oleh Amazon FSx untuk mengautentikasi permintaan akses file yang dibuat menggunakan titik akses ini. Pastikan bahwa pengguna sistem file yang Anda tentukan memiliki izin yang benar pada volume FSx untuk ONTAP.

Untuk tipe identitas pengguna sistem file, pilih UNIX atau Windows.

8. Untuk Nama Pengguna, masukkan nama pengguna.
9. Di panel konfigurasi Jaringan Anda memilih apakah titik akses dapat diakses dari Internet, atau akses dibatasi ke cloud pribadi virtual tertentu.

Untuk Network origin, pilih Internet untuk membuat jalur akses dapat diakses dari internet, atau pilih Virtual private cloud (VPC), dan masukkan ID VPC yang ingin Anda batasi akses ke titik akses.

Untuk informasi lebih lanjut tentang asal jaringan untuk titik akses, lihat [Membuat titik akses terbatas pada cloud privat virtual](#).

10. (Opsional) Di bawah Kebijakan Titik Akses - opsional, tentukan kebijakan jalur akses opsional. Pastikan untuk menyelesaikan peringatan, kesalahan, dan saran kebijakan apa pun. Untuk informasi selengkapnya tentang menentukan kebijakan jalur akses, lihat [Mengonfigurasi kebijakan IAM untuk menggunakan titik akses](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.
11. Pilih Buat titik akses untuk meninjau konfigurasi lampiran titik akses.

Untuk membuat titik akses S3 yang dilampirkan ke FSx volume (CLI)

Contoh perintah berikut membuat titik akses bernama *my-ontap-ap* yang dilampirkan ke volume FSx untuk ONTAP *fsvol-0123456789abcdef9* di akun *111122223333*.

```
$ aws fsx create-and-attach-s3-access-point --name my-ontap-ap --type ONTAP --ontap-configuration \
  VolumeId=fsvol-0123456789abcdef9,FileSystemIdentity='{Type=UNIX,UnixUser={Name=ec2-user}}' \
  --s3-access-point VpcConfiguration='{VpcId=vpc-0123467},Policy=access-point-policy-
json
```

Untuk permintaan yang berhasil, sistem merespons dengan mengembalikan lampiran titik akses S3 baru.

```
$ {
  {
    "S3AccessPointAttachment": {
      "CreationTime": 1728935791.8,
      "Lifecycle": "CREATING",
      "LifecycleTransitionReason": {
        "Message": "string"
      },
      "Name": "my-ontap-ap",
      "OntapConfiguration": {
        "VolumeId": "fsvol-0123456789abcdef9",
        "FileSystemIdentity": {
          "Type": "UNIX",
          "UnixUser": {
            "Name": "ec2-user"
          }
        }
      },
      "S3AccessPoint": {
        "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-ontap-ap",
        "Alias": "my-ontap-ap-aqfqprnstn7aefdfbarligizwggyfouse1a-ext-s3alias",
        "VpcConfiguration": {
          "VpcId": "vpc-0123467"
        }
      }
    }
  }
}
```

Membuat titik akses terbatas pada cloud privat virtual

Saat Anda membuat titik akses, Anda dapat memilih untuk membuat jalur akses dapat diakses dari internet, atau Anda dapat menentukan bahwa semua permintaan yang dibuat melalui jalur akses tersebut harus berasal dari Amazon Virtual Private Cloud tertentu. Titik akses yang dapat diakses dari internet dikatakan memiliki asal jaringan dari Internet. Ini dapat digunakan dari mana saja di internet, tunduk pada batasan akses lain yang berlaku untuk titik akses, bucket atau FSx volume Amazon yang mendasari, dan sumber daya terkait, seperti objek yang diminta. Jalur akses yang hanya dapat diakses dari VPC Amazon tertentu memiliki asal jaringan VPC, dan Amazon S3 menolak permintaan apa pun yang dibuat ke titik akses yang tidak berasal dari VPC Amazon itu.

⚠ Important

Anda hanya dapat menentukan asal jaringan titik akses saat membuat titik akses. Setelah membuat titik akses, Anda tidak dapat mengubah asal jaringannya.

Untuk membatasi jalur akses ke akses khusus Amazon VPC, Anda menyertakan `VpcConfiguration` parameter dengan permintaan untuk membuat titik akses. Dalam `VpcConfiguration` parameter, Anda menentukan ID VPC Amazon yang Anda inginkan untuk dapat menggunakan titik akses. Jika permintaan dibuat melalui jalur akses, permintaan harus berasal dari Amazon VPC atau Amazon S3 akan menolaknya.

Anda dapat mengambil asal jaringan titik akses menggunakan AWS CLI, AWS SDKs, atau REST APIs. Jika titik akses memiliki konfigurasi VPC Amazon yang ditentukan, asal jaringannya adalah VPC. Jika tidak, asal jaringan titik aksesnya adalah Internet.

Example

Contoh: Buat jalur akses yang dibatasi untuk akses VPC Amazon

Contoh berikut membuat titik akses bernama `example-vpc-ap` bucket `amzn-s3-demo-bucket` in account `123456789012` yang memungkinkan akses hanya dari `vpc-1a2b3c` VPC Amazon. Contoh tersebut kemudian memverifikasi bahwa titik akses yang baru memiliki asal jaringan VPC.

AWS CLI

```
$ aws fsx create-and-attach-s3-access-point --name example-vpc-ap --type ONTAP --
ontap-configuration \

  VolumeId=fsvol-0123456789abcdef9,FileSystemIdentity='{Type=UNIX,UnixUser={Name=ec2-
user}}}' \
  --s3-access-point VpcConfiguration='{VpcId=vpc-id},Policy=access-point-policy-
json'
```

```
$ {
  {
    "S3AccessPointAttachment": {
      "Lifecycle": "CREATING",
      "CreationTime": 1728935791.8,
      "Name": "example-vpc-ap",
```

```

    "OntapConfiguration": {
      "VolumeId": "fsvol-0123456789abcdef9",
      "FileSystemIdentity": {
        "Type": "UNIX",
        "UnixUser": {
          "Name": "my-unix-user"
        }
      }
    },
    "S3AccessPoint": {
      "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/example-
vpc-ap",
      "Alias": "access-point-abcdef0123456789ab12jj77xy51zacd4-ext-s3alias",
      "VpcConfiguration": {
        "VpcId": "vpc-1a2b3c"
      }
    }
  }
}

```

Untuk menggunakan titik akses dengan VPC Amazon, Anda harus mengubah kebijakan akses untuk titik akhir VPC Amazon Anda. Titik akhir Amazon VPC memungkinkan lalu lintas mengalir dari VPC Amazon Anda ke Amazon S3. Mereka memiliki kebijakan kontrol akses yang mengontrol bagaimana sumber daya dalam VPC Amazon diizinkan untuk berinteraksi dengan Amazon S3. Permintaan dari VPC Amazon Anda ke Amazon S3 hanya berhasil melalui titik akses jika kebijakan titik akhir VPC Amazon memberikan akses ke titik akses dan bucket yang mendasarinya.

Note

Agar sumber daya hanya dapat diakses dalam VPC Amazon, pastikan untuk membuat [zona host pribadi](#) untuk titik akhir VPC Amazon Anda. Untuk menggunakan zona yang dihosting pribadi, [ubah setelan VPC Amazon Anda](#) sehingga [atribut jaringan VPC](#) Amazon `enableDnsHostnames` dan `enableDnsSupport` disetel ke `true`

Contoh pernyataan kebijakan berikut mengonfigurasi titik akhir VPC Amazon untuk mengizinkan panggilan `GetObject` ke dan titik akses bernama `example-vpc-ap`

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Principal": "*",
      "Action": [
        "s3:GetObject"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:s3:us-east-1:123456789012:accesspoint/example-vpc-ap/object/*"
      ]
    }
  ]
}
```

Note

Pernyataan Resource di dalam contoh ini menggunakan Amazon Resource Name (ARN) untuk menentukan titik akses.

Untuk informasi selengkapnya tentang kebijakan titik akhir Amazon VPC, lihat Titik [akhir Gateway untuk Amazon S3 di](#) Panduan Pengguna Amazon VPC.

Mengelola titik akses Amazon S3

Bagian ini menjelaskan cara mengelola dan menggunakan jalur akses Amazon S3 Anda menggunakan Konsol Manajemen AWS, AWS Command Line Interface, atau API.

Topik

- [Daftar lampiran titik akses S3](#)
- [Melihat detail titik akses](#)
- [Menghapus lampiran titik akses S3](#)

Daftar lampiran titik akses S3

Bagian ini menjelaskan cara membuat daftar titik akses S3 menggunakan Konsol Manajemen AWS, AWS Command Line Interface, atau REST API.

Untuk mencantumkan semua titik akses S3 yang dilampirkan ke volume FSx untuk ONTAP (konsol Amazon FSx)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi di sisi kiri konsol, pilih Volume.
3. Pada halaman Volume, pilih volume ONTAP yang ingin Anda lihat lampiran titik akses.
4. Pada halaman Detail volume, pilih S3 untuk melihat daftar semua titik akses S3 yang dilampirkan pada volume.

Untuk mencantumkan semua titik akses S3 yang dilampirkan ke volume FSx untuk ONTAP ()AWS CLI

[describe-s3-access-point-attachments](#) Contoh perintah berikut menunjukkan bagaimana Anda dapat menggunakan AWS CLI untuk daftar lampiran titik akses S3.

Perintah berikut mencantumkan semua titik akses S3 yang dilampirkan ke volume pada sistem file FSx untuk ONTAP fs-0abcdef123456789.

```
aws fsx describe-s3-access-point-attachments --filter {[Name: file-system-id, Values:
{[fs-0abcdef123456789]}]}
```

Perintah berikut mencantumkan titik akses S3 yang dilampirkan ke volume ONTAP FSx vol-9abcdef123456789].

```
aws fsx describe-s3-access-point-attachments --filter {[Name: volume-id, Values:
{[vol-9abcdef123456789]}]}
```

Untuk informasi dan contoh selengkapnya, lihat [list-access-points](#) di AWS CLI Referensi Perintah.

Melihat detail titik akses

Bagian ini menjelaskan cara melihat detail titik akses S3 menggunakan Konsol Manajemen AWS, AWS Command Line Interface, atau REST API.

Untuk melihat detail titik akses S3 yang dilampirkan ke volume FSx untuk ONTAP (konsol Amazon FSx)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Arahkan ke volume yang dilampirkan ke titik akses yang detailnya ingin Anda lihat.
3. Pilih S3 untuk menampilkan daftar titik akses yang melekat pada volume.
4. Pilih titik akses yang detailnya ingin Anda lihat.
5. Di bawah ringkasan lampiran titik akses S3, lihat detail konfigurasi dan properti untuk titik akses yang dipilih.

Konfigurasi identitas pengguna sistem File dan kebijakan izin titik akses S3 juga terdaftar untuk lampiran titik akses.

6. Untuk melihat konfigurasi S3 titik akses di konsol Amazon S3, pilih nama titik akses S3 yang ditampilkan di bawah titik akses S3. Ini membawa Anda ke halaman detail titik akses di konsol Amazon S3.

Menghapus lampiran titik akses S3

Bagian ini menjelaskan cara menghapus titik akses S3 menggunakan Konsol Manajemen AWS, AWS Command Line Interface, atau REST API.

`s3control:DeleteAccessPointIn fsx:DetachAndDeleteS3AccessPoint` dan diperlukan untuk menghapus lampiran titik akses S3.

Untuk menghapus titik akses S3 yang dilampirkan ke volume FSx untuk ONTAP (konsol Amazon FSx)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Arahkan ke volume yang dilampirkan lampiran titik akses S3 yang ingin Anda hapus.
3. Pilih S3 untuk menampilkan daftar titik akses S3 yang melekat pada volume.
4. Pilih lampiran titik akses S3 yang ingin Anda hapus.
5. Pilih Hapus.
6. Konfirmasikan bahwa Anda ingin menghapus titik akses S3, dan pilih Hapus.

Untuk menghapus titik akses S3 yang dilampirkan ke volume FSx untuk ONTAP ()AWS CLI

- Untuk menghapus lampiran titik akses S3, gunakan perintah CLI [detach-and-delete-s3-access-point](#) (atau operasi API AccessPoint S3 yang [DetachAndDeleteSetara](#)), seperti yang ditunjukkan pada contoh berikut. Gunakan `--name` properti untuk menentukan nama lampiran titik akses S3 yang ingin Anda hapus.

```
aws fsx detach-and-delete-s3-access-point \  
  --region us-east-1 \  
  --name my-ontap-ap
```

Menggunakan titik akses

Contoh berikut menunjukkan cara menggunakan titik akses untuk mengakses data file yang disimpan pada volume FSx untuk ONTAP menggunakan API S3. Untuk daftar lengkap operasi Amazon S3 API yang didukung oleh titik akses yang dilampirkan ke volume ONTAP, lihat. FSx [Kompatibilitas titik akses](#)

Note

File FSx untuk volume ONTAP diidentifikasi dengan `fileStorageClass.FSX_ONTAP`

Topik

- [Mengunduh file menggunakan titik akses S3](#)
- [Mengunggah file menggunakan titik akses S3](#)
- [Daftar file menggunakan titik akses S3](#)
- [Menandai file menggunakan titik akses S3](#)
- [Menghapus file menggunakan titik akses S3](#)

Mengunduh file menggunakan titik akses S3

`get-object` Contoh perintah berikut menunjukkan bagaimana Anda dapat menggunakan AWS CLI untuk men-download file melalui titik akses. Anda harus menyertakan outfile, yang merupakan nama file untuk objek yang diunduh.

Contoh meminta file *my-image.jpg* melalui titik akses *my-ontap-ap* dan menyimpan file yang diunduh sebagai file *download.jpg*.

```
$ aws s3api get-object --key my-image.jpg --bucket my-ontap-ap-  
hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias download.jpg  
{  
  "AcceptRanges": "bytes",  
  "LastModified": "Mon, 14 Oct 2024 17:01:48 GMT",  
  "ContentLength": 141756,  
  "ETag": "\"00751974dc146b76404bb7290f8f51bb-1\"",  
  "ContentType": "binary/octet-stream",  
  "ServerSideEncryption": "SSE_FSX",  
  "Metadata": {},  
  "StorageClass": "FSX_ONTAP"  
}
```

Anda juga dapat menggunakan REST API untuk mengunduh objek melalui titik akses. Untuk informasi selengkapnya, lihat [GetObject](#) dalam Referensi API Amazon Simple Storage Service.

Mengunggah file menggunakan titik akses S3

`put-object` Contoh perintah berikut menunjukkan bagaimana Anda dapat menggunakan AWS CLI untuk meng-upload file melalui titik akses. Anda harus menyertakan outfile, yang merupakan nama file untuk objek yang diunggah.

Contoh mengunggah file *my-new-image.jpg* melalui titik akses *my-ontap-ap* dan menyimpan file yang diunggah sebagai file *my-new-image.jpg*

```
$ aws s3api put-object --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-  
s3alias --key my-new-image.jpg --body my-new-image.jpg
```

Anda juga dapat menggunakan REST API untuk mengunggah objek melalui titik akses. Untuk informasi selengkapnya, lihat [PutObject](#) dalam Referensi API Amazon Simple Storage Service.

Daftar file menggunakan titik akses S3

Contoh berikut mencantumkan file melalui alias access point yang *my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias* dimiliki oleh ID akun *111122223333* di Region *us-east-2*.

```
$ aws s3api list-objects-v2 --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias
{
  "Contents": [
    {
      "Key": ".hidden-dir-with-data/file.txt",
      "LastModified": "2024-10-29T14:22:05.4359",
      "ETag": "\"88990077ab44cd55ef66aa77-1\"",
      "Size": 18,
      "StorageClass": "FSX_ONTAP"
    },
    {
      "Key": "documents/report.rtf",
      "LastModified": "2024-11-02T10:18:15.6621",
      "ETag": "\"ab12cd34ef56a89219zg6aa77-1\"",
      "Size": 1048576,
      "StorageClass": "FSX_ONTAP"
    }
  ]
}
```

Anda juga dapat menggunakan REST API untuk membuat daftar file Anda. Untuk informasi selengkapnya, lihat [ListObjectsV2](#) dalam Referensi API Amazon Simple Storage Service.

Menandai file menggunakan titik akses S3

put-object-tagging Contoh perintah berikut menunjukkan bagaimana Anda dapat menggunakan AWS CLI untuk menambahkan tag-set melalui titik akses. Setiap tag adalah pasangan nilai kunci. Untuk informasi selengkapnya, lihat [Mengategorikan penyimpanan menggunakan tag](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Contoh menambahkan tag-set ke file yang ada `my-image.jpg` menggunakan titik akses. **my-ontap-ap**

```
$ aws s3api put-object-tagging --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias --key my-image.jpg --tagging TagSet=[{Key="finance",Value="true"}]
```

Anda juga dapat menggunakan REST API untuk menambahkan tag-set ke objek melalui titik akses. Untuk informasi selengkapnya, lihat [PutObjectTagging](#) dalam Referensi API Amazon Simple Storage Service.

Menghapus file menggunakan titik akses S3

`delete-object` Contoh perintah berikut menunjukkan bagaimana Anda dapat menggunakan AWS CLI untuk menghapus file melalui titik akses.

```
$ aws s3api delete-object --bucket my-ontap-ap-hrzrLukc5m36ft7okagglf3gmwLuquse1b-ext-s3alias --key my-image.jpg
```

Anda juga dapat menggunakan REST API untuk menghapus objek melalui titik akses. Untuk informasi selengkapnya, lihat [DeleteObject](#) dalam Referensi API Amazon Simple Storage Service.

Memecahkan masalah titik akses S3

Bagian ini menjelaskan gejala, penyebab, dan resolusi ketika Anda mengalami masalah saat mengakses FSx data Anda dari titik akses S3.

Pembuatan jalur akses S3 gagal karena kegagalan pencarian identitas pengguna sistem file

Saat membuat dan melampirkan Titik Akses S3, a [FileSystemIdentity](#) harus disediakan. Anda bertanggung jawab untuk mengonfigurasi pengguna UNIX atau Windows yang disediakan dalam ONTAP.

Jika a [UnixUser](#) disediakan, ONTAP harus dapat memetakan UnixUser nama ke UNIX UID/. GIDs ONTAP menentukan cara melakukan pemetaan ini menggunakan konfigurasi [sakelar layanan nama](#).

```
> vservers services name-service ns-switch show
```

Vserver	Database	Order
svm_1	hosts	files, dns
svm_1	group	files, ldap
svm_1	passwd	files, ldap
svm_1	netgroup	nis, files

Pastikan Anda UnixUser memiliki entri di group database passwd dan menggunakan sumber yang valid (files,ldap, dll). filesSumber dapat dikonfigurasi menggunakan `vserver services name-service unix-group` perintah `vserver services name-service unix-user` and. ldapSumber dapat dikonfigurasi menggunakan `vserver services name-service ldap` perintah.

Jika a [WindowsUser](#) disediakan, ONTAP harus dapat menemukan WindowsUser nama di domain Active Directory yang bergabung.

Untuk mengonfirmasi apakah disediakan UnixUser atau WindowsUser dipetakan dengan benar, menggunakan fsxadmin Anda dapat menggunakan perintah berikut (ganti `-unix-user-name` dengan `-win-name` for WindowsUsers):

```
> vserver services access-check authentication show-creds -  
node FsxId0fd48ff588b9d3eee-01 -vserver svm_name -unix-user-name root -show-partial-  
unix-creds true
```

Contoh output yang berhasil:

```
UNIX UID: root  
  
GID: daemon  
Supplementary GIDs:  
daemon
```

Contoh output yang tidak berhasil:

```
Error: Acquire UNIX credentials procedure failed  
[ 2 ms] Entry for user-name: unmapped-user not found in the  
        current source: FILES. Entry for user-name: unmapped-user  
        not found in any of the available sources  
**[    3] FAILURE: Unable to retrieve UID for UNIX user  
**      unmapped-user  
  
Error: command failed: Failed to resolve user name to a UNIX ID. Reason: "SecD Error:  
object not found".
```

Pemetaan pengguna yang salah dapat mengakibatkan Access Denied kesalahan dari S3. Lihat contoh alasan kegagalan di bawah ini.

Entry for user-name not found in the current source: LDAP

Jika Anda ns-switch dikonfigurasi untuk menggunakan ldap sumber, pastikan ONTAP dikonfigurasi untuk menggunakan server LDAP Anda dengan benar. Lihat [NetAppLaporan Teknis untuk mengonfigurasi LDAP](#) untuk informasi selengkapnya.

RESULT_ERROR_DNS_CANT_REACH_SERVER atau RESULT_ERROR_SECD_IN_DISCOVERY

Kesalahan ini menunjukkan masalah dengan konfigurasi DNS vserver di ONTAP. Jalankan yang berikut ini untuk memastikan DNS vserver Anda dikonfigurasi dengan benar:

```
> dns check -vserver svm_name
```

Pembuatan titik akses S3 gagal karena volume tidak dipasang.

Titik akses S3 hanya dapat dilampirkan FSx untuk volume ONTAP yang dipasang (memiliki jalur persimpangan). Ini juga berlaku untuk jenis volume DP (Perlindungan Data). Lihat [dokumentasi pemasangan volume ONTAP](#) untuk informasi selengkapnya.

Sistem file tidak dapat menangani permintaan S3

Jika volume permintaan S3 untuk beban kerja tertentu melebihi kapasitas sistem file untuk menangani lalu lintas, Anda mungkin mengalami kesalahan permintaan S3 (misalnya, Internal Server Error503 Slow Down, dan). Service Unavailable Anda dapat secara proaktif memantau dan alarm kinerja sistem file Anda menggunakan CloudWatch metrik Amazon (misalnya, Network throughput utilization danCPU utilization). Jika Anda mengamati kinerja yang menurun, Anda dapat mengatasi masalah ini dengan meningkatkan kapasitas throughput sistem file.

Akses Ditolak dengan izin titik akses S3 default untuk peran layanan yang dibuat secara otomatis

Beberapa AWS layanan terintegrasi S3 akan membuat peran layanan khusus dan menyesuaikan izin terlampir ke kasus penggunaan spesifik Anda. Saat menentukan alias titik akses S3 Anda sebagai sumber daya S3, izin terlampir tersebut mungkin menyertakan titik akses Anda menggunakan format ARN bucket (misalnya,) `arn:aws:s3:::my-fsx-ap-foo7detztxouyjpwtu8krroppytruse1a-ext-s3alias` daripada format ARN titik akses (misalnya,) `arn:aws:s3:us-east-1:1234567890:accesspoint/my-fsx-ap` Untuk mengatasi hal ini, ubah kebijakan untuk menggunakan ARN dari titik akses.

Mengakses data dari layanan lain AWS

Selain Amazon EC2, Anda dapat menggunakan AWS layanan lain dengan volume Anda untuk mengakses data Anda.

Topik

- [Menggunakan Amazon WorkSpaces dengan FSx untuk ONTAP](#)
- [Menggunakan Amazon Elastic Container Service dengan FSx untuk ONTAP](#)
- [Menggunakan Amazon Elastic VMware Service dengan FSx untuk ONTAP](#)
- [Menggunakan VMware Cloud dengan FSx untuk ONTAP](#)

Menggunakan Amazon WorkSpaces dengan FSx untuk ONTAP

FSx untuk ONTAP dapat digunakan dengan Amazon WorkSpaces untuk menyediakan penyimpanan terlampir jaringan bersama (NAS) atau untuk menyimpan profil roaming untuk akun Amazon. WorkSpaces Setelah menghubungkan ke berbagi file SMB dengan sebuah WorkSpaces instance, pengguna dapat membuat dan mengedit file pada berbagi file.

Prosedur berikut menunjukkan cara menggunakan Amazon FSx dengan Amazon WorkSpaces untuk memberikan profil roaming dan akses folder rumah pengalaman yang konsisten dan untuk menyediakan folder tim bersama untuk WorkSpaces pengguna Windows dan Linux. Jika Anda baru mengenal Amazon WorkSpaces, Anda dapat membuat WorkSpaces lingkungan Amazon pertama Anda dengan petunjuk di [Memulai dengan Pengaturan WorkSpaces Cepat](#) di Panduan WorkSpaces Administrasi Amazon.

Topik

- [Berikan dukungan Profil Roaming](#)
- [Menyediakan folder bersama untuk mengakses file umum](#)

Berikan dukungan Profil Roaming

Anda dapat menggunakan Amazon FSx untuk memberikan dukungan Profil Roaming kepada pengguna di organisasi Anda. Seorang pengguna akan memiliki izin untuk hanya mengakses Profil Roaming mereka. Folder akan terhubung secara otomatis menggunakan Kebijakan Grup Direktori Aktif. Dengan Profil Roaming, data pengguna dan pengaturan desktop disimpan saat mereka keluar dari berbagi FSx file Amazon yang memungkinkan dokumen dan pengaturan untuk dibagikan

di antara WorkSpaces instans yang berbeda, dan secara otomatis dicadangkan menggunakan cadangan otomatis harian Amazon FSx .

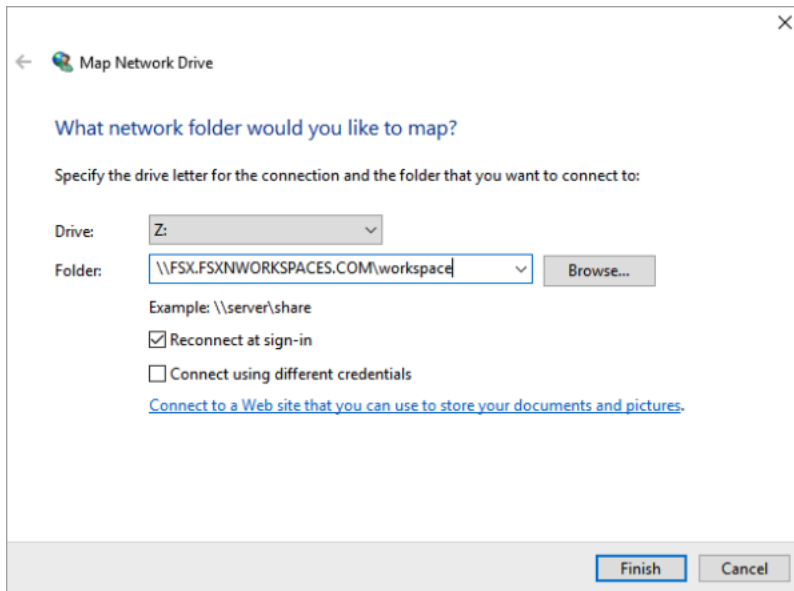
Langkah 1: Buat lokasi folder profil untuk pengguna domain yang menggunakan Amazon FSx

1. Buat sistem file FSx untuk ONTAP menggunakan FSx konsol Amazon. Untuk informasi selengkapnya, lihat [Untuk membuat sistem file \(konsol\)](#).

 Important

Masing-masing FSx untuk sistem file ONTAP memiliki rentang alamat IP titik akhir dari mana titik akhir yang terkait dengan sistem file dibuat. Untuk sistem file multi-AZ, FSx untuk ONTAP memilih rentang alamat IP default yang tidak digunakan dari 198.19.0.0/16 sebagai rentang alamat IP titik akhir. Rentang alamat IP ini juga digunakan oleh WorkSpaces untuk rentang lalu lintas manajemen, seperti yang dijelaskan dalam [alamat IP dan persyaratan port untuk WorkSpaces](#) dalam Panduan WorkSpaces Administrasi Amazon. Akibatnya, untuk mengakses sistem file Multi-AZ FSx untuk ONTAP WorkSpaces, Anda harus memilih rentang alamat IP titik akhir yang tidak tumpang tindih dengan 198.19.0.0/16.

2. Jika Anda tidak memiliki mesin virtual penyimpanan (SVM) yang bergabung dengan Active Directory, buat sekarang. Misalnya, Anda dapat menyediakan SVM bernama `fsx` dan mengatur gaya keamanan keNTFS. Untuk informasi selengkapnya, lihat [Untuk membuat penyimpanan mesin virtual \(konsol\)](#).
3. Buat volume untuk SVM Anda. Misalnya, Anda dapat membuat volume bernama `fsx-vol` yang mewarisi gaya keamanan volume root SVM Anda. Untuk informasi selengkapnya, lihat [Untuk membuat FlexVol volume \(konsol\)](#).
4. Buat berbagi SMB pada volume Anda. Misalnya, Anda dapat membuat share yang dipanggil `workspace` pada volume Anda bernama `fsx-vol`, di mana Anda membuat folder bernama `profiles`. Untuk informasi selengkapnya, lihat [Mengelola saham SMB](#).
5. Akses Amazon FSx SVM Anda dari EC2 instans Amazon yang menjalankan Windows Server atau dari file. Workspace Untuk informasi selengkapnya, lihat [Mengakses data FSx ONTAP Anda](#).
6. Anda memetakan bagian Anda ke `Z:\WorkSpaces` instans Windows Anda:



Langkah 2: FSx Tautkan berbagi file ONTAP ke Akun Pengguna

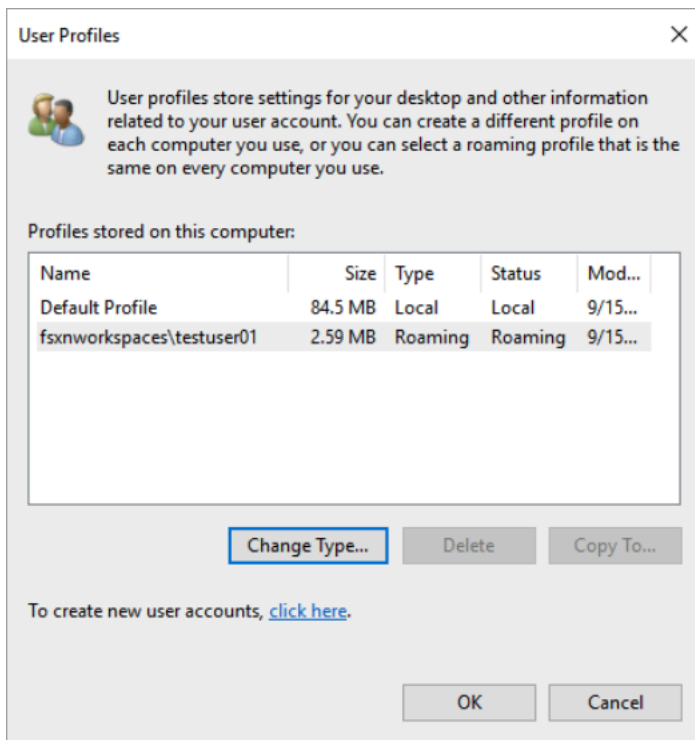
1. Pada pengguna pengujian Anda Workspace, pilih Windows > System > Advanced System Settings.
2. Di System Properties, pilih tab Advanced dan tekan tombol Pengaturan di bagian Profil Pengguna. Pengguna yang masuk akan memiliki tipe profil. Local
3. Keluar dari pengguna uji dari file Workspace.
4. Atur pengguna uji agar profil roaming berada di sistem FSx file Amazon Anda. Di administrator Anda WorkSpaces, buka PowerShell konsol dan gunakan perintah yang mirip dengan contoh berikut (yang menggunakan profiles folder yang sebelumnya Anda buat di Langkah 1):

```
Set-ADUser username -ProfilePath \\filesystem-dns-name\\sharename\\foldername\\username
```

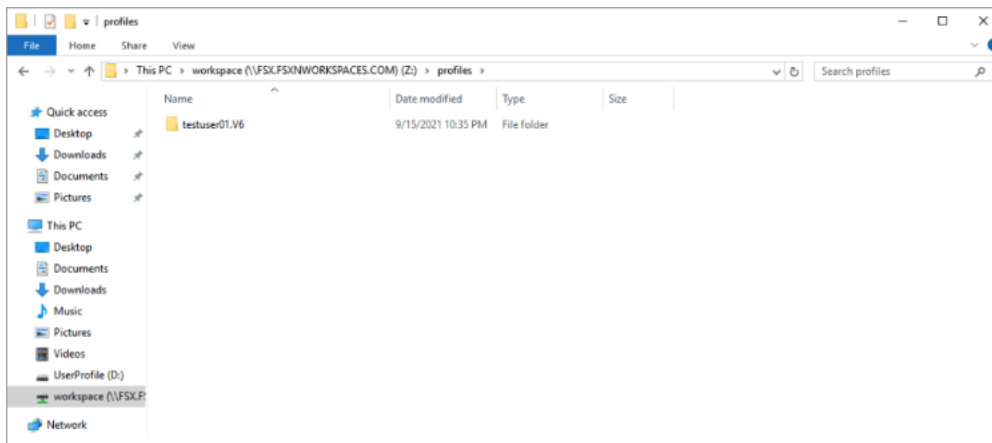
Sebagai contoh:

```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxworkspaces.com\\workspace\\profiles\\testuser01
```

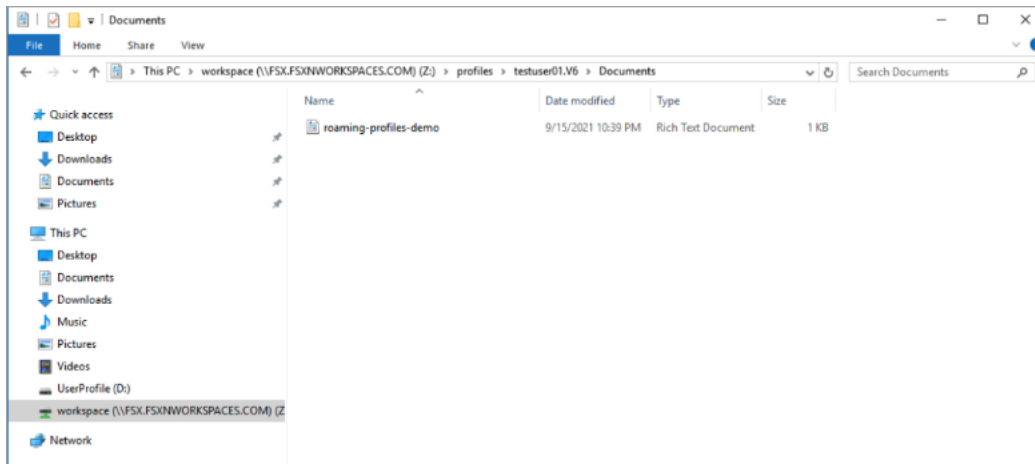
5. Masuk ke pengguna uji Workspace.
6. Di System Properties, pilih tab Advanced dan tekan tombol Pengaturan di bagian Profil Pengguna. Pengguna yang masuk akan memiliki tipe profil. Roaming



7. Jelajahi folder bersama ONTAP FSx untuk. Di profiles folder, Anda akan melihat folder untuk pengguna.



8. Buat dokumen di Documents folder pengguna uji
9. Keluar dari pengguna uji dari mereka WorkSpace.
10. Jika Anda masuk kembali sebagai pengguna uji dan menjelajah ke toko profil mereka, Anda akan melihat dokumen yang Anda buat.

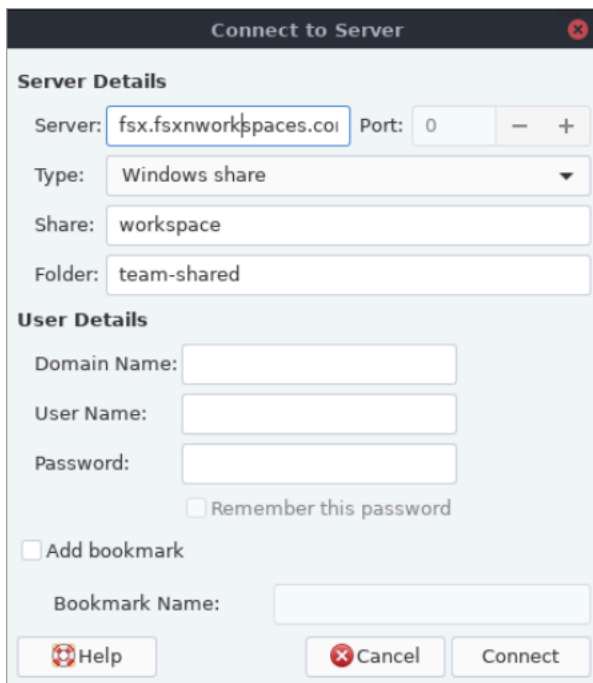


Menyediakan folder bersama untuk mengakses file umum

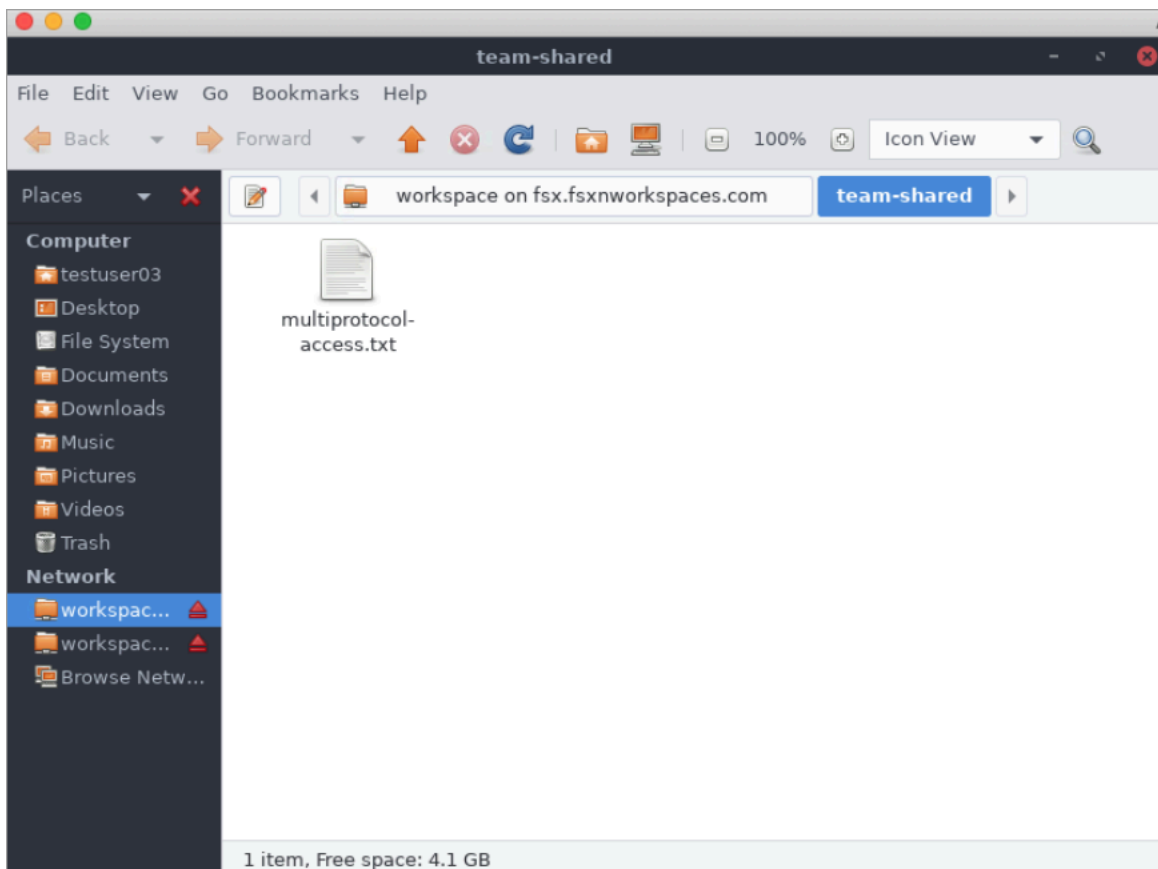
Anda dapat menggunakan Amazon FSx untuk menyediakan folder bersama kepada pengguna di organisasi Anda. Folder bersama dapat digunakan untuk menyimpan file yang digunakan oleh komunitas pengguna Anda, seperti file demo, contoh kode, dan instruksi manual yang dibutuhkan oleh semua pengguna. Biasanya, Anda memiliki drive yang dipetakan untuk folder bersama; Namun karena drive yang dipetakan menggunakan huruf, ada batasan jumlah saham yang dapat Anda miliki. Prosedur ini membuat folder FSx bersama Amazon yang tersedia tanpa huruf drive, memberi Anda fleksibilitas yang lebih besar dalam menetapkan pembagian ke tim.

Untuk memasang folder bersama untuk akses lintas platform dari Linux dan Windows WorkSpaces

1. Dari Taskbar, pilih Places > Connect to Server.
 - a. Untuk Server, masukkan *file-system-dns-name*.
 - b. Atur Type ke Windows share.
 - c. Setel Bagikan ke nama berbagi SMB, seperti *workspace*.
 - d. Anda dapat meninggalkan Folder sebagai / atau mengaturnya ke folder, seperti folder bernama *team-shared*.
 - e. Untuk Linux WorkSpace, Anda tidak perlu memasukkan detail pengguna jika Linux Anda WorkSpace berada di domain yang sama dengan Amazon FSx share.
 - f. Pilih Hubungkan.



2. Setelah koneksi dibuat, Anda dapat melihat folder bersama (dinamai team-shared dalam contoh ini) di berbagi SMB bernama workspace.



Menggunakan Amazon Elastic Container Service dengan FSx untuk ONTAP

Anda dapat mengakses sistem file Amazon FSx untuk NetApp ONTAP dari wadah Amazon Elastic Container Service (Amazon ECS) Docker Container Service (Amazon ECS) di instans Amazon EC2 Linux atau Windows.

Memasang pada wadah Amazon ECS Linux

1. Buat cluster ECS menggunakan template cluster EC2 Linux + Networking untuk wadah Linux Anda. Untuk informasi selengkapnya, lihat [Membuat klaster](#) di Panduan Pengembang Layanan Amazon Elastic Container.
2. Buat direktori pada EC2 instance untuk memasang volume SVM sebagai berikut:

```
sudo mkdir /fsxontap
```

3. Pasang volume ONTAP Anda FSx pada EC2 instance Linux dengan menggunakan skrip data pengguna selama peluncuran instance, atau dengan menjalankan perintah berikut:

```
sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
```

4. Pasang volume menggunakan perintah berikut:

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /  
fsxontap
```

Contoh berikut menggunakan nilai sampel.

```
sudo mount -t nfs -o nfsvers=4.1  
svm-01234567890abcdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /  
fsxontap
```

Anda juga dapat menggunakan alamat IP SVM alih-alih nama DNS-nya.

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. Saat membuat definisi tugas Amazon ECS, tambahkan properti berikut `volumes` dan `mountPoints` container dalam definisi container JSON. Ganti `sourcePath` dengan titik pemasangan dan direktori di FSx untuk sistem file ONTAP Anda.

```
{
  "volumes": [
    {
      "name": "ontap-volume",
      "host": {
        "sourcePath": "mountpoint"
      }
    }
  ],
  "mountPoints": [
    {
      "containerPath": "containermountpoint",
      "sourceVolume": "ontap-volume"
    }
  ],
  .
  .
  .
}
```

Memasang pada wadah Amazon ECS Windows

1. Buat cluster ECS menggunakan template cluster EC2 Windows+Networking untuk wadah Windows Anda. Untuk informasi selengkapnya, lihat [Membuat klaster](#) di Panduan Pengembang Layanan Amazon Elastic Container.
2. Tambahkan EC2 instance Windows yang bergabung dengan domain ke cluster ECS Windows dan petakan berbagi SMB.

Luncurkan EC2 instance Windows yang dioptimalkan ECS yang digabungkan ke domain Active Directory Anda dan inisialisasi agen ECS dengan menjalankan perintah berikut.

```
PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
EnableTaskIAMRole
```

Anda juga dapat meneruskan informasi dalam skrip ke bidang teks data pengguna sebagai berikut.

```
<powershell>
Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
```



```
</powershell>
```

3. Buat pemetaan global SMB pada EC2 instance sehingga Anda dapat memetakan berbagi SMB Anda ke drive. Ganti nilai di bawah netbios atau nama DNS untuk sistem FSx file Anda dan bagikan nama. Volume NFS vol1 yang dipasang pada EC2 instance Linux dikonfigurasi sebagai fsxontap berbagi CIFS pada sistem file. FSx

```
vserver cifs share show -vserver svm08 -share-name fsxontap
```

```

Vserver: svm08
Share: fsxontap
CIFS Server NetBIOS Name: FSXONTAPDEMO
Path: /vol1
Share Properties: oplocks
                  browsable
                  changenotify
                  show-previous-versions
Symlink Properties: symlinks
File Mode Creation Mask: -
Directory Mode Creation Mask: -
Share Comment: -
Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
Volume Name: vol1
Offline Files: manual
Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
UNIX Group for File Create: -
```

4. Buat pemetaan global SMB pada EC2 instance menggunakan perintah berikut:

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. Saat membuat definisi tugas Amazon ECS, tambahkan properti berikut volumes dan mountPoints container dalam definisi container JSON. Ganti sourcePath dengan titik pemasangan dan direktori di FSx untuk sistem file ONTAP Anda.

```
{
  "volumes": [
    {
      "name": "ontap-volume",
```

```
        "host": {
            "sourcePath": "mountpoint"
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Menggunakan Amazon Elastic VMware Service dengan FSx untuk ONTAP

Anda dapat menggunakan FSx ONTAP sebagai datastore eksternal untuk Amazon Elastic Service VMware (Amazon EVS) Software-Defined Data Center (). SDDCs Untuk informasi selengkapnya, lihat [Menjalankan beban kerja berkinerja tinggi dengan Amazon FSx untuk NetApp ONTAP](#). Untuk petunjuk terperinci, lihat [Mengonfigurasi Amazon FSx untuk NetApp ONTAP sebagai datastore NFS](#) dan [Mengonfigurasi Amazon FSx untuk NetApp ONTAP sebagai datastore iSCSI](#).

Menggunakan VMware Cloud dengan FSx untuk ONTAP

Anda dapat menggunakan FSx ONTAP sebagai datastore eksternal untuk VMware Cloud pada Pusat Data yang Ditetapkan AWS Perangkat Lunak (). SDDCs Untuk informasi selengkapnya, lihat [Mengonfigurasi Amazon FSx untuk NetApp ONTAP sebagai Penyimpanan Eksternal](#) dan [VMware Cloud AWS dengan Amazon FSx untuk Panduan Penerapan NetApp ONTAP](#).

Opsi ketersediaan, daya tahan, dan penerapan

Amazon FSx untuk NetApp ONTAP menggunakan tipe penerapan Single-AZ dan Multi-AZ. Anda dapat memilih dari empat opsi: Single-AZ 1, Single-AZ 2, Multi-AZ 1, dan Multi-AZ 2. Topik ini menjelaskan fitur ketersediaan dan daya tahan dari setiap jenis penerapan untuk membantu Anda memilih salah satu yang tepat untuk beban kerja Anda. Untuk informasi tentang ketersediaan layanan SLA (Perjanjian Tingkat Layanan), lihat [Perjanjian Tingkat FSx Layanan Amazon](#).

Topik

- [Memilih jenis penyebaran sistem file](#)
- [Memilih pembuatan sistem file](#)
- [Proses failover FSx untuk ONTAP](#)
- [Sumber daya jaringan](#)

Memilih jenis penyebaran sistem file

Fitur ketersediaan dan daya tahan tipe penyebaran sistem file Single-AZ dan Multi-AZ dijelaskan di bagian berikut.

Jenis penyebaran AZ tunggal

Anda dapat memilih antara Single-AZ 1 dan Single-AZ 2 untuk sistem file Single-AZ Anda. Single-AZ 1 adalah sistem file generasi pertama dengan satu pasangan ketersediaan tinggi (HA), sedangkan Single-AZ 2 adalah sistem file generasi kedua dengan 1—12 pasangan HA. Untuk informasi selengkapnya, lihat [Memilih pembuatan sistem file](#).

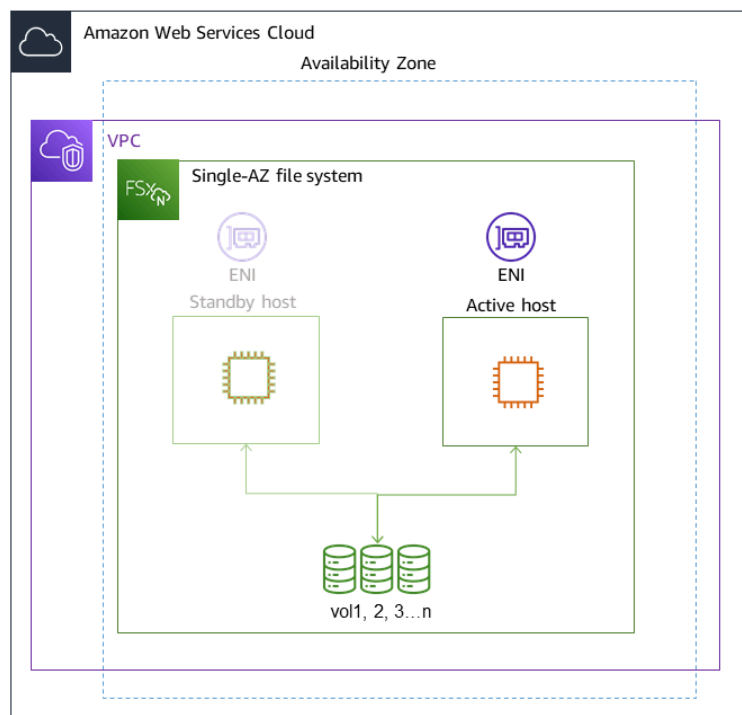
Saat Anda membuat sistem file Single-AZ, Amazon FSx secara otomatis menyediakan satu hingga dua belas pasang server file dalam konfigurasi siaga aktif, dengan server file aktif dan siaga di setiap pasangan yang terletak di domain kesalahan terpisah dalam satu Availability Zone di file. Wilayah AWS Selama pemeliharaan sistem file yang direncanakan atau gangguan layanan yang tidak direncanakan dari server file aktif apa pun, Amazon FSx secara otomatis dan independen gagal atas pasangan ketersediaan tinggi (HA) ke server file siaga, biasanya dalam beberapa detik. Selama failover, Anda terus memiliki akses ke data Anda tanpa intervensi manual.

Untuk memastikan ketersediaan yang tinggi, Amazon FSx terus memantau kegagalan perangkat keras, dan secara otomatis mengganti komponen infrastruktur jika terjadi kegagalan. Untuk mencapai daya tahan tinggi, Amazon FSx secara otomatis mereplikasi data Anda dalam Availability Zone

untuk melindunginya dari kegagalan komponen. Selain itu, Anda memiliki opsi untuk mengonfigurasi pencadangan harian otomatis dari data sistem file Anda. Pencadangan ini disimpan di beberapa Availability Zone untuk memberikan ketahanan Multi-AZ untuk semua data cadangan.

Sistem file single-AZ dirancang untuk kasus penggunaan yang tidak memerlukan model ketahanan data dari sistem file Multi-AZ. Mereka menyediakan solusi yang dioptimalkan biaya untuk kasus penggunaan seperti lingkungan pengembangan dan pengujian, atau menyimpan salinan sekunder data yang sudah disimpan di tempat atau di tempat lain Wilayah AWS, dengan hanya mereplikasi data dalam satu Availability Zone.

Diagram berikut menggambarkan arsitektur untuk sistem file generasi pertama ONTAP Single-AZ. FSx



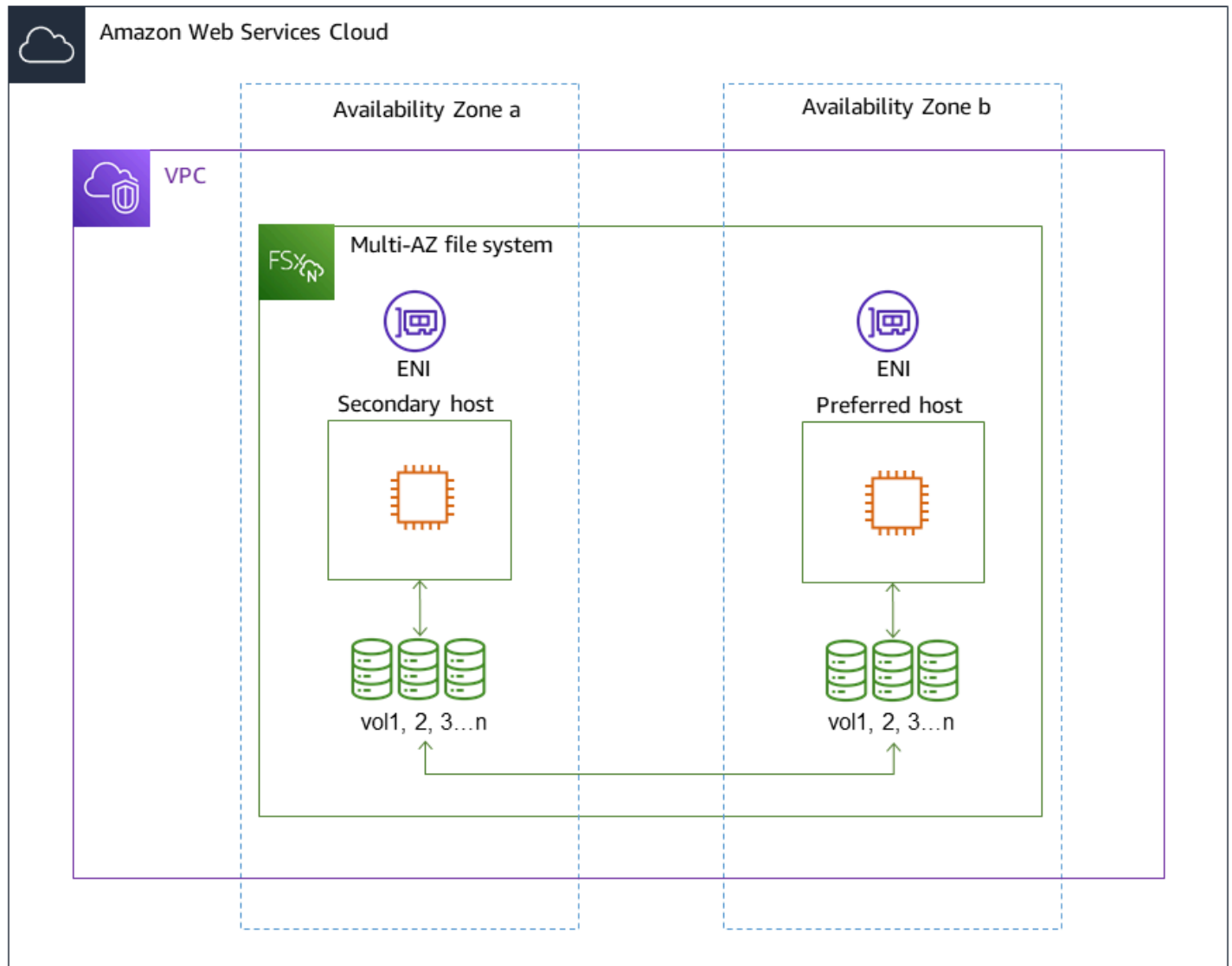
Jenis penyebaran multi-AZ

Anda dapat memilih antara Multi-AZ 1 dan Multi-AZ 2 untuk sistem file Multi-AZ Anda. Multi-AZ 1 adalah sistem file generasi pertama dan Multi-AZ 2 adalah sistem file generasi kedua. Kedua opsi memiliki satu pasangan HA. Untuk informasi selengkapnya, lihat [Memilih pembuatan sistem file](#).

Sistem file Multi-AZ mendukung semua fitur ketersediaan dan daya tahan sistem file Single-AZ. Selain itu, mereka dirancang untuk menyediakan ketersediaan data yang berkelanjutan bahkan

ketika Availability Zone tidak tersedia. Penerapan multi-AZ memiliki sepasang HA tunggal server file, server file siaga digunakan di Availability Zone yang berbeda dari server file aktif yang sama. Wilayah AWS Setiap perubahan yang ditulis ke sistem file Anda direplikasi secara sinkron di seluruh Availability Zones ke standby.

Sistem file multi-AZ dirancang untuk kasus penggunaan seperti beban kerja produksi penting bisnis yang memerlukan ketersediaan tinggi untuk data file ONTAP bersama dan membutuhkan penyimpanan dengan replikasi bawaan di seluruh Availability Zone. Diagram berikut menggambarkan arsitektur untuk sistem file generasi pertama ONTAP Multi-AZ. FSx



Memilih pembuatan sistem file

Tabel berikut menggambarkan perbedaan antara generasi pertama dan kedua Single-AZ dan FSx Multi-AZ untuk sistem file ONTAP.

FSx untuk generasi sistem file ONTAP

Dimensi	Generasi pertama	Generasi kedua (pasangan HA tunggal)	Generasi kedua (multi-pasangan)
Jenis deployment	TUNGKAL_AZ_1 MULTI_AZ_1	SINGLE_AZ_2 MULTI_AZ_2	SINGLE_AZ_2
Pasangan HA	1 pasangan HA		1—12 pasangan HA
Penyimpanan SSD	Minimal: 1 TiB Maksimal: 192 TiB	Minimal: 1 TiB Maksimal: 512 TiB	Minimum: 1 TiB (per pasangan HA) Maksimum: 1 PiB (total)
SSD IOPS	Minimal: 3 IOPS/GIB SSD Maksimal: 160.000	Minimal: 3 IOPS/GIB SSD Maksimal: 200.000	Minimal: 3 IOPS/GIB SSD Maksimum: 2.400.000 (200.000 per pasangan HA)
Kapasitas throughput	128 MBps; 256; 512 MBps; 1.024 MBps; 2.048 MBps; 4.096 MBps MBps	384 MBps; 768; 1.536 MBps; 3.072 MBps; 6.144 MBps MBps	1.536 MBps (per pasangan HA); 3.072 MBps (per pasangan HA); 6.144 MBps (per pasangan HA)

Note

Anda tidak dapat mengubah jenis penerapan sistem file setelah pembuatan. Jika Anda ingin mengubah jenis penerapan (misalnya, untuk berpindah dari Single-AZ 1 ke Single-AZ 2), Anda dapat mencadangkan data Anda dan mengembalikannya pada sistem file baru. Anda juga dapat memigrasikan data Anda dengan NetApp SnapMirror, dengan AWS DataSync, atau dengan alat penyalinan data pihak ketiga. Untuk informasi selengkapnya, silakan lihat [Migrasi ke FSx untuk ONTAP menggunakan NetApp SnapMirror](#) dan [Migrasi ke FSx untuk ONTAP menggunakan AWS DataSync](#).

Proses failover FSx untuk ONTAP

Sistem file single-AZ dan Multi-AZ secara otomatis gagal pada pasangan HA tertentu dari server file pilihan atau aktif ke server file siaga jika salah satu kondisi berikut terjadi:

- Server file pilihan atau aktif menjadi tidak tersedia
- Kapasitas throughput sistem file diubah
- Server file yang disukai atau aktif menjalani pemeliharaan yang direncanakan
- Terjadi pemadaman Zona Ketersediaan (hanya sistem file multi-AZ)

Note

Untuk sistem file generasi kedua dengan beberapa pasangan HA, perilaku failover setiap pasangan HA bersifat independen. Jika server file pilihan untuk satu pasangan HA tidak tersedia, hanya pasangan HA yang akan gagal ke server file siaga.

Ketika gagal dari satu server file ke server lain, server file aktif baru secara otomatis mulai melayani semua permintaan baca dan tulis sistem file ke pasangan HA tersebut. Untuk sistem file multi-AZ, ketika server file pilihan sepenuhnya pulih dan tersedia, Amazon FSx secara otomatis gagal kembali ke sana, dengan failback biasanya selesai dalam waktu kurang dari 60 detik. Untuk sistem file Single-AZ dan Multi-AZ, failover biasanya selesai dalam waktu kurang dari 60 detik dari deteksi kegagalan pada server file aktif hingga promosi server file siaga ke status aktif. Karena alamat IP endpoint yang digunakan klien untuk mengakses data melalui NFS atau SMB tetap sama, failover transparan untuk aplikasi Linux, Windows, dan macOS, yang melanjutkan operasi sistem file tanpa intervensi manual.

Untuk memastikan bahwa failover transparan ke klien yang terhubung ke sistem file ONTAP Single-AZ dan Multi-AZ Anda FSx, lihat [Mengakses data dari dalam AWS Cloud](#)

Menguji failover pada sebuah sistem file

Anda dapat menguji failover pada sistem file Anda dengan memodifikasi kapasitas throughputnya. Saat Anda memodifikasi kapasitas throughput sistem file Anda, Amazon FSx mengganti server file sistem file secara serial. Sistem file secara otomatis gagal ke server sekunder sementara Amazon FSx menggantikan server file pilihan terlebih dahulu. Setelah diperbarui, 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. Untuk informasi lebih lanjut tentang memodifikasi kapasitas throughput sistem file Anda dan memantau kemajuan permintaan, lihat [Mengelola kapasitas throughput](#).

Sumber daya jaringan

Bagian ini menjelaskan sumber daya jaringan yang dikonsumsi oleh sistem file Single-AZ dan Multi-AZ.

Subnet

Saat Anda membuat sistem file Single-AZ, Anda menentukan satu subnet untuk sistem file. Subnet yang Anda pilih mendefinisikan Availability Zone tempat sistem file tersebut dibuat. Ketika Anda membuat sebuah sistem file Multi-AZ, Anda menentukan 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 hal yang sama Wilayah AWS. Untuk informasi selengkapnya tentang Amazon VPC, lihat [Apa itu Amazon VPC?](#) di Panduan Pengguna Amazon Virtual Private Cloud.

Note

Terlepas dari subnet yang Anda tentukan, Anda dapat mengakses sistem file Anda dari subnet apa pun dalam VPC sistem file.

Antarmuka jaringan elastis sistem file

Untuk sistem file Single-AZ, Amazon FSx menyediakan dua [antarmuka jaringan elastis](#) (ENI) di subnet yang Anda kaitkan dengan sistem file Anda. Untuk sistem file multi-AZ, Amazon FSx juga

menyediakan dua ENIs, satu di setiap subnet yang Anda kaitkan dengan sistem file Anda. Klien berkomunikasi dengan sistem FSx file Amazon Anda menggunakan elastic network interface. Antarmuka jaringan dianggap berada dalam lingkup layanan Amazon FSx, meskipun menjadi bagian dari VPC akun Anda. Sistem file multi-AZ menggunakan alamat protokol internet (IP) mengambang sehingga klien yang terhubung dengan mulus bertransisi antara server file pilihan dan siaga selama acara failover.

Warning

- Anda tidak boleh mengubah atau menghapus antarmuka jaringan elastis yang dikaitkan dengan sistem file Anda. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan koneksi hilang permanen antara VPC dan sistem file Anda.
- Antarmuka jaringan elastis yang terkait dengan sistem file Anda akan memiliki rute yang dibuat secara otomatis dan ditambahkan ke tabel rute VPC dan subnet default Anda. Memodifikasi atau menghapus rute ini dapat menyebabkan hilangnya konektivitas sementara atau permanen untuk klien sistem file Anda.

Tabel berikut merangkum sumber daya subnet, elastic network interface, dan alamat IP untuk masing-masing jenis penyebaran sistem file ONTAP: FSx

	Generasi pertama Single-AZ	AZ tunggal generasi kedua	Multi-AZ
Jumlah subnet	1	1	2
Jumlah antarmuka jaringan elastis	2	2 per pasangan HA	2
Jumlah alamat IP per ENI	1 + jumlah SVMs dalam sistem file	Jumlah pasangan HA+jumlah pasangan HA dikalikan dengan jumlah	1 + jumlah SVMs dalam sistem file

	Generasi pertama Single-AZ	AZ tunggal generasi kedua	Multi-AZ
	SVMs dalam sistem file		
Jumlah rute tabel rute VPC	N/A	N/A	1 + jumlah SVMs dalam sistem file

Setelah sistem file atau SVM 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. Amazon FSx secara otomatis melepaskan alamat IP Elastic yang merupakan alamat IP publik yang dapat dijangkau dari Internet, yang akan dilampirkan ke antarmuka network elastis sistem file.

Amazon FSx untuk kinerja NetApp ONTAP

Berikut ini adalah ikhtisar Amazon FSx untuk kinerja sistem file NetApp ONTAP, dengan diskusi tentang opsi kinerja dan throughput yang tersedia serta tip kinerja yang berguna.

Topik

- [Bagaimana kinerja diukur FSx untuk sistem file ONTAP](#)
- [Detail performa](#)
- [Dampak jenis penerapan pada kinerja](#)
- [Dampak kapasitas penyimpanan terhadap performa](#)
- [Dampak kapasitas throughput terhadap performa](#)
- [Contoh: kapasitas penyimpanan dan kapasitas throughput](#)

Bagaimana kinerja diukur FSx untuk sistem file ONTAP

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

Latensi

Amazon FSx untuk NetApp ONTAP menyediakan latensi operasi file sub-milidetik dengan penyimpanan solid state drive (SSD), dan latensi puluhan milidetik untuk penyimpanan kolam kapasitas. Di atas itu, Amazon FSx memiliki dua lapisan cache baca di setiap server file — drive NVMe (non-volatile memory express) dan dalam memori — untuk memberikan latensi yang lebih rendah saat Anda mengakses data yang paling sering dibaca.

Throughput dan IOPS

Setiap sistem FSx file Amazon menyediakan hingga GBps puluhan throughput dan jutaan IOPS. Jumlah spesifik throughput dan IOPS yang dapat didorong oleh beban kerja Anda pada sistem file Anda tergantung pada total kapasitas throughput dan konfigurasi kapasitas penyimpanan sistem file Anda, bersama dengan sifat beban kerja Anda, termasuk ukuran set kerja aktif.

SMB Multichannel dan dukungan NFS nconnect

Dengan Amazon FSx, Anda dapat mengonfigurasi SMB Multichannel untuk menyediakan beberapa koneksi antara ONTAP dan klien dalam satu sesi SMB. SMB Multichannel menggunakan beberapa

koneksi jaringan antara klien dan server secara bersamaan untuk agregat bandwidth jaringan untuk pemanfaatan maksimal. Untuk informasi tentang penggunaan NetApp ONTAP CLI untuk mengonfigurasi SMB Multichannel, lihat [Mengonfigurasi Multichannel SMB untuk performa dan redundansi](#).

Klien NFS dapat menggunakan opsi `nconnect mount` untuk memiliki beberapa koneksi TCP (hingga 16) yang terkait dengan satu pemasangan NFS. Klien NFS semacam itu melakukan multipleks operasi file ke beberapa koneksi TCP secara round-robin dan dengan demikian memperoleh throughput yang lebih tinggi dari bandwidth jaringan yang tersedia. NFSv3 dan dukungan NFSv4 .1+. `nconnect` [Bandwidth jaringan EC2 instans Amazon menggambarkan batas bandwidth](#) aliran 5 Gbps penuh duplex per jaringan. Anda dapat mengatasi batas ini dengan menggunakan beberapa aliran jaringan dengan `nconnect` atau SMB multichannel. Lihat dokumentasi klien NFS Anda untuk mengonfirmasi `nconnect` apakah didukung dalam versi klien Anda. Untuk informasi selengkapnya tentang NetApp ONTAP dukungannconnect, lihat [ONTAPdukungan untuk NFSv4 .1](#).

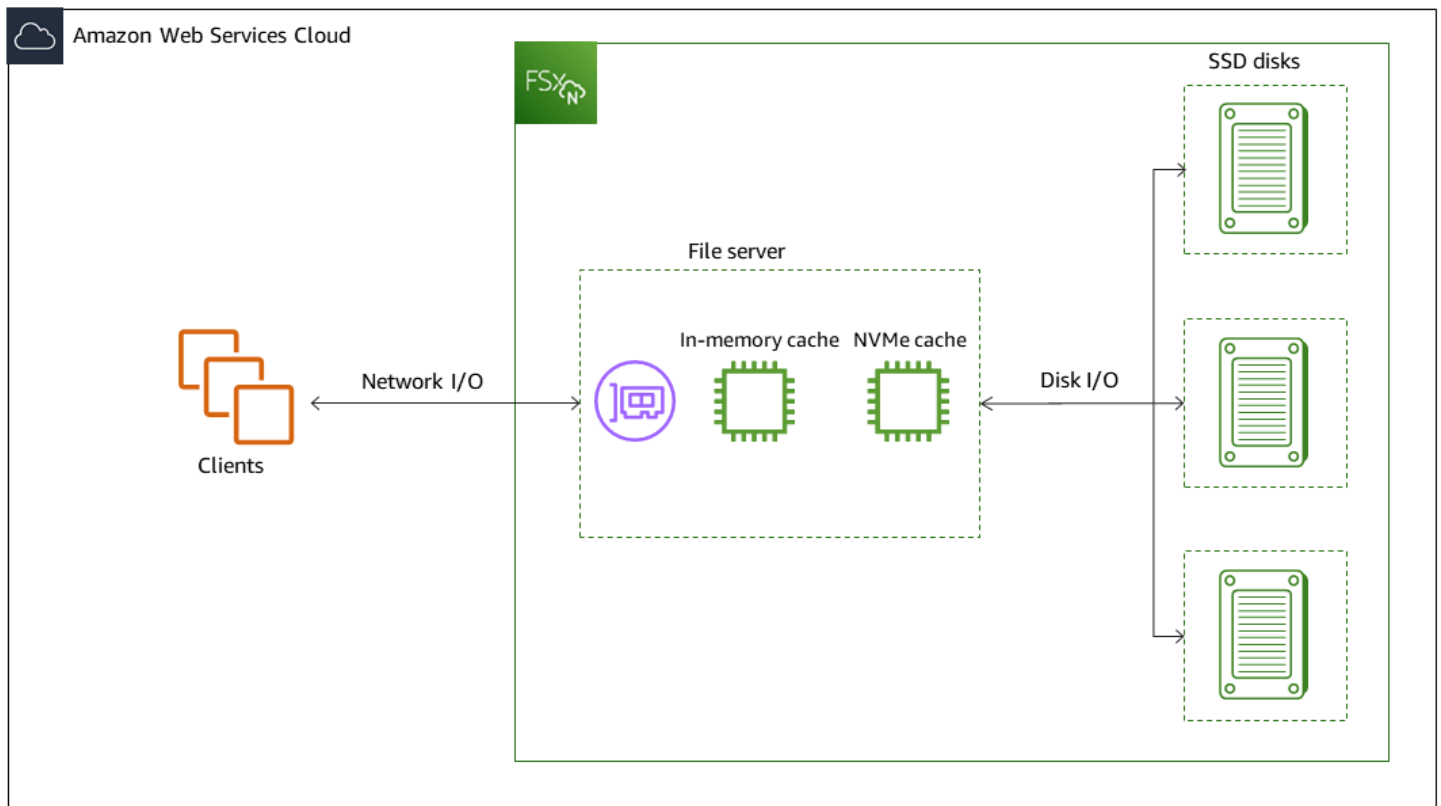
Bingkai jumbo

Untuk mencapai throughput baca atau tulis maksimum, sebaiknya aktifkan jumbo frame pada semua antarmuka jaringan di jalur data ke sistem FSx file Amazon Anda, termasuk instance klien Anda. EC2 Pengaturan unit transmisi maksimum (MTU) default untuk antarmuka jaringan pada sistem file ONTAP Anda FSx adalah 9.001 byte.

Detail performa

Untuk memahami model kinerja Amazon FSx untuk NetApp ONTAP secara detail, Anda dapat memeriksa komponen arsitektur sistem FSx file Amazon. Instans komputasi klien Anda, baik yang ada di dalam AWS maupun di tempat, mengakses sistem file Anda melalui satu atau beberapa antarmuka jaringan elastis (ENI). Antarmuka jaringan ini berada di Amazon VPC yang Anda kaitkan dengan sistem file Anda. Di belakang setiap sistem file ENI adalah NetApp ONTAP file server yang melayani data melalui jaringan ke klien yang mengakses sistem file. Amazon FSx menyediakan cache dan NVMe cache dalam memori yang cepat di setiap server file untuk meningkatkan kinerja data yang paling sering diakses. Terlampir ke setiap server file adalah disk SSD yang menghosting data sistem file Anda.

Komponen ini digambarkan dalam diagram berikut.



Sesuai dengan komponen arsitektur ini—antarmuka jaringan, cache dalam memori, NVMe cache, dan volume penyimpanan—adalah karakteristik kinerja utama sistem file Amazon FSx untuk NetApp ONTAP yang menentukan keseluruhan throughput dan kinerja IOPS.

- I/O Kinerja jaringan: throughput/IOPS permintaan antara klien dan server file (secara agregat)
- Ukuran dalam memori dan NVMe cache pada server file: ukuran set kerja aktif yang dapat ditampung untuk caching
- I/O Kinerja disk: throughput/IOPS permintaan antara server file dan disk penyimpanan

Ada dua faktor yang menentukan karakteristik kinerja ini untuk sistem file Anda: jumlah total IOPS SSD dan kapasitas throughput yang Anda konfigurasi untuk itu. Dua karakteristik kinerja pertama - I/O kinerja jaringan dan ukuran dalam memori dan NVMe cache - hanya ditentukan oleh kapasitas throughput, sedangkan yang ketiga - kinerja I/O disk - ditentukan oleh kombinasi kapasitas throughput dan SSD IOPS.

Beban kerja berbasis file biasanya runcing, ditandai dengan periode tinggi yang pendek dan intens I/O dengan banyak waktu idle di 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

jaringan dan disk. I/O I/O Amazon FSx menggunakan mekanisme I/O kredit jaringan 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

Note

Untuk protokol iSCSI NVMe/TCP dan SAN, operasi klien baca sekuensial dapat mencapai ledakan jaringan maksimum atau throughput dasar sistem file. I/O

Operasi tulis menggunakan bandwidth jaringan dua kali lebih banyak daripada operasi baca. Operasi tulis harus direplikasi pada server file sekunder, sehingga operasi penulisan tunggal menghasilkan dua kali jumlah throughput jaringan.

Dampak jenis penerapan pada kinerja

Anda dapat membuat sistem file Single-AZ dan Multi-AZ dengan FSx ONTAP. Sistem file generasi pertama (baik Single-AZ dan Multi-AZ) dan sistem file multi-AZ generasi kedua didukung oleh satu pasangan ketersediaan tinggi (HA). Sistem file Single-AZ generasi kedua didukung oleh hingga 12 pasang HA. Untuk informasi selengkapnya, lihat [Mengelola pasangan ketersediaan tinggi \(HA\)](#).

FSx untuk sistem file ONTAP Multi-AZ dan Single-AZ menyediakan latensi operasi file sub-milidetik yang konsisten dengan penyimpanan SSD dan latensi puluhan milidetik dengan penyimpanan kolam kapasitas. Selain itu, sistem file yang memenuhi persyaratan berikut menyediakan cache NVMe baca untuk mengurangi latensi baca dan meningkatkan IOPS untuk data yang sering dibaca:

- Sistem file multi-AZ 1 dan Multi-AZ 2
- Sistem file Single-AZ 1 dibuat setelah 28 November 2022 dengan setidaknya 2 GBps kapasitas throughput
- Sistem file single-AZ 2 dengan setidaknya 6 GBps kapasitas throughput per pasang

Note

Untuk sistem file generasi kedua (Single-AZ 2 dan Multi-AZ 2), menggunakan NVMe cache dapat mengakibatkan beban kerja Anda mencapai throughput total yang lebih sedikit untuk throughput tinggi atau beban kerja I/O yang besar. Jika Anda memiliki beban kerja yang

terikat throughput, sebaiknya nonaktifkan cache. NVMe Untuk informasi selengkapnya, lihat [Mengelola NVMe cache](#).

Tabel berikut menunjukkan jumlah kapasitas throughput yang dapat ditingkatkan oleh sistem file tergantung pada faktor-faktor seperti jumlah pasangan ketersediaan tinggi (HA) dan Wilayah AWS ketersediaan.

First-generation file systems

Spesifikasi kinerja ini berlaku untuk sistem file Single-AZ dan Multi-AZ generasi pertama.

Throughput maksimum dari penyimpanan SSD per pasangan HA untuk sistem file generasi pertama

	Wilayah Timur AS (Ohio), Wilayah AS Timur (Virginia N.), Wilayah Barat AS (Oregon), dan Eropa (Irlandia)		Semua Wilayah AWS tempat lain FSx untuk ONTAP tersedia	
	Baca throughput () MBps	Tulis throughput () MBps	Baca throughput () MBps	Tulis throughput () MBps
Single-AZ	4,096 ¹	1.000	2,048	750
Multi-AZ	4,096 ¹	1.800	2,048	1.300

Note

¹ Untuk menyediakan 4 GBps kapasitas throughput, sistem file Anda harus dikonfigurasi dengan kapasitas penyimpanan SSD minimal 5.120 GiB dan 160.000 IOPS SSD.

Second-generation file systems

Spesifikasi kinerja ini berlaku untuk sistem file Single-AZ dan Multi-AZ generasi kedua. Umumnya, sistem file generasi kedua dapat mengirimkan seluruh kapasitas yang disediakan penuh untuk

pembacaan dan hingga sepertiga dari kapasitas throughput yang disediakan untuk penulisan. Pengecualian adalah MB/s opsi 6.144, yang tercantum dalam tabel ini.

Throughput maksimum dari penyimpanan SSD per pasangan HA untuk sistem file generasi kedua

	Baca throughput () MBps	Tulis throughput () MBps
Single-AZ	6,144 ¹	1,024 ¹
Multi-AZ	6,144	2,048

 Note

¹ Per pasangan HA (hingga 12). Untuk informasi selengkapnya, lihat [Mengelola pasangan ketersediaan tinggi \(HA\)](#).

Dampak kapasitas penyimpanan terhadap performa

Tingkat throughput dan IOPS disk maksimum tingkat yang dapat dicapai sistem file Anda lebih rendah dari:

- tingkat kinerja disk yang disediakan oleh server file Anda, berdasarkan kapasitas throughput yang Anda pilih untuk sistem file Anda
- tingkat kinerja disk yang disediakan oleh jumlah IOPS SSD yang Anda berikan untuk sistem file Anda

Secara default, penyimpanan SSD sistem file Anda menyediakan hingga tingkat throughput disk dan IOPS berikut:

- Throughput disk (MBps per TiB penyimpanan): 768
- Disk IOPS (IOPs per TiB penyimpanan): 3.072

 Note

Saat mengurangi kapasitas penyimpanan SSD pada sistem file generasi kedua, sebagian besar beban kerja mengalami dampak kinerja minimal. Namun, beban kerja berat tulis mungkin mengalami penurunan kinerja sementara. Anda mungkin juga mengalami I/O jeda singkat (hingga 60 detik) karena akses klien dialihkan ke disk baru.

Untuk meminimalkan dampak kinerja, pastikan beban kerja yang sedang berlangsung tidak secara konsisten mengkonsumsi lebih dari 50% CPU, 50% disk throughput, atau 50% SSD IOPS sebelum memulai operasi penurunan SSD. Untuk informasi selengkapnya tentang penurunan kapasitas penyimpanan SSD, lihat [Kapan mengurangi kapasitas penyimpanan SSD](#)

Dampak kapasitas throughput terhadap performa

Setiap sistem FSx file Amazon memiliki kapasitas throughput yang Anda konfigurasi saat sistem file dibuat. Kapasitas throughput sistem file Anda menentukan tingkat I/O kinerja jaringan, atau kecepatan di mana setiap server file yang menghosting sistem file Anda dapat melayani data file melalui jaringan ke klien yang mengaksesnya. Tingkat kapasitas throughput yang lebih tinggi datang dengan lebih banyak memori dan non-volatile memory express (NVMe) penyimpanan untuk caching data pada setiap server file, dan tingkat I/O kinerja disk yang lebih tinggi didukung oleh setiap file server.

Anda dapat secara opsional menyediakan tingkat IOPS SSD yang lebih tinggi saat membuat sistem file Anda. Tingkat maksimum SSD IOPS yang dapat dicapai oleh sistem file Anda juga ditentukan oleh kapasitas throughput sistem file Anda, bahkan ketika menyediakan IOPS SSD tambahan.

Tabel berikut menunjukkan set lengkap spesifikasi untuk kapasitas throughput, bersama dengan tingkat dasar dan burst, dan jumlah memori untuk caching pada server file yang sesuai. Wilayah AWS

First-generation Single-AZ file system

Spesifikasi kinerja ini berlaku untuk sistem file Single-AZ generasi pertama yang dibuat setelah 28 November 2022 dalam yang ditentukan. Wilayah AWS

Spesifikasi kinerja untuk sistem file sebagai berikut Wilayah AWS: AS Timur (Virginia N.), AS Timur (Ohio), AS Barat (Oregon), dan Eropa (Irlandia)

FSx kapasitas throughput jaringan () MBps	Kapasitas throughput jaringan () MBps	IOPS Jaringan	Caching dalam memori (GB)	NVMe baca caching (GB)	Throughput disk () MBps	Drive SSD IOPS *			
	Baseline	Meledak			Baseline	Meledak	Baseline	Meledak	
128	188	1.500	Puluhan ribu baseline	16	–	128	1.250	6.000	40.000
256	375	1.500		32	–	256	1.250	12.000	40.000
512	750	1.500	Puluhan ribu baseline	64	–	512	1.250	20.000	40.000
1,024	1.500	–		128	–	1,024	1.250	40.000	–
2,048	3,125	–		256	1.900	2,048	–	80.000	–
4,096	6,250	–		512	5.400	4,096	–	160.000	–

Note

* IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache atau cache memori server file Anda. NVMe

Spesifikasi kinerja ini berlaku untuk sistem file Single-AZ generasi pertama di semua Wilayah AWS tempat lain FSx untuk ONTAP tersedia.

Spesifikasi kinerja untuk sistem file di [semua Wilayah AWS tempat lain FSx untuk ONTAP tersedia](#)

FSx	Kapasitas	IOPS	Caching	Throughput disk ()	Drive SSD IOPS *
kapasitas	throughput	Jaringan	dalam	MBps	
throughput jaringan ()	MBps		memori		
t ()			(GB)		
MBps					
	Baseline	Meledak		Baseline	Meledak
128	150	1.250	Puluhan	128	600
			ribu		
256	300	1.250	baseline	256	600
512	625	1.250	Puluhan	512	600
			ribu		
1,024	1.500	–	baseline	1,024	–
2,048	3,125	–		2,048	–

Note

* IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache atau cache memori server file Anda. NVMe

Second-generation Single-AZ file system

Spesifikasi kinerja ini berlaku untuk sistem file Single-AZ generasi kedua.

Spesifikasi kinerja untuk sistem file Single-AZ generasi kedua

FSx	Kapasitas	IOPS	Caching	NVMe	Throughput disk	Drive SSD IOPS			
kapasitasthroughput	Jaringan	dalam	caching	() MBps	*				
throughputjaringan () MBps		memori	(GB)						
t ()		(GB)							
MBps									
	Baseline	Meledak			Baseline	Meledak			
384**	781	6,250	Puluhan ribu baseline	16	–	384	3,125	12.500	65.000
768**	1,563	6,250		32	–	768	3,125	25.000	65.000
1,536	3,125	6,250		64	–	1,536	3,125	50.000	65.000
3,072	6,250	–		128	–	3,072	–	100.000	–
6,144	12.500	–		256	1.900	6,144	–	200.000	–

Note

* IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache atau cache memori server file Anda. NVMe

** Sistem file Single-AZ generasi kedua mendukung kapasitas throughput 384 dan 768, tetapi hanya dengan satu pasangan HA. Untuk menambahkan pasangan HA, sistem file Anda harus dikonfigurasi dengan setidaknya 1.536 MBps kapasitas throughput.

First-generation Multi-AZ file system

Spesifikasi kinerja ini berlaku untuk sistem file Multi-AZ generasi pertama yang dibuat setelah 28 November 2022 dalam yang ditentukan. Wilayah AWS

Spesifikasi kinerja untuk sistem file sebagai berikut Wilayah AWS: AS Timur (Virginia N.), AS Timur (Ohio), AS Barat (Oregon), dan Eropa (Irlandia)

FSx	Kapasitas		IOPS	Caching	NVMe	Throughput disk	Drive SSD IOPS		
	kapasitas	throughput	Jaringan	dalam	caching	() MBps	*		
t ()	throughput	jaringan () MBps		memori	(GB)				
MBps				(GB)					
	Baseline	Meledak				Baseline	Meledak	Baseline	Meledak
128	188	1.500	Puluhan	16	238	128	1.250	6.000	40.000
256	375	1.500	ribu	32	475	256	1.250	12.000	40.000
512	750	1.500	baseline	64	950	512	1.250	20.000	40.000
1,024	1.500	–	ribu	128	1.900	1,024	1.250	40.000	–
2,048	3,125	–	baseline	256	3,800	2,048	–	80.000	–
4,096	6,250	–		512	7,600	4,096	–	160.000	–

Note

* IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache atau cache memori server file Anda. NVMe

Spesifikasi kinerja ini berlaku untuk sistem file Multi-AZ generasi pertama di semua Wilayah AWS tempat lain FSx untuk ONTAP tersedia.

Spesifikasi kinerja untuk sistem file di [semua Wilayah AWS tempat lain FSx untuk ONTAP tersedia](#)

FSx	Kapasitas	IOPS	Caching	NVMe	Throughput disk	Drive SSD IOPS			
kapasitasthroughput	Jaringan	dalam	caching	() MBps	*				
throughputjaringan () MBps	memori	(GB)							
t ()									
MBps									
	Baseline	Meledak							
128	150	1.250	Puluhan	16	150	128	600	6.000	18,750
256	300	1.250	ribu	32	300	256	600	12.000	18,750
			baseline						
512	625	1.250	Puluhan	64	600	512	600	18,750	–
1,024	1.500	–	ribu	128	1.200	1,024	–	40.000	–
			baseline						
2,048	3,125	–		256	2,400	2,048	–	80.000	–

Note

* IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache atau cache memori server file Anda. NVMe

Second-generation Multi-AZ file systems

Spesifikasi kinerja ini berlaku untuk sistem file Multi-AZ generasi kedua.

Spesifikasi kinerja untuk sistem file Multi-AZ generasi kedua

FSx	Kapasitas		IOPS	Caching	NVMe	Throughput disk		Drive SSD IOPS	
kapasitas	throughput		Jaringan	dalam	caching	() MBps		*	
throughput	jaringan	() MBps		memori	(GB)				
t ()				(GB)					
MBps									
	Baseline	Meledak				Baseline	Meledak	Baseline	Meledak
384	781	6,250	Puluhan ribu baseline	16	237	384	3,125	12.500	65.000
768	1,563	6,250		32	474	768	3,125	25.000	65.000
1,536	3,125	6,250		64	950	1,536	3,125	50.000	65.000
3,072	6,250	–		128	1.900	3,072	–	100.000	–
6,144	12.500	–		256	3,800	6,144	–	200.000	–

Note

* IOPS SSD Anda hanya digunakan saat Anda mengakses data yang tidak di-cache di cache atau cache memori server file Anda. NVMe

Contoh: kapasitas penyimpanan dan kapasitas throughput

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

Sistem file generasi pertama yang dikonfigurasi dengan kapasitas penyimpanan SSD 2 TiB dan kapasitas throughput MBps 512 memiliki tingkat throughput berikut:

- Throughput jaringan — 625 MBps baseline dan 1.250 MBps burst (lihat tabel kapasitas throughput)
- Throughput disk — 512 MBps baseline dan 600 burst. MBps

Beban kerja Anda yang mengakses sistem file akan dapat mendorong hingga 625 MBps baseline dan 1.250 MBps burst throughput untuk operasi file yang dilakukan pada data yang diakses secara aktif yang di-cache di cache dan cache server file dalam memori. NVMe

Mengelola sumber daya FSx ONTAP

Dengan menggunakan Konsol Manajemen AWS, AWS CLI, dan ONTAP CLI dan API, Anda dapat melakukan tindakan administratif berikut FSx untuk sumber daya ONTAP:

- Membuat, mencantumkan, memperbarui, dan menghapus sistem file, penyimpanan mesin virtual (SVMs), volume, cadangan, dan tag.
- Mengelola akses, akun administratif dan kata sandi, persyaratan kata sandi, protokol SMB dan iSCSI, aksesibilitas jaringan untuk target pemasangan sistem file yang ada

Topik

- [Mengelola kapasitas penyimpanan](#)
- [Mengelola FSx untuk sistem file ONTAP](#)
- [Mengelola FSx mesin virtual penyimpanan ONTAP](#)
- [Mengelola FSx volume ONTAP](#)
- [Membuat iSCSI LUN](#)
- [Mengoptimalkan kinerja dengan jendela FSx pemeliharaan Amazon](#)
- [Mengelola kapasitas throughput](#)
- [Mengelola saham SMB](#)
- [Mengelola FSx sumber daya ONTAP menggunakan aplikasi NetApp](#)
- [Menandai sumber daya Amazon FSx](#)

Mengelola kapasitas penyimpanan

Amazon FSx untuk NetApp ONTAP menyediakan sejumlah fitur terkait penyimpanan yang dapat Anda gunakan untuk mengelola kapasitas penyimpanan pada sistem file Anda.

Topik

- [FSx untuk tingkatan penyimpanan ONTAP](#)
- [Memilih jumlah penyimpanan SSD sistem file yang tepat](#)
- [Kapasitas penyimpanan sistem file dan IOPS](#)
- [Kapasitas penyimpanan volume](#)

FSx untuk tingkatan penyimpanan ONTAP

Tingkat penyimpanan adalah media penyimpanan fisik untuk Amazon FSx untuk sistem file NetApp ONTAP. FSx untuk ONTAP menawarkan tingkatan penyimpanan berikut:

- Tingkat SSD - Penyimpanan solid-state drive (SSD) berkinerja tinggi yang disediakan pengguna yang dibuat khusus untuk bagian aktif kumpulan data Anda.
- Tingkat kolam kapasitas — Penyimpanan yang sepenuhnya elastis yang secara otomatis menskalakan ke ukuran petabyte, dan dioptimalkan biaya untuk data Anda yang jarang diakses.

Volume FSx untuk ONTAP adalah sumber daya virtual yang, mirip dengan folder, tidak mengkonsumsi kapasitas penyimpanan. Data yang Anda simpan—dan yang menghabiskan penyimpanan fisik—hidup di dalam volume. Saat Anda membuat volume, Anda menentukan ukurannya—yang dapat Anda ubah setelah dibuat. FSx untuk volume ONTAP disediakan tipis, dan penyimpanan sistem file tidak dicadangkan sebelumnya. Sebaliknya, SSD dan penyimpanan kolam kapasitas dialokasikan secara dinamis, sesuai kebutuhan. [Kebijakan tiering](#), yang Anda konfigurasi pada tingkat volume, menentukan apakah dan kapan data yang disimpan dalam transisi tingkat SSD ke tingkat kumpulan kapasitas.

Diagram berikut menggambarkan contoh data yang diletakkan di beberapa FSx untuk volume ONTAP dalam sistem file.

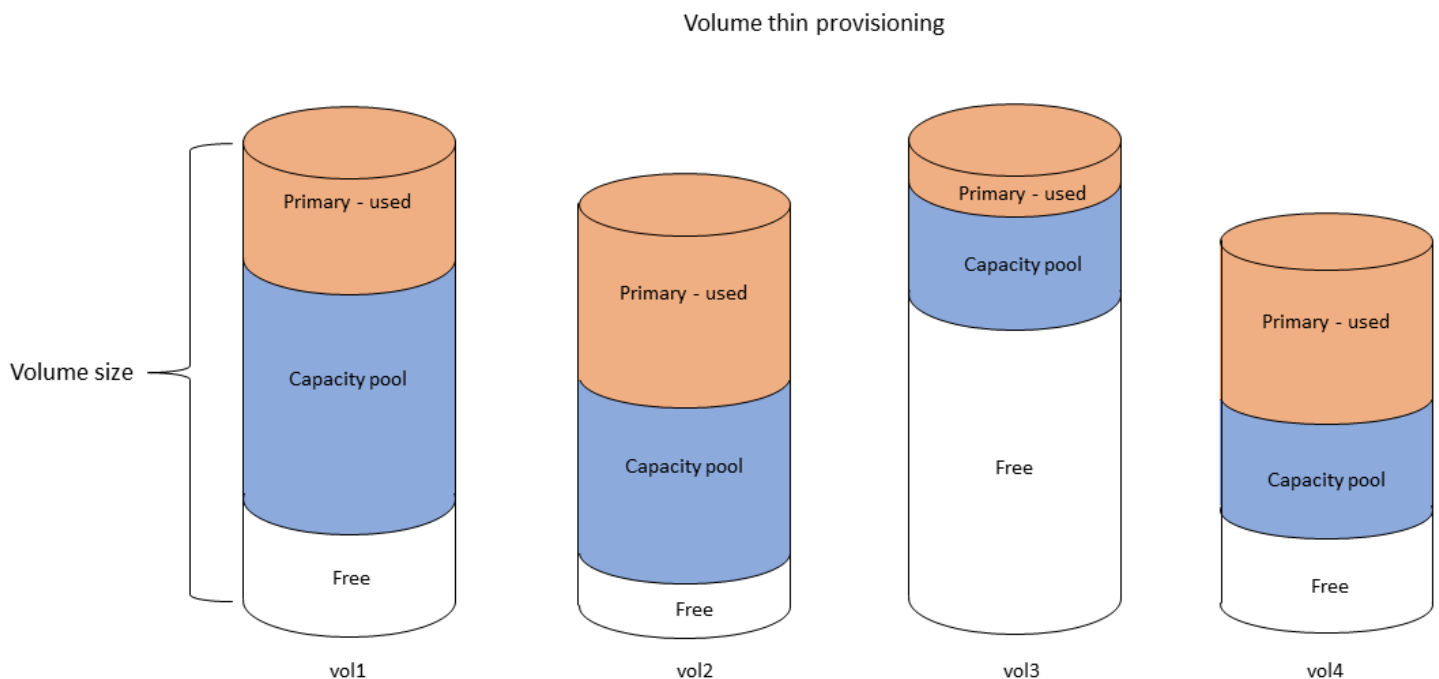
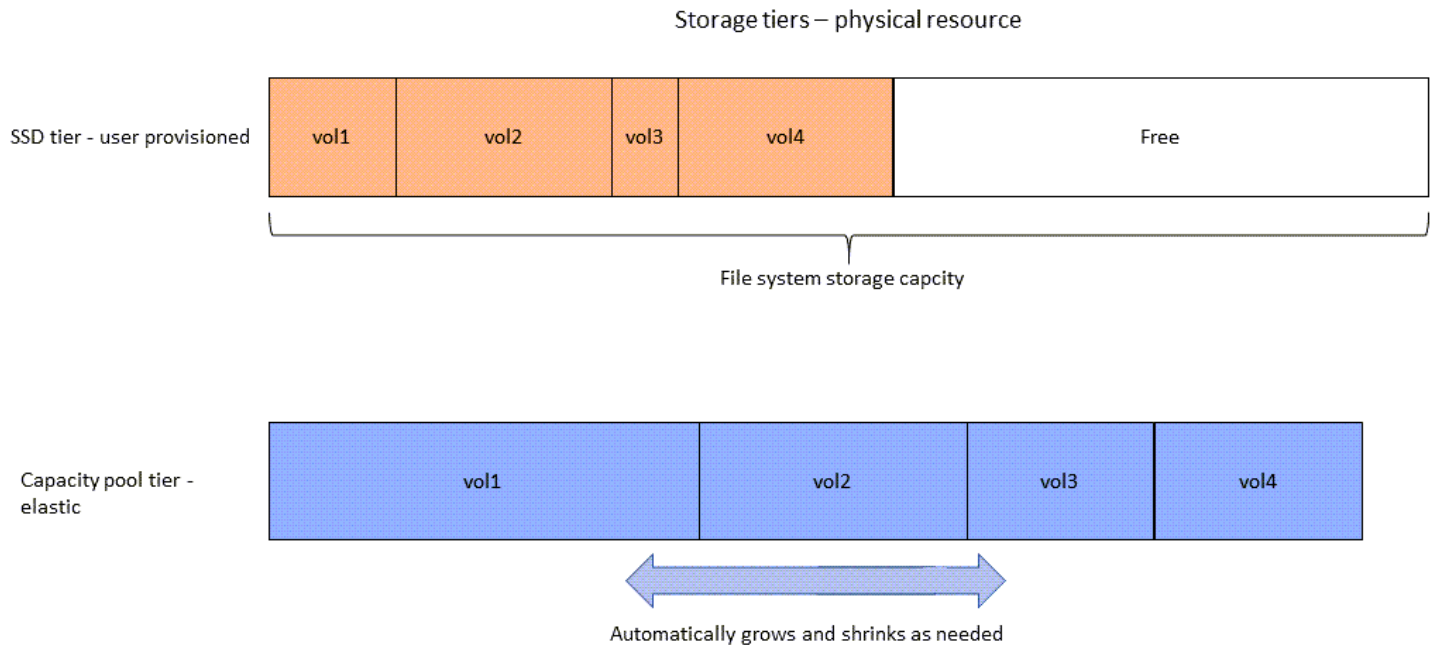


Diagram berikut menggambarkan bagaimana kapasitas penyimpanan fisik sistem file dikonsumsi oleh data dalam empat volume pada diagram sebelumnya.



Anda dapat mengurangi biaya penyimpanan dengan memilih kebijakan tiering yang paling memenuhi persyaratan untuk setiap volume pada sistem file Anda. Untuk informasi selengkapnya, lihat [Tingkat data volume](#).

Memilih jumlah penyimpanan SSD sistem file yang tepat

Saat memilih jumlah kapasitas penyimpanan SSD untuk sistem file ONTAP Anda, Anda perlu mengingat item berikut yang memengaruhi jumlah penyimpanan SSD yang tersedia untuk menyimpan data Anda: FSx

- Kapasitas penyimpanan dicadangkan untuk overhead perangkat lunak NetApp ONTAP.
- Metadata berkas
- Data yang baru ditulis
- File yang ingin Anda simpan di penyimpanan SSD, apakah itu data yang belum mencapai periode pendinginannya, atau data yang baru-baru ini Anda baca yang diambil kembali ke SSD.

Bagaimana penyimpanan SSD digunakan

Penyimpanan SSD sistem file Anda digunakan untuk kombinasi perangkat lunak NetApp ONTAP (overhead), metadata file, dan data Anda.

NetApp Overhead perangkat lunak ONTAP

Seperti sistem file NetApp ONTAP lainnya, hingga 16% dari kapasitas penyimpanan SSD sistem file dicadangkan untuk overhead ONTAP, yang berarti tidak tersedia untuk menyimpan file Anda. Overhead ONTAP dialokasikan sebagai berikut:

- 11% dicadangkan untuk perangkat lunak NetApp ONTAP. Untuk sistem file dengan kapasitas penyimpanan SSD lebih dari 30 tebibytes (TiB), 6% dicadangkan.
- 5% dicadangkan untuk snapshot agregat, yang diperlukan untuk menyinkronkan data antara kedua server file sistem file.

Metadata berkas

Metadata file biasanya mengkonsumsi 3-7% dari kapasitas penyimpanan yang dikonsumsi oleh file. Persentase ini tergantung pada ukuran file rata-rata (ukuran file rata-rata yang lebih kecil membutuhkan lebih banyak metadata), dan jumlah penghematan efisiensi penyimpanan yang dicapai pada file Anda. Perhatikan bahwa metadata file tidak mendapat manfaat dari penghematan efisiensi penyimpanan. Anda dapat menggunakan panduan berikut untuk memperkirakan jumlah penyimpanan SSD yang digunakan untuk metadata pada sistem file Anda.

Ukuran file rata-rata	Ukuran metadata sebagai persentase data file
4 KB	7%
8 KB	3,5%
32 KB atau lebih	1-3%

Saat mengukur jumlah kapasitas penyimpanan SSD yang Anda butuhkan untuk metadata file yang Anda rencanakan untuk disimpan pada tingkat kolam kapasitas, kami sarankan untuk menggunakan rasio konservatif 1 GiB penyimpanan SSD untuk setiap 10 GiB data yang Anda rencanakan untuk disimpan pada tingkat kolam kapasitas.

Data file yang disimpan di tingkat SSD Anda

Selain kumpulan data aktif Anda dan semua metadata file, semua data yang ditulis ke sistem file Anda pada awalnya ditulis ke tingkat SSD sebelum di-tiered-off ke penyimpanan kolam kapasitas. Hal ini berlaku terlepas dari kebijakan tingkatan volume, dengan pengecualian bahwa data ditulis

langsung ke penyimpanan kumpulan kapasitas saat menggunakan SnapMirror pada volume yang dikonfigurasi dengan kebijakan tiering Semua data.

Pembacaan acak dari tingkat kolam kapasitas di-cache di tingkat SSD, selama tingkat SSD di bawah pemanfaatan 90%. Untuk informasi selengkapnya, lihat [Tingkat data volume](#).

Pemanfaatan kapasitas SSD yang disarankan

Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan tingkat penyimpanan SSD Anda secara berkelanjutan. Untuk sistem file generasi kedua, kami juga menyarankan agar Anda tidak melebihi 80% pemanfaatan agregat sistem file Anda secara berkelanjutan. Rekomendasi ini konsisten dengan NetApp rekomendasi untuk ONTAP. Karena tingkat SSD sistem file Anda juga digunakan untuk pementasan penulisan, dan untuk pembacaan acak dari, tingkat kumpulan kapasitas, setiap perubahan mendadak dalam pola akses dapat dengan cepat menyebabkan pemanfaatan tingkat SSD Anda meningkat.

Pada pemanfaatan SSD 90%, data yang dibaca dari tier pool kapasitas tidak lagi di-cache pada tingkat SSD sehingga kapasitas SSD yang tersisa dipertahankan untuk setiap data baru yang ditulis ke sistem file. Hal ini menyebabkan pembacaan berulang data yang sama dari tingkat kumpulan kapasitas dibaca dari penyimpanan kumpulan kapasitas alih-alih di-cache dan dibaca dari tingkat SSD, yang dapat memengaruhi kapasitas throughput sistem file Anda.

Semua fungsionalitas tiering berhenti ketika tingkat SSD berada pada atau di atas pemanfaatan 98%. Untuk informasi selengkapnya, lihat [Ambang batas jenjang](#).

Efisiensi penyimpanan

NetApp ONTAP menawarkan fitur efisiensi penyimpanan tingkat blok pada tingkat volume yang mencakup kompresi, pemadatan, dan deduplikasi. Fitur-fitur ini dapat menghemat hingga 65% dalam kapasitas penyimpanan untuk berbagi file umum, tanpa mengorbankan kinerja. Anda dapat mengaktifkan efisiensi penyimpanan berdasarkan volume per volume. Fitur-fitur ini mengurangi jumlah kapasitas penyimpanan yang dikonsumsi data Anda, memungkinkan Anda untuk mengkonsumsi lebih sedikit ruang penyimpanan di SSD, kumpulan kapasitas, dan penyimpanan cadangan. Anda dapat mengaktifkan kompresi dan deduplikasi pada setiap volume untuk data dalam penyimpanan SSD. Penghematan penyimpanan dari kompresi dan deduplikasi dalam penyimpanan SSD dipertahankan ketika data berjenjang ke penyimpanan kolam kapasitas. Efisiensi penyimpanan selalu diaktifkan untuk data cadangan, terlepas dari konfigurasi efisiensi penyimpanan sistem file Anda.

Tabel berikut menunjukkan contoh penghematan penyimpanan tipikal.

	Kompresi saja	Hanya deduplikasi	Kompresi & deduplikasi
Berbagi file tujuan umum	50%	30%	65%
Server virtual dan desktop	55%	70%	70%
Basis Data	65-70%	0%	65-70%
Data rekayasa	55%	30%	75%
Data geoseismik	40%	3%	40%

Untuk sebagian besar beban kerja, mengaktifkan kompresi dan deduplikasi tidak akan berdampak buruk pada kinerja sistem file. Untuk sebagian besar beban kerja, kompresi meningkatkan kinerja secara keseluruhan. Untuk memberikan pembacaan dan penulisan cepat dari cache RAM, FSx untuk server file ONTAP dilengkapi dengan tingkat bandwidth jaringan yang lebih tinggi pada kartu antarmuka jaringan front-end (NICs) daripada yang tersedia antara server file dan disk penyimpanan. Karena kompresi data mengurangi jumlah data yang dikirim antara server file dan disk penyimpanan, untuk sebagian besar beban kerja, Anda akan melihat peningkatan kapasitas throughput sistem file secara keseluruhan saat menggunakan kompresi data. Peningkatan kapasitas throughput yang terkait dengan kompresi data akan dibatasi setelah Anda memenuhi NIC front-end sistem file Anda.

Amazon FSx untuk NetApp ONTAP juga mendukung ONTAP fitur lain yang menghemat ruang Anda, termasuk snapshot, penyediaan tipis, dan volume. FlexClone

Fitur efisiensi penyimpanan tidak diaktifkan secara default. Anda dapat mengaktifkannya sebagai berikut:

- Pada volume root SVM saat Anda [membuat sistem file](#).
- Saat Anda [membuat volume baru](#).
- Saat Anda [memodifikasi volume yang ada](#).

Untuk melihat jumlah penghematan penyimpanan pada sistem file dengan efisiensi penyimpanan diaktifkan, lihat [Memantau penghematan efisiensi penyimpanan](#).

Menghitung penghematan efisiensi penyimpanan

Anda dapat menggunakan metrik sistem CloudWatch file `LogicalDataStored` dan `StorageUsed` FSx untuk ONTAP untuk menghitung penghematan penyimpanan dari kompresi, deduplikasi, pemadatan, snapshot, dan. FlexClones Metrik ini memiliki dimensi tunggal, `FileSystemId`. Untuk informasi selengkapnya, lihat [Metrik sistem file](#).

- Untuk menghitung penghematan efisiensi penyimpanan dalam byte, ambil Rata-rata `StorageUsed` selama periode tertentu dan kurangi dari Rata-rata selama periode yang sama. `LogicalDataStored`
- Untuk menghitung penghematan efisiensi penyimpanan sebagai persentase dari total ukuran data logis, ambil Average dari `StorageUsed` selama periode tertentu dan kurangi dari `LogicalDataStored` periode yang samaAverage. Kemudian bagi perbedaannya Average dengan `LogicalDataStored` periode yang sama.

Contoh ukuran SSD

Asumsikan Anda ingin menyimpan 100 TiB data untuk aplikasi di mana 80% data jarang diakses. Dalam skenario ini, 80% (80 TiB) data Anda secara otomatis berjenjang ke tingkat kumpulan kapasitas dan 20% sisanya (20 TiB) tetap dalam penyimpanan SSD. Berdasarkan penghematan efisiensi penyimpanan tipikal sebesar 65% untuk beban kerja berbagi file tujuan umum, yang setara dengan 7 TiB data. Untuk mempertahankan tingkat pemanfaatan SSD 80%, Anda memerlukan kapasitas penyimpanan SSD 8,75 TiB untuk 20 TiB data yang diakses secara aktif. Jumlah penyimpanan SSD yang Anda berikan juga perlu memperhitungkan overhead penyimpanan perangkat lunak ONTAP sebesar 16%, seperti yang ditunjukkan dalam perhitungan berikut.

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

Jadi dalam contoh ini, Anda perlu menyediakan setidaknya 10,42 TiB penyimpanan SSD. Anda juga akan menggunakan 28 TiB penyimpanan kolam kapasitas untuk sisa 80 TiB data yang jarang diakses.

Kapasitas penyimpanan sistem file dan IOPS

Saat Anda membuat sistem file FSx untuk ONTAP, Anda menentukan kapasitas penyimpanan tingkat SSD. Untuk sistem file single-AZ generasi kedua, kapasitas penyimpanan yang Anda tentukan

tersebar merata di antara kumpulan penyimpanan dari setiap pasangan ketersediaan tinggi (HA); kumpulan penyimpanan ini disebut agregat.

Untuk setiap GiB penyimpanan SSD yang Anda sediakan, Amazon FSx secara otomatis menyediakan 3 input/output operasi SSD per detik (IOPS) untuk sistem file, hingga maksimum 160.000 IOPS SSD per sistem file. Untuk sistem file Single-AZ generasi kedua, IOPS SSD Anda tersebar merata di setiap agregat sistem file Anda. Anda memiliki opsi untuk menentukan tingkat IOPS SSD yang disediakan di atas IOPS 3 SSD otomatis per GiB. Untuk informasi selengkapnya tentang jumlah maksimum IOPS SSD yang dapat Anda berikan untuk sistem file ONTAP, lihat [FSx Dampak kapasitas throughput terhadap performa](#)

Topik

- [Memperbarui penyimpanan SSD sistem file dan IOPS](#)
- [Kapan meningkatkan kapasitas penyimpanan SSD](#)
- [Meningkatkan kapasitas penyimpanan SSD](#)
- [Pertimbangan untuk meningkatkan kapasitas penyimpanan SSD](#)
- [Kapan mengurangi kapasitas penyimpanan SSD](#)
- [Mengurangi kapasitas penyimpanan SSD](#)
- [Pertimbangan untuk mengurangi kapasitas penyimpanan SSD](#)
- [Keterbatasan untuk mengurangi kapasitas penyimpanan SSD](#)
- [Membuat alarm pemanfaatan kapasitas penyimpanan untuk sistem file Anda](#)
- [Memperbarui kapasitas penyimpanan dan IOPS yang disediakan](#)
- [Memperbarui kapasitas penyimpanan secara dinamis](#)
- [Memantau pemanfaatan penyimpanan SSD](#)
- [Memantau penghematan efisiensi penyimpanan](#)
- [Memantau kapasitas penyimpanan dan pembaruan IOPS](#)

Memperbarui penyimpanan SSD sistem file dan IOPS

Saat Anda membutuhkan penyimpanan tambahan untuk bagian aktif kumpulan data Anda, Anda dapat meningkatkan kapasitas penyimpanan SSD Amazon Anda FSx untuk sistem file NetApp ONTAP. Untuk sistem file generasi kedua, Anda bahkan dapat mengurangi kapasitas penyimpanan SSD agar sesuai dengan kebutuhan penyimpanan yang berubah dari beban kerja Anda. Gunakan

FSx konsol Amazon, Amazon FSx API, atau AWS Command Line Interface (AWS CLI) untuk menambah atau mengurangi kapasitas penyimpanan SSD. Untuk informasi selengkapnya, lihat [Memperbarui kapasitas penyimpanan dan IOPS yang disediakan](#).

Kapan meningkatkan kapasitas penyimpanan SSD

Jika Anda kehabisan penyimpanan tingkat SSD yang tersedia, kami sarankan Anda meningkatkan kapasitas penyimpanan sistem file Anda. Kehabisan penyimpanan menunjukkan bahwa tingkat SSD Anda berukuran terlalu kecil untuk bagian aktif kumpulan data Anda.

Untuk memantau jumlah penyimpanan gratis yang tersedia di sistem file, gunakan metrik tingkat sistem file dan `StorageCapacity` `StorageUsed` Amazon CloudWatch . Anda dapat membuat CloudWatch alarm pada metrik dan diberi tahu saat turun di bawah ambang batas tertentu. Untuk informasi selengkapnya, lihat [Pemantauan CloudWatch dengan Amazon](#).

Note

Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan kapasitas penyimpanan SSD untuk memastikan bahwa tiering data, penskalaan throughput, dan aktivitas pemeliharaan lainnya berfungsi dengan baik, dan bahwa ada kapasitas yang tersedia untuk data tambahan. Untuk sistem file generasi kedua, rekomendasi ini berlaku untuk pemanfaatan rata-rata di semua agregat sistem file Anda dan untuk setiap agregat individu.

Untuk informasi selengkapnya tentang bagaimana penyimpanan SSD sistem file digunakan dan berapa banyak penyimpanan SSD yang dicadangkan untuk metadata file dan perangkat lunak operasi, lihat. [Memilih jumlah penyimpanan SSD sistem file yang tepat](#)

Meningkatkan kapasitas penyimpanan SSD

Saat Anda meningkatkan kapasitas penyimpanan SSD dari sistem FSx file Amazon Anda, kapasitas baru biasanya tersedia untuk digunakan dalam beberapa menit. Anda ditagih untuk kapasitas penyimpanan SSD baru setelah tersedia untuk Anda. Untuk informasi selengkapnya, lihat [Amazon FSx untuk Harga NetApp ONTAP](#) dan [AWS laporan penagihan dan penggunaan FSx untuk ONTAP](#).

Setelah Anda meningkatkan kapasitas penyimpanan, Amazon FSx menjalankan proses pengoptimalan penyimpanan di latar belakang untuk menyeimbangkan kembali data Anda. Untuk sebagian besar sistem file, pengoptimalan penyimpanan membutuhkan waktu beberapa jam dengan dampak nyata minimal terhadap kinerja beban kerja Anda.

Anda dapat melacak kemajuan proses pengoptimalan penyimpanan kapan saja dengan menggunakan FSx konsol Amazon, AWS CLI, dan API. Untuk informasi selengkapnya, lihat [Memantau kapasitas penyimpanan dan pembaruan IOPS](#).

Pertimbangan untuk meningkatkan kapasitas penyimpanan SSD

Berikut adalah beberapa hal penting yang perlu dipertimbangkan saat meningkatkan kapasitas penyimpanan SSD dan IOPS sistem file Anda:

- (Hanya sistem file generasi pertama) Kapasitas penyimpanan hanya meningkat — Anda hanya dapat meningkatkan jumlah kapasitas penyimpanan SSD untuk sistem file; Anda tidak dapat mengurangi kapasitas penyimpanan.
- Peningkatan kapasitas penyimpanan minimum - Setiap peningkatan kapasitas penyimpanan SSD harus minimal 10% dari kapasitas penyimpanan SSD sistem file saat ini, hingga kapasitas penyimpanan SSD maksimum untuk konfigurasi sistem file Anda.
- Waktu antara peningkatan — Setelah meningkatkan kapasitas penyimpanan SSD, IOPS yang disediakan, atau kapasitas throughput pada sistem file, Anda harus menunggu setidaknya enam jam sebelum memodifikasi konfigurasi ini pada sistem file yang sama lagi. Ini terkadang disebut sebagai periode pendinginan.
- Mode IOPS yang disediakan — Untuk perubahan IOPS yang disediakan, Anda harus menentukan salah satu dari dua mode IOPS:
 - Mode otomatis - Amazon FSx secara otomatis menskalakan IOPS SSD Anda untuk mempertahankan 3 IOPS SSD yang disediakan per GiB kapasitas penyimpanan SSD, hingga IOPS SSD maksimum untuk konfigurasi sistem file Anda.

Note

Untuk informasi selengkapnya tentang jumlah maksimum IOPS SSD yang dapat Anda berikan untuk sistem file ONTAP, lihat. FSx [Dampak kapasitas throughput terhadap performa](#)

- Mode yang disediakan pengguna - Anda menentukan jumlah IOPS SSD, yang harus lebih besar dari atau sama dengan 3 IOPS per GiB kapasitas penyimpanan SSD. Jika Anda memilih untuk memberikan tingkat IOPS yang lebih tinggi, Anda membayar IOPS rata-rata yang disediakan di atas tarif yang disertakan untuk bulan tersebut, yang diukur dalam IOP-bulan.

Untuk informasi selengkapnya tentang harga, lihat [Amazon FSx untuk Harga NetApp ONTAP](#).

Kapan mengurangi kapasitas penyimpanan SSD

Anda mungkin ingin mengurangi kapasitas penyimpanan SSD sistem file generasi kedua ONTAP dalam skenario seperti berikut: FSx

- Setelah menyelesaikan beban kerja berbasis proyek di mana penyimpanan berkinerja tinggi tidak lagi diperlukan
- Setelah menyelesaikan migrasi data skala besar di mana kapasitas ekstra sementara digunakan untuk mempercepat konsumsi data

Mengurangi kapasitas penyimpanan SSD

Ketika Anda mengurangi kapasitas penyimpanan SSD dari sistem file Anda, Amazon FSx melampirkan set disk (agregat) baru yang lebih kecil ke masing-masing pasangan HA sistem file Anda. Amazon FSx kemudian menjalankan proses pengoptimalan penyimpanan di latar belakang untuk memindahkan data per volume dari disk lama ke disk baru. Setelah data di setiap volume dipindahkan, Amazon FSx mengalihkan akses klien ke volume pada disk baru. Amazon FSx kemudian melepaskan disk lama dari sistem file Anda.

Anda ditagih untuk ukuran tingkat SSD yang ada dan yang baru diminta selama operasi penurunan SSD. Misalnya, ketika Anda mengurangi kapasitas penyimpanan SSD dari 10 tebibytes (TiB) menjadi 5 TiB, Anda ditagih sebesar 15 TiB selama operasi penurunan SSD dan 5 TiB setelah operasi penurunan SSD selesai. Untuk informasi selengkapnya tentang penagihan, lihat [AWS laporan penagihan dan penggunaan FSx untuk ONTAP](#).

Penurunan kapasitas penyimpanan SSD dapat memakan waktu antara beberapa jam dan beberapa minggu tergantung pada faktor-faktor seperti jumlah data yang disimpan pada sistem file Anda, jumlah penulisan net-new yang didorong ke sistem file Anda selama operasi penurunan, dan jumlah sumber daya jaringan dan disk yang tersedia pada sistem file.

Selama operasi penurunan, data Anda tetap tersedia untuk dibaca dan ditulis. Sebagian besar beban kerja mengalami dampak kinerja minimal, meskipun beban kerja berat tulis mungkin mengalami penurunan kinerja sementara. I/O Jeda singkat (hingga 60 detik) mungkin terjadi karena akses klien dialihkan ke disk baru untuk setiap volume.

Untuk meminimalkan dampak kinerja, Anda harus mempertahankan headroom yang memadai di sistem file Anda dengan memastikan bahwa beban kerja yang sedang berlangsung tidak secara konsisten mengkonsumsi lebih dari 50% CPU, 50% disk throughput, atau 50% SSD IOPS sebelum

memulai operasi penurunan SSD. Anda dapat memantau metrik pemanfaatan ini di tab Pemantauan & kinerja sistem file Anda di konsol Amazon FSx .

Note

Jika tingkat penyimpanan SSD Anda melebihi 80% pemanfaatan selama operasi penurunan, Amazon FSx menghentikan operasi dan secara otomatis melanjutkannya setelah pemanfaatan turun di bawah 80%. Untuk mengurangi pemanfaatan SSD pada disk baru, Anda dapat mengatur data ke kumpulan kapasitas atau menghapus data dari volume yang akses kliennya telah berhasil dialihkan ke set disk baru.

Jika Anda memerlukan kapasitas SSD tambahan selama operasi penurunan, Anda dapat mengajukan permintaan untuk meningkatkan kapasitas SSD dengan memanggil [update-file-system](#) AWS CLI atau operasi [UpdateFileSystem](#) API yang setara dan memberikan nilai target baru. Amazon FSx memprioritaskan menyelesaikan permintaan peningkatan SSD, sehingga kapasitas SSD baru tersedia untuk digunakan dalam beberapa menit sebelum melanjutkan operasi penurunan SSD.

Pertimbangan untuk mengurangi kapasitas penyimpanan SSD

Berikut adalah beberapa hal penting yang perlu dipertimbangkan saat mengurangi kapasitas penyimpanan SSD sistem file dan IOPS yang disediakan:

- Meningkatkan kapasitas penyimpanan selama operasi yang berkurang — Anda dapat meningkatkan kapasitas penyimpanan SSD dari sistem file Anda bahkan saat operasi yang berkurang sedang berlangsung. Fleksibilitas ini memungkinkan Anda untuk memastikan kinerja dan ketersediaan jika agregat Anda terisi selama operasi penurunan. Jika Anda meningkatkan kapasitas SSD ke ukuran yang lebih rendah dari kapasitas aslinya, Amazon FSx hanya menyesuaikan ukuran agregat (target) yang baru diminta. Namun, jika Anda meningkatkan kapasitas SSD ke ukuran yang lebih besar dari aslinya, Amazon FSx meningkatkan ukuran kedua agregat agar sesuai dengan nilai target baru. Misalnya, jika Anda mengurangi kapasitas penyimpanan dari 10.000 GiB menjadi 5.000 GiB, dan kemudian meminta peningkatan menjadi 7.000 GiB, hanya agregat target yang ditingkatkan menjadi 7.000 GiB, menghasilkan kapasitas penyimpanan SSD akhir 7.000 GiB untuk sistem file Anda. Tetapi jika Anda meminta peningkatan menjadi 12.000 GiB, kedua agregat ditingkatkan menjadi 12.000 GiB. Kami menyarankan perencanaan yang cermat untuk menghindari skenario di mana Anda harus meningkatkan kapasitas SSD ke ukuran yang sama dengan atau lebih besar dari kapasitas SSD asli.

- FSx Menjeda penurunan SSD — Amazon menghentikan operasi penurunan SSD jika Anda melebihi 80% pemanfaatan pada agregat baru dan secara otomatis melanjutkan operasi penurunan setelah pemanfaatan turun di bawah 80%.
- (Hanya sistem file Single-AZ generasi kedua) Penyebaran kapasitas penyimpanan — Kapasitas penyimpanan baru atau IOPS SSD yang Anda pilih untuk sistem file Anda tersebar merata di setiap agregat sistem file Anda.
- Penambalan selama penurunan kapasitas penyimpanan — Amazon FSx membatalkan pemindahan data untuk volume jika sistem file Anda ditambah selama operasi penurunan SSD. Akibatnya, Anda mungkin kehilangan kemajuan pada operasi penurunan SSD jika tambalan terjadi selama operasi. Amazon FSx secara otomatis memulai ulang `vol move` setelah operasi tambalan selesai.
- Mode IOPS yang disediakan — Untuk perubahan IOPS yang disediakan, Anda harus menentukan salah satu dari dua mode IOPS:
 - Mode otomatis - Amazon FSx secara otomatis menskalakan IOPS SSD Anda untuk mempertahankan 3 IOPS SSD yang disediakan per GiB kapasitas penyimpanan SSD, hingga IOPS SSD maksimum untuk konfigurasi sistem file Anda. Saat mengurangi kapasitas SSD, IOPS SSD otomatis Anda akan turun secara proporsional.

 Note

Untuk informasi selengkapnya tentang jumlah maksimum IOPS SSD yang dapat Anda berikan untuk sistem file ONTAP, lihat. FSx [Dampak kapasitas throughput terhadap performa](#)

- Mode yang disediakan pengguna - Anda harus memberikan nilai IOPS yang sama dengan atau lebih tinggi dari IOPS yang Anda sediakan saat ini. Saat mengurangi kapasitas SSD, Anda dapat mempertahankan IOPS SSD tambahan yang disediakan pengguna selama mereka tidak melebihi IOPS SSD maksimum yang didukung oleh agregat yang lebih kecil (50 IOPS per GB kapasitas SSD yang diminta). Jika IOPS yang Anda sediakan lebih tinggi dari maksimum yang didukung oleh agregat yang lebih kecil, kurangi IOPS sebelum mengurangi kapasitas SSD.
- Jenis volume yang tidak didukung - Amazon FSx tidak mendukung penurunan kapasitas penyimpanan pada sistem file dengan SnapLock volume, volume offline FlexClones, atau volume perlindungan data (DP) yang tidak berisi snapshot apa pun.
- Operasi yang Tidak Didukung Selama Penyusutan — Anda tidak dapat offline volume, memindahkan volume, membuat FlexClones, membuat SnapLock volume, atau memodifikasi pengaturan efisiensi penyimpanan volume selama operasi penurunan.

Keterbatasan untuk mengurangi kapasitas penyimpanan SSD

Batasan berikut berlaku saat mengurangi kapasitas penyimpanan SSD dari sistem file Anda:

- (Hanya sistem file generasi kedua) Penurunan kapasitas penyimpanan — Anda dapat mengurangi kapasitas penyimpanan hanya pada sistem file generasi kedua.
- Penurunan kapasitas penyimpanan minimum - Setiap penurunan kapasitas penyimpanan SSD harus minimal 9 persen dari kapasitas penyimpanan SSD sistem file saat ini. Penurunan ini juga harus memastikan bahwa kapasitas SSD yang dihasilkan sistem file Anda tidak melebihi 80% pemanfaatan setelah operasi berkurang. Misalnya, jika sistem file Anda memiliki kapasitas penyimpanan 10.000 GiB dan 5.000 GiB penyimpanan yang digunakan, Anda dapat mengurangi kapasitas penyimpanan hingga 6.251 GiB sehingga pemanfaatan SSD Anda tetap di bawah 80%. Anda dapat mengurangi kapasitas penyimpanan SSD hingga ukuran minimum yang didukung 1.024 GiB per pasangan HA.
- Untuk mengurangi kapasitas penyimpanan SSD pada sistem file yang berisi satu atau lebih volume dengan lebih dari 50 TiB data di tingkat SSD, Anda harus menyediakan setidaknya 1.536 kapasitas throughput per MB/s pasangan HA. Jika ada volume yang berisi lebih dari 100 TiB data di tingkat SSD, Anda harus menyediakan setidaknya 3.072 kapasitas throughput per MB/s pasangan HA. Untuk volume dengan lebih dari 200 TiB data di tingkat SSD, Anda harus menyediakan 6.144 kapasitas throughput per MB/s pasangan HA.
- Waktu antara pembaruan — Setelah memodifikasi kapasitas penyimpanan SSD, IOPS yang disediakan, atau kapasitas throughput pada sistem file, Anda harus menunggu setidaknya enam jam sebelum memodifikasi konfigurasi ini pada sistem file yang sama lagi. Ini terkadang disebut sebagai periode pendinginan.
- Anda dapat meningkatkan tetapi tidak mengurangi kapasitas throughput untuk sistem file Anda
- Anda tidak dapat menambahkan pasangan HA ke sistem file Anda
- Anda tidak dapat mengembalikan volume ke status sebelumnya (menggunakan `volume snapshot restore`) saat data dalam volume tersebut dipindahkan ke agregat baru. Namun, Anda dapat menjalankan `volume snapshot restore` volume lain yang tidak dipindahkan saat ini.

Membuat alarm pemanfaatan kapasitas penyimpanan untuk sistem file Anda

Kami menyarankan agar Anda tidak melebihi pemanfaatan kapasitas penyimpanan SSD rata-rata 80% secara berkelanjutan. Lonjakan pemanfaatan penyimpanan SSD sesekali di atas 80% dapat diterima. Mempertahankan penggunaan rata-rata di bawah 80% memberi Anda kapasitas

yang cukup untuk meningkatkan penyimpanan Anda tanpa mengalami masalah. Prosedur berikut menunjukkan cara membuat CloudWatch alarm yang memberi tahu Anda kapan penggunaan penyimpanan SSD sistem file Anda mendekati 80%.

Untuk membuat alarm pemanfaatan kapasitas penyimpanan sistem file

Anda dapat menggunakan `StorageCapacityUtilization` metrik untuk membuat alarm yang dipicu ketika satu atau lebih sistem file ONTAP Anda FSx telah mencapai ambang batas pemanfaatan penyimpanan.

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Di panel navigasi kiri, di bawah Alarm, pilih Semua alarm. Kemudian, pilih Buat alarm. Dalam wizard buat alarm, pilih Pilih metrik.
3. Di penjelajah grafik, pilih tab Kueri multi sumber.
4. Di pembuat kueri, pilih yang berikut ini:
 - Untuk Namespace, pilih AWS/FSx> Metrik Sistem File Terperinci.
 - Untuk nama Metrik, pilih MAX (`StorageCapacityUtilization`).
 - Untuk Filter by, Anda dapat secara opsional menyertakan atau mengecualikan sistem file tertentu dengan ID mereka. Jika Anda membiarkan Filter kosong, alarm Anda akan terpicu ketika salah satu sistem file Anda melebihi ambang batas pemanfaatan kapasitas penyimpanan alarm Anda.
 - Biarkan sisa opsi kosong, dan pilih Kueri grafik.
5. Pilih Pilih Metrik. Kembali ke wizard, di bagian Metrik, berikan label pada metrik Anda. Kami merekomendasikan untuk menjaga Periode hingga 5 menit.
6. Di bawah Kondisi, pilih jenis ambang Statis, setiap kali metrik Anda lebih besar/sama dengan 80.
7. Pilih Berikutnya untuk pergi ke halaman Configure actions.

Untuk mengkonfigurasi tindakan alarm

Anda dapat mengonfigurasi berbagai tindakan agar alarm dapat dipicu saat mencapai ambang batas yang Anda konfigurasi. Dalam contoh ini, kami memilih topik Simple Notification Service (SNS), tetapi Anda dapat mempelajari tentang tindakan lain di Menggunakan [CloudWatch alarm Amazon](#) di Panduan Pengguna Amazon. CloudWatch

1. Di bagian Pemberitahuan, pilih topik SNS untuk memberi tahu saat alarm Anda dalam status. ALARM Anda dapat memilih topik yang ada atau membuat yang baru. Anda akan menerima

pemberitahuan berlangganan yang perlu Anda konfirmasi sebelum menerima pemberitahuan alarm ke alamat email.

2. Pilih Berikutnya.

Untuk menyelesaikan alarm

Ikuti petunjuk ini untuk menyelesaikan proses pembuatan CloudWatch alarm Anda.

1. Pada halaman Tambahkan nama dan deskripsi, beri nama alarm Anda, dan deskripsi opsional, lalu pilih Berikutnya.
2. Tinjau semua yang telah Anda konfigurasi di halaman Pratinjau dan buat, lalu pilih Buat alarm.

Memperbarui kapasitas penyimpanan dan IOPS yang disediakan

Anda dapat menambah atau mengurangi penyimpanan berbasis SSD sistem file dan jumlah IOPS SSD yang disediakan dengan menggunakan FSx konsol Amazon, API, dan API. AWS CLI

Untuk meningkatkan kapasitas penyimpanan SSD atau IOPS yang disediakan untuk sistem file (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Sistem file. Dalam daftar Sistem file, pilih sistem file ONTAP FSx untuk yang ingin Anda perbarui kapasitas penyimpanan SSD dan IOPS SSD.
3. Pilih Tindakan > Perbarui kapasitas penyimpanan. Atau, di bagian Ringkasan, pilih Perbarui di sebelah nilai kapasitas penyimpanan SSD sistem file.
4. Untuk meningkatkan kapasitas penyimpanan SSD, pilih Ubah kapasitas penyimpanan.
5. Untuk jenis Input, pilih salah satu dari berikut ini:
 - Untuk memasukkan kapasitas penyimpanan SSD baru sebagai persentase perubahan dari nilai saat ini, pilih Persentase.
 - Untuk memasukkan nilai baru di GiB, pilih Absolute.
6. Tergantung pada jenis input, masukkan nilai untuk kenaikan% yang diinginkan.
 - Untuk Persentase, masukkan nilai kenaikan persentase. Nilai ini harus setidaknya 10 persen lebih besar dari nilai saat ini.
 - Untuk Absolute, masukkan nilai baru di GiB, hingga nilai maksimum yang diizinkan 196.608 GiB.

7. Untuk Provisioned SSD IOPS, Anda memiliki dua opsi untuk mengubah jumlah IOPS SSD yang disediakan untuk sistem file Anda:
 - Jika Anda FSx ingin Amazon secara otomatis menskalakan IOPS SSD Anda untuk mempertahankan 3 IOPS SSD yang disediakan per GiB kapasitas penyimpanan SSD (hingga maksimum 160.000), pilih Otomatis.
 - Jika Anda ingin menentukan jumlah IOPS SSD, pilih User-provisioned. Masukkan jumlah absolut IOPS yang setidaknya tiga kali jumlah GiB dari tingkat penyimpanan SSD Anda, dan kurang dari atau sama dengan 160.000.

 Note

Untuk informasi selengkapnya tentang jumlah maksimum IOPS SSD yang dapat Anda berikan untuk sistem file ONTAP, lihat. FSx [Dampak kapasitas throughput terhadap performa](#)

8. Pilih Perbarui.

 Note

Di bagian bawah prompt, pratinjau konfigurasi ditampilkan untuk kapasitas penyimpanan SSD baru Anda dan IOPS SSD. Untuk sistem file generasi kedua, per-HA-pair nilainya juga ditampilkan.

Untuk meningkatkan kapasitas penyimpanan SSD dan menyediakan IOPS untuk sistem file (CLI)

Untuk meningkatkan kapasitas penyimpanan SSD dan IOPS yang disediakan untuk sistem file ONTAP, gunakan AWS CLI perintah [update-file-system](#) atau tindakan API yang setara. FSx [UpdateFileSystem](#) Tetapkan parameter berikut dengan nilai Anda:

- Atur `--file-system-id` ke ID dari sistem file yang Anda perbarui.
- Untuk meningkatkan kapasitas penyimpanan SSD Anda, atur `--storage-capacity` ke nilai kapasitas penyimpanan target, yang harus setidaknya 10 persen lebih besar dari nilai saat ini.
- Untuk memodifikasi IOPS SSD yang disediakan, gunakan properti. `--ontap-configuration DiskIopsConfiguration` Properti ini memiliki dua parameter, `Iops` dan `Mode`:

- Jika Anda ingin menentukan jumlah IOPS yang disediakan, gunakan `Iops=number_of_IOPS` (hingga maksimum 160.000) dan. `Mode=USER_PROVISIONED` Nilai IOPS harus lebih besar dari atau sama dengan tiga kali kapasitas penyimpanan SSD yang diminta. Jika Anda tidak meningkatkan kapasitas penyimpanan, IOPS nilainya harus lebih besar dari atau sama dengan tiga kali kapasitas penyimpanan SSD saat ini.
- Jika Anda FSx ingin Amazon meningkatkan IOPS SSD Anda secara otomatis, gunakan `Mode=AUTOMATIC` dan jangan gunakan Iops parameternya. Amazon FSx akan secara otomatis mempertahankan 3 SSD IOPS per GiB dari kapasitas penyimpanan SSD yang disediakan (hingga maksimum 160.000).

Note

Untuk informasi selengkapnya tentang jumlah maksimum IOPS SSD yang dapat Anda berikan untuk sistem file ONTAP, lihat. FSx [Dampak kapasitas throughput terhadap performa](#)

Contoh berikut meningkatkan penyimpanan SSD sistem file menjadi 2000 GiB dan menetapkan jumlah IOPS SSD yang disediakan pengguna menjadi 7000.

```
aws fsx update-file-system \  
--file-system-id fs-0123456789abcdef0 \  
--storage-capacity 2000 \  
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

Untuk memantau kemajuan pembaruan, gunakan [describe-file-systems](#) AWS CLI perintah. Cari `AdministrativeActions` bagian dalam output.

Untuk informasi selengkapnya, lihat [AdministrativeAction](#) di Amazon FSx untuk Referensi API NetApp ONTAP.

Untuk mengurangi kapasitas penyimpanan SSD untuk sistem file (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Sistem file. Dalam daftar Sistem file, pilih sistem file ONTAP FSx untuk yang ingin Anda perbarui kapasitas penyimpanan SSD dan IOPS SSD.
3. Pilih Tindakan > Perbarui sistem file > Perbarui kapasitas penyimpanan SSD/IOPS. Atau, di bagian Ringkasan, pilih Perbarui di sebelah nilai kapasitas penyimpanan SSD sistem file.

4. Untuk mengurangi kapasitas penyimpanan SSD, untuk tipe Action, pilih Kurangi.
5. Untuk jenis Input, pilih salah satu dari berikut ini:
 - Untuk memasukkan kapasitas penyimpanan SSD baru sebagai persentase perubahan dari nilai saat ini, pilih Persentase.
 - Untuk memasukkan nilai baru di GiB, pilih Absolute.
6. Tergantung pada jenis input, lakukan salah satu hal berikut.
 - Untuk Persentase, masukkan nilai penurunan% yang diinginkan. Nilai ini harus setidaknya 9 persen lebih rendah dari nilai saat ini.
 - Untuk Absolute, masukkan nilai kapasitas penyimpanan yang diinginkan di GiB.
7. Pilih Perbarui.

 Note

Di bagian bawah prompt, pratinjau konfigurasi ditampilkan untuk kapasitas penyimpanan SSD baru Anda dan IOPS SSD. Untuk sistem file generasi kedua, per-HA-pair nilainya juga ditampilkan.

Untuk mengurangi kapasitas penyimpanan SSD dan menyediakan IOPS untuk sistem file (CLI)

Untuk mengurangi kapasitas penyimpanan SSD dan IOPS yang disediakan untuk sistem file ONTAP, gunakan AWS CLI perintah [update-file-system](#) atau tindakan API yang setara. FSx [UpdateFileSystem](#). Tetapkan parameter berikut dengan nilai Anda:

1. Untuk mengurangi kapasitas SSD, gunakan perintah berikut:

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 4096
```

Jika Anda menggunakan mode IOPS yang disediakan pengguna dan ingin mempertahankan level IOPS Anda saat ini, sertakan parameternya: `DiskIopsConfiguration`

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 4096 \
```

```
--ontap-configuration 'DiskIopsConfiguration={Iops=15000,Mode=USER_PROVISIONED}'
```

2. Untuk memantau kemajuan operasi penurunan, gunakan `describe-file-systems` perintah:

```
aws fsx describe-file-systems --file-system-id fs-0123456789abcdef0
```

Perintah mengembalikan informasi tentang operasi penurunan di `AdministrativeActions` bagian tersebut. Contoh:

```
{
  "FileSystem": {
    "StorageCapacity": 4096,
    "StorageType": "SSD",
    "AdministrativeActions": [
      {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "Message": "Moving data for [vol1 vol2]. 2 volume(s) remaining.
https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/troubleshooting.html",
        "ProgressPercent": 4,
        "RequestTime": 1748981251.591,
        "Status": "IN_PROGRESS",
        "TargetFileSystemValues": {
          "StorageCapacity": 4096
        }
      }
    ]
  }
}
```

Untuk memantau kemajuan pembaruan, gunakan [describe-file-systems](#) AWS CLI perintah. Cari `AdministrativeActions` bagian dalam output.

Untuk informasi selengkapnya, lihat [AdministrativeAction](#) di Amazon FSx untuk Referensi API NetApp ONTAP.

Memperbarui kapasitas penyimpanan secara dinamis

Anda dapat menggunakan solusi berikut untuk secara dinamis meningkatkan kapasitas penyimpanan SSD dari sistem file FSx untuk ONTAP ketika jumlah kapasitas penyimpanan SSD yang digunakan melebihi ambang batas yang Anda tentukan. AWS CloudFormation Template ini secara otomatis menyebarkan semua komponen yang diperlukan untuk menentukan ambang kapasitas

penyimpanan, CloudWatch alarm Amazon berdasarkan ambang batas ini, dan AWS Lambda fungsi yang meningkatkan kapasitas penyimpanan sistem file.

Solusinya secara otomatis menyebarkan semua komponen yang dibutuhkan, dan menggunakan parameter berikut:

- ID sistem file FSx untuk ONTAP Anda.
- Ambang kapasitas penyimpanan SSD yang digunakan (nilai numerik). Ini adalah persentase di mana CloudWatch alarm akan dipicu.
- Persentase yang digunakan untuk meningkatkan kapasitas penyimpanan (%).
- Alamat email yang digunakan untuk menerima pemberitahuan penskalaan.

Topik

- [Gambaran umum arsitektur](#)
- [CloudFormation Template](#)
- [Penerapan otomatis dengan CloudFormation](#)

Gambaran umum arsitektur

Men-deploy solusi ini untuk membangun sumber daya berikut di AWS Cloud.

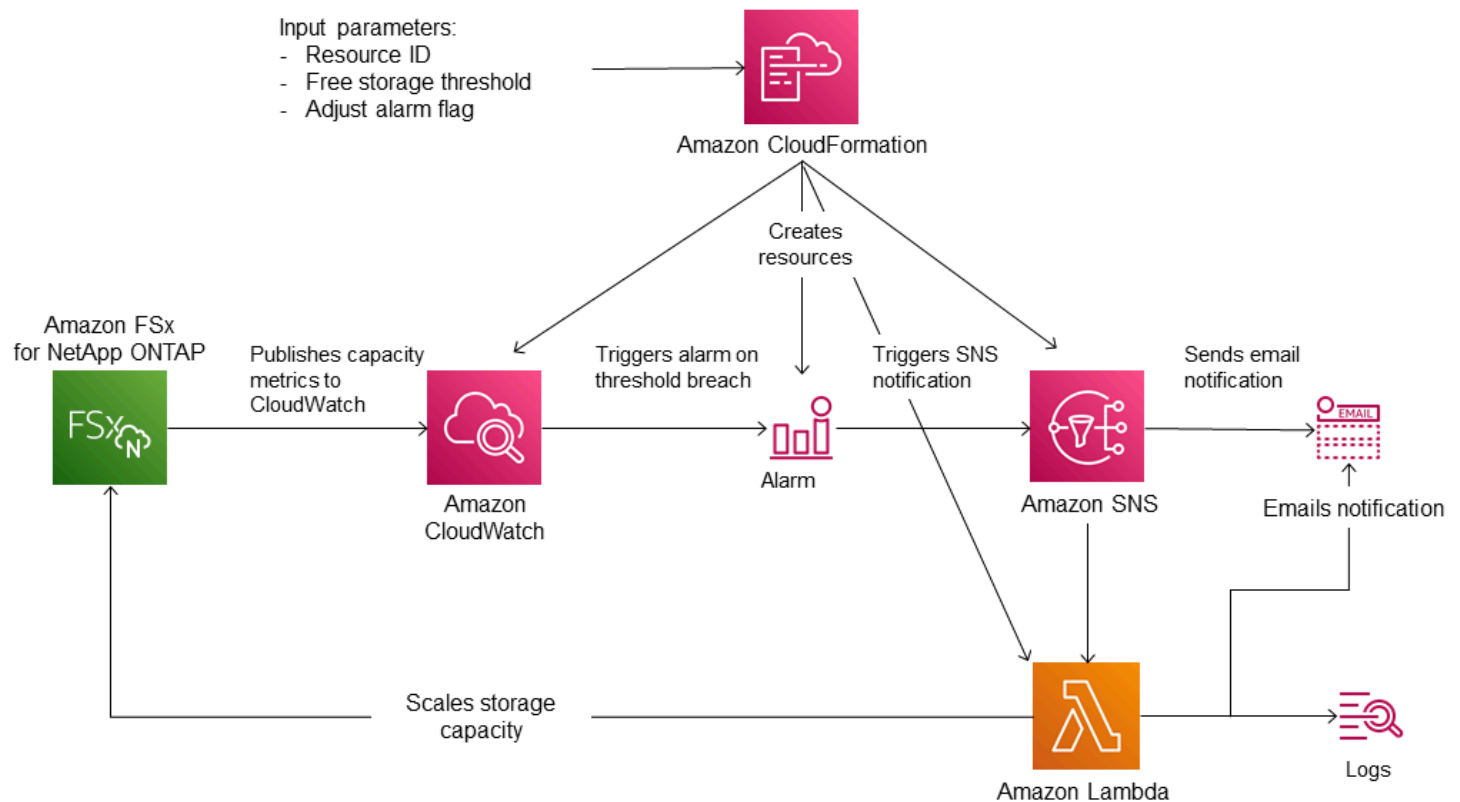


Diagram ini menggambarkan langkah-langkah berikut:

1. CloudFormation Template menyebarkan CloudWatch alarm, AWS Lambda fungsi, antrian 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 yang digunakan sistem file melebihi ambang batas yang ditentukan, dan mengirim pesan ke antrian Amazon SNS. Alarm dipicu hanya ketika kapasitas yang digunakan sistem file melebihi ambang batas terus menerus selama periode 5 menit.
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. 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.

CloudFormation Template

Solusi ini digunakan CloudFormation untuk mengotomatiskan penyebaran komponen yang digunakan untuk secara otomatis meningkatkan kapasitas penyimpanan sistem file FSx untuk ONTAP. Untuk menggunakan solusi ini, unduh [FSxOntapDynamicStorageScaling](#) CloudFormation template.

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. Menentukan ambang kapasitas penyimpanan yang digunakan untuk memicu alarm dan secara otomatis meningkatkan kapasitas penyimpanan sistem file, yang ditentukan dalam persentase (%) dari kapasitas penyimpanan sistem file saat ini. Sistem file dianggap memiliki kapasitas penyimpanan gratis yang rendah ketika penyimpanan yang digunakan melebihi ambang batas ini.

EmailAddress

Tidak ada nilai default. Menentukan alamat email yang akan digunakan untuk langganan SNS dan menerima peringatan ambang kapasitas penyimpanan.

PercentIncrease

Default adalah 20%. Tentukan jumlah yang digunakan untuk meningkatkan kapasitas penyimpanan, yang dinyatakan sebagai persentase dari kapasitas penyimpanan saat ini.

Note

Penskalaan penyimpanan dicoba sekali setiap kali CloudWatch alarm memasuki status. ALARM Jika pemanfaatan kapasitas penyimpanan SSD Anda tetap di atas ambang batas setelah operasi penskalaan penyimpanan dicoba, operasi penskalaan penyimpanan tidak dicoba lagi.

Maks FSx SizeinGi B

Defaultnya adalah 196608. Menentukan kapasitas penyimpanan maksimum yang didukung untuk penyimpanan SSD.

Penerapan otomatis dengan CloudFormation

Prosedur berikut mengkonfigurasi dan menyebarkan CloudFormation tumpukan untuk secara otomatis meningkatkan kapasitas penyimpanan FSx untuk sistem file ONTAP. Dibutuhkan beberapa menit untuk menyebarkan. Untuk informasi selengkapnya tentang membuat CloudFormation tumpukan, lihat [Membuat tumpukan di AWS CloudFormation konsol](#) di Panduan AWS CloudFormation Pengguna.

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 situs Anda. Akun AWS Untuk informasi selengkapnya tentang membuat FSx sumber daya Amazon, lihat [Memulai dengan Amazon FSx untuk NetApp ONTAP](#).

Untuk meluncurkan kapasitas penyimpanan otomatis yang meningkatkan tumpukan solusi

1. Unduh templat [FSxOntapDynamicStorageScaling](#) CloudFormation .

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. Dari CloudFormation konsol, pilih Buat tumpukan> Dengan sumber daya baru.
3. Pilih Template sudah siap. Di bagian Tentukan templat, pilih Unggah file templat dan unggah templat yang Anda unduh.
4. Dalam Spesifikasikan detail tumpukan, masukkan nilai untuk solusi peningkatan kapasitas penyimpanan otomatis Anda.

Stack name

Stack name

FsxN-Storage-Scaling

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Dynamic Storage Scaling Parameters

File system ID
Amazon FSx file system ID

fs-0123456789abcd

Threshold
Used storage capacity threshold (%)

70

Percentage Capacity Increase
The percentage increase in storage capacity when used storage exceeds LowFreeDataStorageCapacityThreshold. Minimum increase is 10 %

20

Email address
The email address for alarm notification.

storagescaler@example.com

Maximum supported file system storage capacity (DO NOT MODIFY)
Maximum size supported for the primary SSD storage tier.

196608

Cancel Previous Next

5. Masukkan Nama tumpukan.
6. Untuk Parameter, tinjau parameter untuk templat dan modifikasi untuk memenuhi kebutuhan sistem file Anda. Lalu pilih Selanjutnya.

 Note

Untuk menerima pemberitahuan email saat penskalaan dicoba oleh CloudFormation templat ini, konfirmasi email langganan SNS yang Anda terima setelah menerapkan templat.

7. Masukkan pengaturan Opsi yang Anda inginkan untuk solusi kustom Anda, lalu pilih Berikutnya.
8. Untuk Meninjau, tinjau dan konfirmasi pengaturan solusi. Pilih kotak centang untuk mengakui bahwa templat membuat sumber daya IAM.
9. Pilih Buat untuk men-deploy tumpukan.

Anda dapat melihat status tumpukan di CloudFormation konsol di kolom Status. Anda akan melihat status CREATE_COMPLETE dalam beberapa 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 .

Memantau pemanfaatan penyimpanan SSD

Anda dapat memantau pemanfaatan kapasitas penyimpanan SSD sistem file Anda menggunakan berbagai AWS NetApp alat. Menggunakan Amazon, CloudWatch Anda dapat memantau pemanfaatan kapasitas penyimpanan dan menyetel alarm untuk mengingatkan Anda ketika pemanfaatan kapasitas penyimpanan mencapai ambang batas yang dapat disesuaikan.

Note

Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan kapasitas penyimpanan dari tingkat penyimpanan SSD Anda. Ini memastikan bahwa tiering berfungsi dengan benar, dan menyediakan overhead untuk data baru. Jika tingkat penyimpanan SSD Anda secara konsisten di atas pemanfaatan kapasitas penyimpanan 80%, Anda dapat meningkatkan kapasitas tingkat penyimpanan SSD Anda. Untuk informasi selengkapnya, lihat [Memperbarui penyimpanan SSD sistem file dan IOPS](#).

Anda dapat melihat penyimpanan SSD sistem file yang tersedia dan distribusi penyimpanan keseluruhan di FSx konsol Amazon. Grafik kapasitas penyimpanan primer yang tersedia menampilkan jumlah kapasitas penyimpanan berbasis SSD yang tersedia pada sistem file dari waktu ke waktu. Grafik distribusi Storage menunjukkan bagaimana kapasitas penyimpanan keseluruhan sistem file saat ini didistribusikan lebih dari 3 kategori:

- Tingkat kolam kapasitas
- SSD tier - tersedia
- SSD tier - digunakan

Anda dapat memantau pemanfaatan kapasitas penyimpanan SSD sistem file Anda di Konsol Manajemen AWS, menggunakan prosedur berikut.

Untuk memantau sistem file tersedia kapasitas penyimpanan SSD tier (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.

2. Pilih Sistem file di kolom navigasi sebelah kiri, lalu pilih sistem ONTAP file yang ingin Anda lihat informasi kapasitas penyimpanan. Halaman detail sistem file muncul.
3. Di panel kedua, pilih tab Monitoring & performance, lalu pilih Storage. Kapasitas penyimpanan utama yang tersedia dan pemanfaatan kapasitas Penyimpanan per grafik agregat ditampilkan.

Memantau penghematan efisiensi penyimpanan

Saat diaktifkan, Anda dapat melihat berapa banyak kapasitas penyimpanan yang Anda hemat di FSx konsol Amazon, CloudWatch konsol Amazon, dan CLI ONTAP.

Untuk melihat penghematan efisiensi penyimpanan (konsol)

Penghematan efisiensi penyimpanan yang ditampilkan di FSx konsol Amazon untuk sistem file FSx untuk ONTAP mencakup penghematan dari FlexClones dan SnapShots.

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Pilih sistem file ONTAP FSx untuk yang ingin Anda lihat hemat efisiensi penyimpanan dari daftar Sistem file.
3. Pilih Ringkasan di tab Pemantauan & kinerja pada panel kedua di halaman detail sistem file.
4. Bagan penghematan efisiensi penyimpanan menunjukkan berapa banyak ruang yang Anda hemat sebagai persentase dari ukuran data logis Anda dan dalam byte fisik.

Untuk melihat penghematan efisiensi penyimpanan (ONTAPCLI)

Anda dapat melihat penghematan efisiensi penyimpanan hanya dari pemadatan, kompresi, dan deduplikasi — tanpa efek snapshot dan FlexClones — dengan menjalankan perintah `storage aggregate show-efficiency` menggunakan CLI. ONTAP Untuk informasi selengkapnya, lihat [efisiensi pertunjukan agregat penyimpanan](#) di Pusat Dokumentasi. NetApp ONTAP

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. `storage aggregate show-efficiency` Perintah menampilkan informasi tentang efisiensi penyimpanan semua agregat. Efisiensi penyimpanan ditampilkan pada empat tingkatan yang berbeda:

- Total
- Agregat
- Volume
- Snapshot dan volume FlexClone

```
::*> aggr show-efficiency
```

```
Aggregate: aggr1
Node: node1
```

```
Total Data Reduction Efficiency Ratio: 3.29:1
```

```
Total Storage Efficiency Ratio: 4.29:1
```

```
Aggregate: aggr2
```

```
Node: node1
```

```
Total Data Reduction Efficiency Ratio: 4.50:1
```

```
Total Storage Efficiency Ratio: 5.49:1
```

```
cluster::*> aggr show-efficiency -details
```

```
Aggregate: aggr1
```

```
Node: node1
```

```
Total Data Reduction Ratio: 2.39:1
```

```
Total Storage Efficiency Ratio: 4.29:1
```

```
Aggregate level Storage Efficiency
```

```
(Aggregate Deduplication and Data Compaction): 1.00:1
```

```
Volume Deduplication Efficiency: 5.03:1
```

```
Compression Efficiency: 1.00:1
```

```
Snapshot Volume Storage Efficiency: 8.81:1
```

```
FlexClone Volume Storage Efficiency: 1.00:1
```

```
Number of Efficiency Disabled Volumes: 1
```

```
Aggregate: aggr2
```

```
Node: node1
```

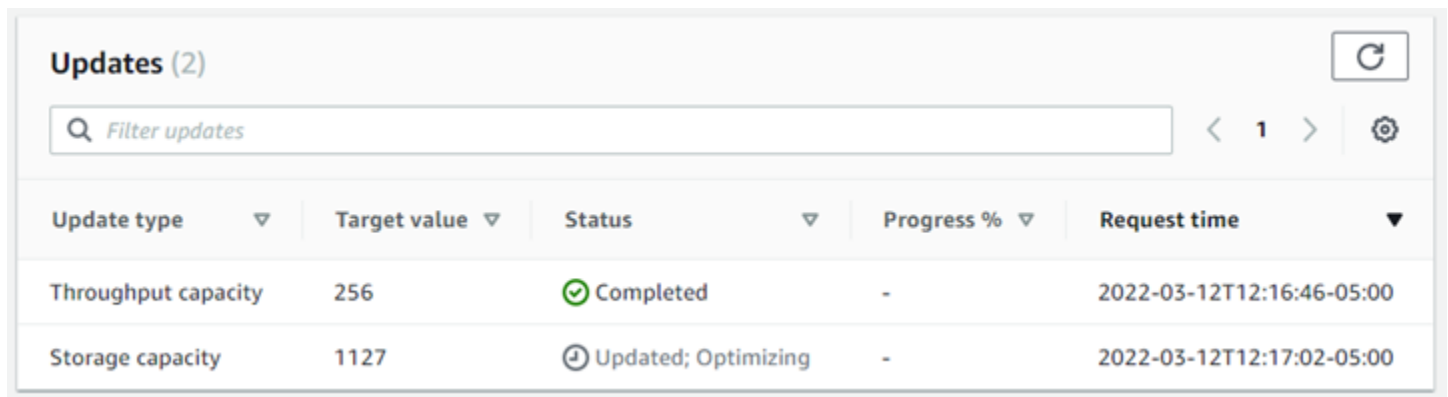
Total Data Reduction Ratio:	2.39:1
Total Storage Efficiency Ratio:	4.29:1
Aggregate level Storage Efficiency (Aggregate Deduplication and Data Compaction):	
Volume Deduplication Efficiency:	1.00:1
Compression Efficiency:	5.03:1
Snapshot Volume Storage Efficiency:	1.00:1
FlexClone Volume Storage Efficiency:	8.81:1
Number of Efficiency Disabled Volumes:	1

Memantau kapasitas penyimpanan dan pembaruan IOPS

Anda dapat memantau kemajuan kapasitas penyimpanan SSD dan pembaruan IOPS dengan menggunakan FSx konsol Amazon, CLI, dan API.

Untuk memantau penyimpanan dan pembaruan IOPS (konsol)

Di tab Pembaruan pada halaman detail sistem file untuk sistem file ONTAP Anda, Anda dapat melihat 10 pembaruan terbaru untuk setiap jenis pembaruan. FSx



Update type	Target value	Status	Progress %	Request time
Throughput capacity	256	Completed	-	2022-03-12T12:16:46-05:00
Storage capacity	1127	Updated; Optimizing	-	2022-03-12T12:17:02-05:00

Untuk kapasitas penyimpanan SSD dan pembaruan IOPS, Anda dapat melihat informasi berikut:

Jenis pembaruan

Jenis yang didukung adalah Kapasitas penyimpanan, Mode, dan IOPS. Nilai Mode dan IOPS terdaftar untuk semua kapasitas penyimpanan dan permintaan penskalaan IOPS.

Nilai target

Nilai yang Anda tentukan untuk memperbarui kapasitas penyimpanan SSD sistem file atau IOPS ke.

Status

Status terkini dari pembaruan. Kemungkinan nilainya adalah sebagai berikut:

- Tertunda - Amazon FSx menerima permintaan pembaruan, tetapi belum mulai memprosesnya.
- Sedang berlangsung - Amazon FSx sedang memproses permintaan pembaruan.
- Diperbarui; Mengoptimalkan - Amazon FSx meningkatkan kapasitas penyimpanan SSD sistem file. Proses optimasi penyimpanan sekarang menyeimbangkan kembali data Anda di latar belakang.
- Selesai - Pembaruan selesai dengan sukses.
- Gagal — Permintaan pembaruan gagal. Pilih tanda tanya (?) untuk melihat detailnya.

Kemajuan%

Menampilkan kemajuan proses pengoptimalan penyimpanan saat persentase selesai.

Waktu permintaan

Waktu Amazon FSx menerima permintaan tindakan pembaruan.

Untuk memantau penyimpanan dan pembaruan IOPS (CLI)

Anda dapat melihat dan memantau sistem file kapasitas penyimpanan SSD meningkatkan dan mengurangi permintaan dengan menggunakan [describe-file-systems](#) AWS CLI perintah dan operasi [DescribeFileSystems](#) API. Array `AdministrativeActions` mencantumkan 10 tindakan pembaruan terbaru untuk setiap jenis tindakan administratif. Saat Anda meningkatkan kapasitas penyimpanan SSD sistem file, dua `AdministrativeActions` tindakan dihasilkan: a `FILE_SYSTEM_UPDATE` dan `STORAGE_OPTIMIZATION` tindakan. Saat Anda mengurangi kapasitas penyimpanan SSD sistem file, hanya satu `AdministrativeActions` tindakan yang dihasilkan: `FILE_SYSTEM_UPDATE` tindakan.

Contoh berikut menunjukkan kutipan respons perintah CLI `describe-file-systems`. Sistem file memiliki tindakan administratif yang tertunda untuk meningkatkan kapasitas penyimpanan SSD menjadi 2000 GiB dan IOPS SSD yang disediakan menjadi 7000.

```
"AdministrativeActions": [  
  {  
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",  
    "RequestTime": 1586797629.095,  
    "Status": "PENDING",
```

```

    "TargetFileSystemValues": {
      "StorageCapacity": 2000,
      "OntapConfiguration": {
        "DiskIopsConfiguration": {
          "Mode": "USER_PROVISIONED",
          "Iops": 7000
        }
      }
    },
    {
      "AdministrativeActionType": "STORAGE_OPTIMIZATION",
      "RequestTime": 1586797629.095,
      "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. Perilaku ini ditunjukkan dalam kutipan berikut dari respons perintah `CLIdescribe-file-systems`.

ProgressPercentProperti menampilkan kemajuan proses optimasi penyimpanan. Setelah proses pengoptimalan penyimpanan berhasil diselesaikan, status FILE_SYSTEM_UPDATE tindakan berubah menjadi COMPLETED, dan STORAGE_OPTIMIZATION tindakan tidak lagi muncul.

```

"AdministrativeActions": [
  {
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
    "RequestTime": 1586799169.445,
    "Status": "UPDATED_OPTIMIZING",
    "TargetFileSystemValues": {
      "StorageCapacity": 2000,
      "OntapConfiguration": {
        "DiskIopsConfiguration": {
          "Mode": "USER_PROVISIONED",
          "Iops": 7000
        }
      }
    }
  }
]

```

```

    },
    {
      "AdministrativeActionType": "STORAGE_OPTIMIZATION",
      "ProgressPercent": 41,
      "RequestTime": 1586799169.445,
      "Status": "IN_PROGRESS"
    }
  ]

```

Saat mengurangi kapasitas SSD, FILE_SYSTEM_UPDATE tindakan tersebut mencakup Message properti yang memberikan informasi tentang volume mana yang saat ini dipindahkan dan berapa volume yang tersisa. Contoh:

```

"AdministrativeActions": [
  {
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
    "Message": "Moving data for [vol1 vol2]. 2 volume(s) remaining. https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/troubleshooting.html",
    "ProgressPercent": 8,
    "RequestTime": 1748981251.591,
    "Status": "IN_PROGRESS",
    "TargetFileSystemValues": {
      "StorageCapacity": 4096,
      "OntapConfiguration": {
        "DiskIopsConfiguration": {
          "Mode": "AUTOMATIC",
          "Iops": 12288
        }
      }
    }
  }
]

```

Jika operasi penurunan SSD dihentikan sementara karena agregat target telah melebihi 80% pemanfaatan, status akan berubah menjadi dengan pesan yang sesuai PAUSED:

```

"AdministrativeActions": [
  {
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
    "Message": "Your file system has insufficient free space in its SSD tier. Please free up space or increase your file system's storage capacity.",
    "ProgressPercent": 8,

```



```

    "RequestTime": 1748981251.591,
    "Status": "PAUSED",
    "TargetFileSystemValues": {
      "StorageCapacity": 4096,
      "OntapConfiguration": {
        "DiskIopsConfiguration": {
          "Mode": "AUTOMATIC",
          "Iops": 12288
        }
      }
    }
  }
}
]

```

Jika kapasitas penyimpanan atau permintaan pembaruan IOPS gagal, status `FILE_SYSTEM_UPDATE` tindakan berubah menjadi `FAILED`, seperti yang ditunjukkan pada contoh berikut. `FailureDetails` properti memberikan informasi tentang kegagalan.

```

"AdministrativeActions": [
  {
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
    "RequestTime": 1586373915.697,
    "Status": "FAILED",
    "TargetFileSystemValues": {
      "StorageCapacity": 2000,
      "OntapConfiguration": {
        "DiskIopsConfiguration": {
          "Mode": "USER_PROVISIONED",
          "Iops": 7000
        }
      }
    },
    "FailureDetails": {
      "Message": "failure-message"
    }
  }
]

```

Kapasitas penyimpanan volume

FSx Volume ONTAP adalah sumber daya virtual yang Anda gunakan untuk mengelompokkan data, menentukan bagaimana data disimpan, dan menentukan jenis akses ke data Anda. Volume, seperti

folder, tidak mengkonsumsi kapasitas penyimpanan sistem file itu sendiri. Hanya data yang disimpan dalam volume yang mengkonsumsi penyimpanan SSD dan, tergantung pada [kebijakan tingkatan volume](#), penyimpanan kolam kapasitas. Anda mengatur ukuran volume saat Anda membuatnya, dan Anda dapat mengubah ukurannya nanti. Anda dapat memantau dan mengelola kapasitas penyimpanan FSx untuk volume ONTAP Anda menggunakan Konsol Manajemen AWS, AWS CLI dan API, dan CLI ONTAP.

Topik

- [Tingkat data volume](#)
- [Snapshot dan kapasitas penyimpanan volume](#)
- [Kapasitas file volume](#)
- [Mengelola efisiensi penyimpanan](#)
- [Mengaktifkan autosizing](#)
- [Mengaktifkan mode tulis cloud](#)
- [Memperbarui kapasitas penyimpanan](#)
- [Memperbarui kebijakan tiering](#)
- [Memperbarui hari pendinginan minimum](#)
- [Memperbarui kebijakan pengambilan cloud volume](#)
- [Memperbarui jumlah maksimum file pada volume](#)
- [Memantau kapasitas penyimpanan volume](#)
- [Memantau kapasitas file volume](#)

Tingkat data volume

Amazon FSx untuk sistem file NetApp ONTAP memiliki dua tingkatan penyimpanan: penyimpanan utama dan penyimpanan kolam kapasitas. Penyimpanan primer disediakan, dapat diskalakan, penyimpanan SSD berkinerja tinggi yang dibuat khusus untuk bagian aktif kumpulan data Anda. Penyimpanan kolam kapasitas adalah tingkat penyimpanan yang sepenuhnya elastis yang dapat menskalakan hingga ukuran petabyte dan dioptimalkan biaya untuk data yang jarang diakses.

Data pada setiap volume secara otomatis berjenjang ke tingkat penyimpanan kumpulan kapasitas berdasarkan kebijakan tingkatan volume, periode pendinginan, dan pengaturan ambang batas. Bagian berikut menjelaskan kebijakan tingkatan ONTAP volume dan ambang batas yang digunakan untuk menentukan kapan data berjenjang ke kumpulan kapasitas.

Note

FSx untuk ONTAP mendukung tiering data ke kumpulan kapasitas pada semua SnapLock volume, apa pun jenisnya. SnapLock Untuk informasi selengkapnya, lihat [Cara kerja SnapLock](#).

Kebijakan tingkatan volume

Anda menentukan cara menggunakan tingkatan penyimpanan sistem file ONTAP Anda FSx dengan memilih kebijakan tiering untuk setiap volume pada sistem file. Anda memilih kebijakan tiering saat membuat volume, dan Anda dapat memodifikasinya kapan saja dengan FSx konsol Amazon, API AWS CLI, atau menggunakan [alat NetApp manajemen](#). Anda dapat memilih dari salah satu kebijakan berikut yang menentukan data mana, jika ada, yang berjenjang ke penyimpanan kumpulan kapasitas.

Note

Tiering dapat memindahkan data file dan data snapshot Anda ke tingkat kumpulan kapasitas. Namun, metadata file selalu tetap pada tingkat SSD. Untuk informasi selengkapnya, lihat [Bagaimana penyimpanan SSD digunakan](#).

- Otomatis — Kebijakan ini memindahkan semua data dingin—data pengguna dan snapshot—ke tingkat kumpulan kapasitas. Tingkat pendinginan data ditentukan oleh periode pendinginan kebijakan, yang secara default adalah 31 hari, dan dapat dikonfigurasi ke nilai antara 2—183 hari. Ketika blok data dingin yang mendasarinya dibaca secara acak (seperti pada akses file biasa), mereka dibuat panas dan ditulis ke tingkat penyimpanan utama. Ketika blok data dingin dibaca secara berurutan (misalnya, dengan pemindaian antivirus), mereka tetap dingin dan tetap berada di tingkat penyimpanan kolam kapasitas. Ini adalah kebijakan default saat membuat volume menggunakan FSx konsol Amazon.
- Hanya Snapshot — Kebijakan ini hanya memindahkan data snapshot ke tingkat penyimpanan kumpulan kapasitas. Tingkat di mana snapshot berjenjang ke kumpulan kapasitas ditentukan oleh periode pendinginan kebijakan, yang secara default diatur ke 2 hari, dan dapat dikonfigurasi ke nilai antara 2—183 hari. Ketika data snapshot dingin dibaca, mereka dibuat panas dan ditulis ke tingkat penyimpanan utama. Ini adalah kebijakan default saat membuat volume menggunakan AWS CLI, Amazon FSx API, atau NetApp ONTAP CLI.

- Semua — Kebijakan ini menandai semua data pengguna dan data snapshot sebagai dingin, dan menyimpannya di tingkat kumpulan kapasitas. Ketika blok data dibaca, mereka tetap dingin dan tidak ditulis ke tingkat penyimpanan utama. Ketika data ditulis ke volume dengan kebijakan All tiering, awalnya masih ditulis ke tingkat penyimpanan SSD, dan berjenjang ke kumpulan kapasitas dengan proses latar belakang. Jika kebijakan Semua diterapkan pada volume yang sudah berisi data, data yang ada berjenjang dari SSD ke kumpulan kapasitas. Perhatikan bahwa metadata file selalu tetap pada tingkat SSD.
- Tidak ada — Kebijakan ini menyimpan semua data volume Anda di tingkat penyimpanan utama, dan mencegahnya dipindahkan ke penyimpanan kumpulan kapasitas. Jika Anda menyetel volume ke kebijakan ini setelah menggunakan kebijakan lain, data yang ada (termasuk snapshot) dalam volume penyimpanan kumpulan kapasitas dipindahkan ke penyimpanan SSD melalui proses latar belakang. Migrasi data ini hanya terjadi ketika pemanfaatan SSD Anda di bawah 90% dan kebijakan pengambilan cloud disetel ke promote atau. on-read Proses latar belakang ini dapat dipercepat dengan sengaja membaca data. Untuk informasi selengkapnya, lihat [Kebijakan pengambilan cloud](#).

Untuk informasi selengkapnya tentang menyetel atau memodifikasi kebijakan tingkatan volume, lihat. [Memperbarui kebijakan tiering](#)

Sebagai praktik terbaik, saat memigrasikan data yang Anda rencanakan untuk disimpan dalam jangka panjang dalam penyimpanan kumpulan kapasitas, sebaiknya gunakan kebijakan tingkatan Otomatis pada volume Anda. Dengan tiering Otomatis, data disimpan di tingkat penyimpanan SSD selama minimal 2 hari (berdasarkan periode pendinginan volume) sebelum dipindahkan ke tingkat kolam kapasitas. ONTAP menjalankan deduplikasi pasca-proses pada data yang disimpan di tingkat penyimpanan SSD secara berkala, secara otomatis menyesuaikan frekuensi berdasarkan laju perubahan data dalam volume — tingkat yang lebih tinggi memicu pekerjaan deduplikasi pasca-proses lebih sering.

Secara default, kompresi pasca-proses dinonaktifkan ONTAP karena dampak kinerja yang dapat ditimbulkannya pada beban kerja yang sedang berlangsung pada sistem file. Anda harus mengevaluasi dampak pada kinerja beban kerja Anda sebelum mengaktifkan kompresi pasca-proses. Untuk mengaktifkan kompresi pasca-proses, asumsikan tingkat hak istimewa diagnostik di ONTAP CLI dan jalankan perintah berikut:

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -is-enabled true
```

ONTAP menjalankan kompresi pasca-proses untuk data yang disimpan pada penyimpanan SSD selama minimal 14 hari. Untuk beban kerja di mana data tidak mungkin diakses setelah periode yang lebih singkat, Anda dapat memodifikasi pengaturan kompresi pasca-proses untuk menjalankan kompresi pasca-proses lebih cepat. Misalnya, untuk menerapkan penghematan kompresi pasca-proses ke data yang belum diakses selama 5 hari, jalankan perintah ONTAP CLI berikut:

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -threshold-days 5 -threshold-days-min 2 -threshold-days-max 14
```

Untuk informasi selengkapnya tentang perintah, lihat [inactive-data-compressionmodifikasi efisiensi volume](#)

Dengan mempertahankan data pada SSD, Anda memaksimalkan kecepatan transfer cadangan volume yang Anda buat, karena kecepatan transfer data lebih tinggi untuk penyimpanan SSD.

Periode pendinginan berjenjang

Periode pendinginan tingkat volume menetapkan jumlah waktu yang diperlukan untuk data di tingkat SSD ditandai sebagai dingin. Periode pendinginan berlaku untuk kebijakan Auto dan Snapshot-only tiering. Anda dapat mengatur periode pendinginan ke nilai dalam kisaran 2-183 hari. Untuk informasi lebih lanjut tentang pengaturan periode pendinginan, lihat [Memperbarui hari pendinginan minimum](#).

Data berjenjang 24-48 jam setelah periode pendinginannya berakhir. Tiering adalah proses latar belakang yang mengkonsumsi sumber daya jaringan, dan memiliki prioritas lebih rendah daripada permintaan yang dihadapi klien. Aktivitas tingkatan dibatasi ketika ada permintaan yang dihadapi klien yang sedang berlangsung.

Kebijakan pengambilan cloud

Kebijakan pengambilan cloud volume menetapkan kondisi yang menentukan kapan data yang dibaca dari tingkat kumpulan kapasitas diizinkan untuk dipromosikan ke tingkat SSD. Jika kebijakan pengambilan cloud disetel ke apa pun selain Default, kebijakan ini akan mengesampingkan perilaku pengambilan kebijakan tiering volume Anda. Volume dapat memiliki salah satu kebijakan pengambilan cloud berikut:

- **Default** — Kebijakan ini mengambil data berjenjang berdasarkan kebijakan tiering yang mendasari volume. Ini adalah kebijakan pengambilan cloud default untuk semua volume.
- **Tidak Pernah** — Kebijakan ini tidak pernah mengambil data berjenjang, terlepas dari apakah pembacaannya berurutan atau acak. Ini mirip dengan menyetel kebijakan tiering volume Anda ke

Semua, kecuali Anda dapat menggunakannya dengan kebijakan lain— Otomatis, Hanya Snapshot —ke data tingkat sesuai dengan periode pendinginan minimum, bukan segera.

- Saat dibaca — Kebijakan ini mengambil data berjenjang untuk semua pembacaan data yang digerakkan oleh klien. Kebijakan ini tidak berpengaruh saat menggunakan kebijakan All tiering.
- Promosikan — Kebijakan ini menandai semua data volume yang ada di kumpulan kapasitas untuk diambil ke tingkat SSD. Data ditandai saat berikutnya pemindai tingkat latar belakang harian berjalan. Kebijakan ini bermanfaat untuk aplikasi yang memiliki beban kerja siklus yang jarang berjalan, tetapi memerlukan kinerja tingkat SSD saat dijalankan. Kebijakan ini tidak berpengaruh saat menggunakan kebijakan All tiering.

Untuk informasi tentang menyetel kebijakan pengambilan cloud volume, lihat [Memperbarui kebijakan pengambilan cloud volume](#).

Ambang batas jenjang

Pemanfaatan kapasitas penyimpanan SSD sistem file menentukan bagaimana ONTAP mengelola perilaku tiering untuk semua volume Anda. Berdasarkan penggunaan kapasitas penyimpanan SSD sistem file, ambang berikut menetapkan perilaku tiering seperti yang dijelaskan. Untuk informasi tentang cara memantau pemanfaatan kapasitas tingkat penyimpanan SSD volume, lihat [Memantau kapasitas penyimpanan volume](#).

Note

Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan kapasitas penyimpanan dari tingkat penyimpanan SSD Anda. Untuk sistem file generasi kedua, rekomendasi ini berlaku untuk pemanfaatan rata-rata total di semua agregat sistem file Anda dan untuk pemanfaatan masing-masing agregat individu. Ini memastikan bahwa tiering berfungsi dengan benar, dan menyediakan overhead untuk data baru. Jika tingkat penyimpanan SSD Anda secara konsisten di atas pemanfaatan kapasitas penyimpanan 80%, Anda dapat meningkatkan kapasitas tingkat penyimpanan SSD Anda. Untuk informasi selengkapnya, lihat [Memperbarui penyimpanan SSD sistem file dan IOPS](#).

FSx untuk ONTAP menggunakan ambang kapasitas penyimpanan berikut untuk mengelola tiering volume:

- $\leq 50\%$ pemanfaatan tingkat penyimpanan SSD — Pada ambang batas ini, tingkat penyimpanan SSD dianggap kurang dimanfaatkan, dan hanya volume yang menggunakan kebijakan All tiering

yang memiliki data berjenjang ke penyimpanan kolam kapasitas. Volume dengan kebijakan Otomatis dan khusus Snapshot tidak membuat data peringkat pada ambang batas ini.

- > Pemanfaatan tingkat penyimpanan SSD 50% — Volume dengan data tingkat kebijakan tiering Otomatis dan Snapshot saja berdasarkan pengaturan hari pendinginan minimum tiering. Pengaturan default adalah 31 hari.
- >= 90% pemanfaatan tingkat penyimpanan SSD — Pada ambang batas ini, Amazon FSx memprioritaskan pelestarian ruang di tingkat penyimpanan SSD. Data dingin dari tingkat kumpulan kapasitas tidak lagi dipindahkan ke tingkat penyimpanan SSD saat dibaca untuk volume menggunakan kebijakan Auto dan Snapshot saja.
- > = 98% Pemanfaatan tingkat penyimpanan SSD — Semua fungsionalitas tiering berhenti ketika tingkat penyimpanan SSD berada pada atau di atas 98% pemanfaatan. Anda dapat terus membaca dari tingkatan penyimpanan, tetapi Anda tidak dapat menulis ke tingkatan.

Snapshot dan kapasitas penyimpanan volume

Snapshot adalah gambar hanya-baca Amazon FSx untuk volume NetApp ONTAP pada suatu titik waktu. Snapshot menawarkan perlindungan terhadap penghapusan atau modifikasi file yang tidak disengaja dalam volume Anda. Dengan snapshot, pengguna Anda dapat dengan mudah melihat dan memulihkan file atau folder individual dari snapshot sebelumnya.

Snapshot disimpan bersama data sistem file Anda, dan mereka menghabiskan kapasitas penyimpanan sistem file. Namun, snapshot mengkonsumsi kapasitas penyimpanan hanya untuk bagian file yang berubah sejak snapshot terakhir. Snapshot tidak disertakan dalam backup volume sistem file Anda.

Snapshot diaktifkan secara default pada volume Anda, menggunakan kebijakan snapshot default. Snapshot disimpan di `.snapshot` direktori di root volume. Anda dapat mengelola kapasitas penyimpanan volume untuk snapshot dengan cara berikut:

- Kebijakan [snapshot — Pilih kebijakan](#) snapshot bawaan atau pilih kebijakan khusus yang Anda buat di ONTAP CLI atau REST API.
- [Hapus snapshot secara manual](#) - Dapatkan kembali kapasitas penyimpanan dengan menghapus snapshot secara manual.
- [Buat kebijakan penghapusan otomatis snapshot — Buat kebijakan](#) yang menghapus lebih banyak snapshot daripada kebijakan snapshot default.

- [Matikan snapshot otomatis](#) — Hemat kapasitas penyimpanan dengan mematikan snapshot otomatis.

Untuk informasi selengkapnya, lihat [Melindungi data Anda dengan snapshot](#).

Kapasitas file volume

Amazon FSx untuk volume NetApp ONTAP memiliki pointer file yang digunakan untuk menyimpan metadata file seperti nama file, waktu akses terakhir, izin, ukuran, dan untuk berfungsi sebagai petunjuk ke blok data. Pointer file ini disebut inode, dan setiap volume memiliki kapasitas terbatas untuk jumlah inode, yang disebut kapasitas file volume. Ketika volume berjalan rendah atau kehabisan file yang tersedia (inode), Anda tidak dapat menulis data tambahan ke volume itu.

Jumlah objek sistem file — file, direktori, salinan Snapshot — volume dapat berisi ditentukan oleh berapa banyak inode yang dimilikinya. Jumlah inode dalam volume meningkat sepadan dengan kapasitas penyimpanan volume (dan jumlah konstituen volume untuk volume). FlexGroup Secara default, FlexVol volume (atau FlexGroup konstituen) dengan kapasitas penyimpanan 648 GiB atau lebih semuanya memiliki jumlah inode yang sama: 21.251.126. Jika Anda membuat volume lebih besar dari 648 GiB dan Anda ingin memiliki lebih dari 21.251.126 inode, Anda harus meningkatkan jumlah maksimum inode (file) secara manual. Untuk informasi selengkapnya tentang melihat jumlah maksimum file untuk volume, lihat [Memantau kapasitas file volume](#).

Jumlah default inode pada volume adalah 1 inode untuk setiap 32 KiB kapasitas penyimpanan volume, hingga ukuran volume 648 GiB. Untuk volume 1 GiB:

$$\text{Volume\_size\_in\_bytes} \times (1 \text{ berkas} \div \text{inode\_size\_in\_bytes}) = \text{maksimum\_number\_of\_files}$$
$$1.073.741.824 \text{ byte} \times (1 \text{ file} \div 32.768 \text{ byte}) = 32.768 \text{ file}$$

Anda dapat meningkatkan jumlah maksimum inode yang dapat dikandung volume, hingga maksimum 1 inode untuk setiap 4 KiB kapasitas penyimpanan. Untuk volume 1 GiB, ini meningkatkan jumlah maksimum inode atau file dari 32.768 menjadi 262.144:

$$1.073.741.824 \text{ byte} \times (1 \text{ file} \div 4096 \text{ byte}) = 262.144 \text{ file}$$

Volume FSx untuk ONTAP dapat memiliki maksimum 2 miliar inode.

Untuk informasi tentang mengubah jumlah maksimum file yang dapat disimpan volume, lihat [Memperbarui jumlah maksimum file pada volume](#).

Mengelola efisiensi penyimpanan

Dengan mengaktifkan efisiensi penyimpanan pada volume ONTAP Anda FSx , Anda dapat mengoptimalkan pemanfaatan penyimpanan, mengurangi biaya penyimpanan, dan meningkatkan kinerja sistem file Anda secara keseluruhan.

Note

Sebaiknya aktifkan efisiensi penyimpanan menggunakan FSx konsol Amazon, API, atau AWS CLI untuk memastikan bahwa pengaturan efisiensi penyimpanan optimal diterapkan pada volume Anda.

ONTAP mengatur file menjadi 4 kibibyte (KiB) blok data. Efisiensi penyimpanan terjadi pada tingkat blok data daripada pada tingkat file individual. Ketika efisiensi penyimpanan diaktifkan, ONTAP menggunakan kombinasi teknik reduksi data untuk menghilangkan data duplikat, memampatkan ukuran data, dan mengatur ulang tata letak data untuk penggunaan disk yang optimal.

Efisiensi penyimpanan diterapkan dalam dua cara. Mereka diterapkan ke data inline (sebelum data ditulis ke disk, dalam memori) untuk memberikan penghematan penyimpanan langsung. Mereka juga diterapkan pada data di latar belakang (setelah data ditulis ke disk) di tingkat penyimpanan SSD melalui pekerjaan efisiensi berkala untuk mengoptimalkan pemanfaatan penyimpanan dari waktu ke waktu. Efisiensi penyimpanan latar belakang tidak berjalan pada data setelah berjenjang ke kumpulan kapasitas. Namun, jika data memiliki penghematan penyimpanan saat berada di SSD, penghematan ini dipertahankan ketika data berjenjang ke kumpulan kapasitas.

Note

ONTAP tidak mendukung mengaktifkan efisiensi penyimpanan pada volume perlindungan data (DP). Namun, penghematan penyimpanan yang dicapai dalam volume sumber read-writable (RW) dipertahankan ketika data direplikasi ke volume DP tujuan.

Kompresi blok data

Grup kompresi adalah pengelompokan logis data yang dikelola dan dikompresi bersama sebagai satu blok. ONTAP secara otomatis mengemas blok data ke dalam kelompok kompresi, yang mengurangi ruang yang dikonsumsi pada disk. Untuk mengoptimalkan kinerja dan pemanfaatan

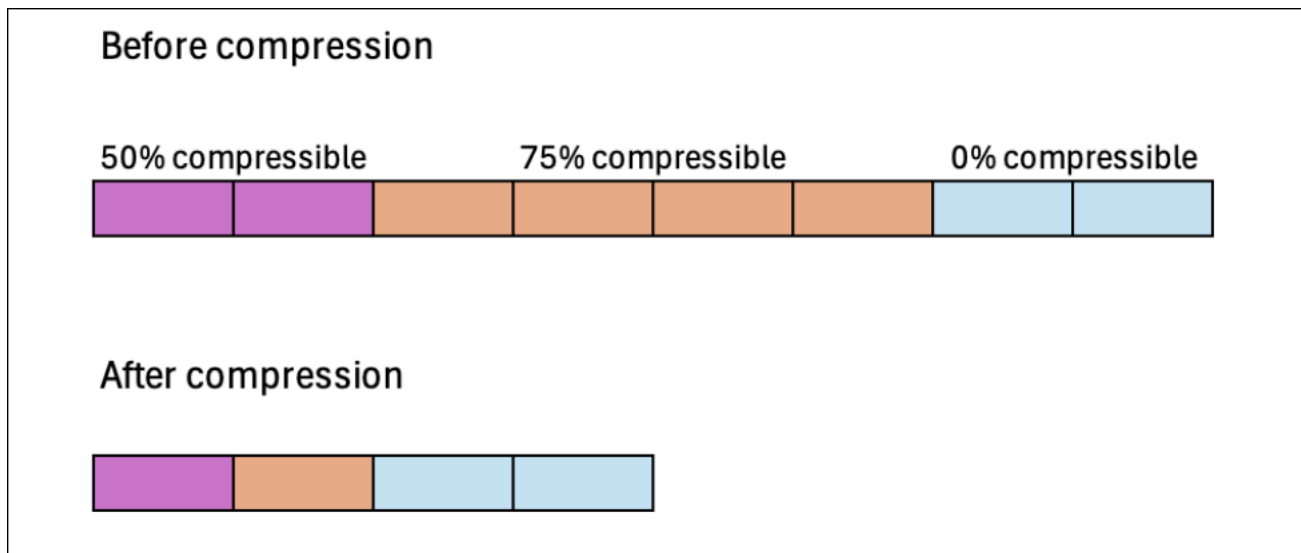
penyimpanan, ONTAP berikan pendekatan yang seimbang untuk mengelola data dengan menyesuaikan tingkat kompresi yang diterapkan pada data berdasarkan pola aksesnya.

Secara default, data dikompresi sebaris menggunakan grup kompresi 8 KB untuk memastikan kinerja optimal saat menulis data ke volume. Secara opsional, Anda dapat menerapkan kompresi yang lebih berat ke data dengan mengaktifkan kompresi data tidak aktif pada volume untuk lebih memampatkan data dalam SSD. Kompresi data tidak aktif menggunakan grup kompresi 32 KB pada data dingin untuk penghematan penyimpanan tambahan. Untuk informasi lebih lanjut, lihat [volume efficiency inactive-data-compression modify](#) perintah diNetApp ONTAP Documentation Center.

Note

Kompresi data tidak aktif mengkonsumsi CPU dan disk IOPS tambahan dan dapat menjadi tugas intensif sumber daya. Kami menyarankan Anda mengevaluasi dampak kinerja menjalankan kompresi data tidak aktif pada beban kerja Anda sebelum mengaktifkan fitur ini.

Gambar berikut menggambarkan penghematan penyimpanan yang dapat dicapai dengan mengompresi blok data.



Deduplikasi blok data

ONTAP mendeteksi dan menghilangkan blok data duplikat untuk mengurangi redundansi dalam data. Blok duplikat diganti dengan referensi ke blok unik bersama.

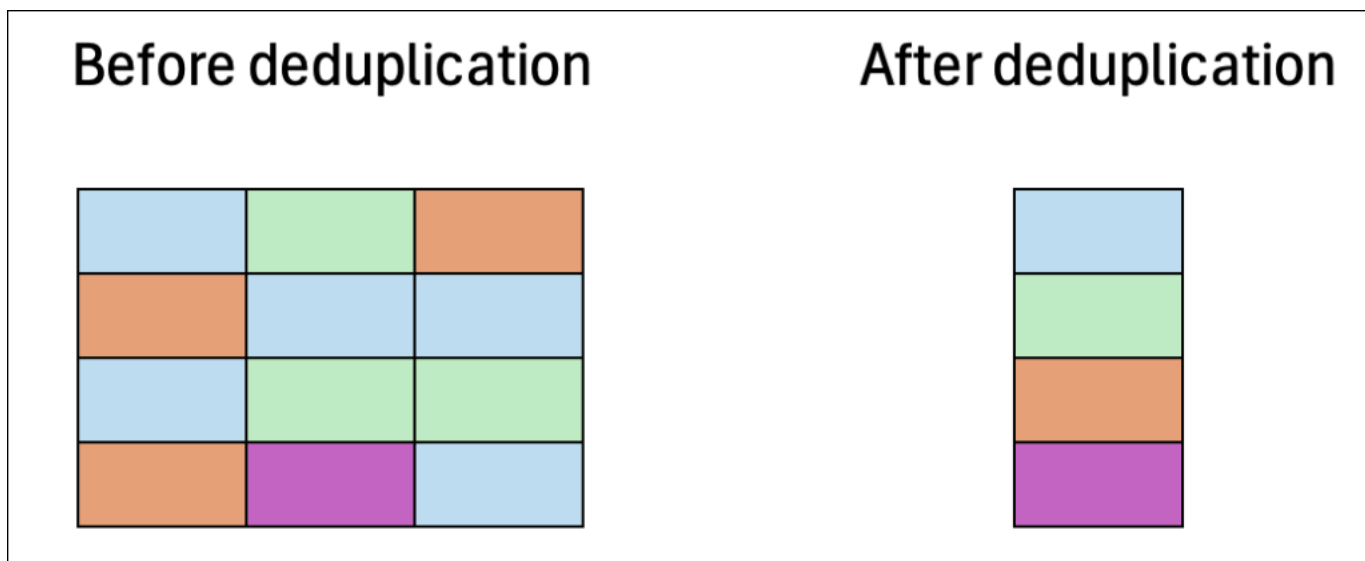
Secara default, data dideduplikasi sebaris untuk mengurangi jejak penyimpanan sebelum data ditulis ke disk. ONTAP juga menjalankan pemindaian deduplikasi latar belakang pada interval tertentu untuk mengidentifikasi dan menghilangkan data duplikat setelah ditulis ke disk. Selama pemindaian terjadwal ini, ONTAP proses log perubahan untuk mengidentifikasi blok data baru atau yang dimodifikasi sejak pemindaian terakhir yang belum di-deduplikasi. Ketika duplikat ditemukan, ONTAP memperbarui metadata untuk menunjuk ke satu salinan blok duplikat dan tandai blok redundan sebagai ruang kosong yang siap untuk direklamasikan.

Note

ONTAP menerapkan deduplikasi ke 4 KB penulisan masuk sekaligus, jadi Anda mungkin melihat penghematan deduplikasi yang lebih rendah saat menjalankan beban kerja dengan penulisan yang berukuran lebih kecil dari 4 KB.

FSx untuk ONTAP tidak mendukung deduplikasi lintas volume.

Gambar berikut menggambarkan penghematan penyimpanan yang dapat dicapai dengan deduplikasi.



Pemadatan blok data

ONTAP mengkonsolidasikan blok data yang terisi sebagian yang masing-masing kurang dari 4 KB menjadi blok 4 KB yang lebih efisien digunakan.

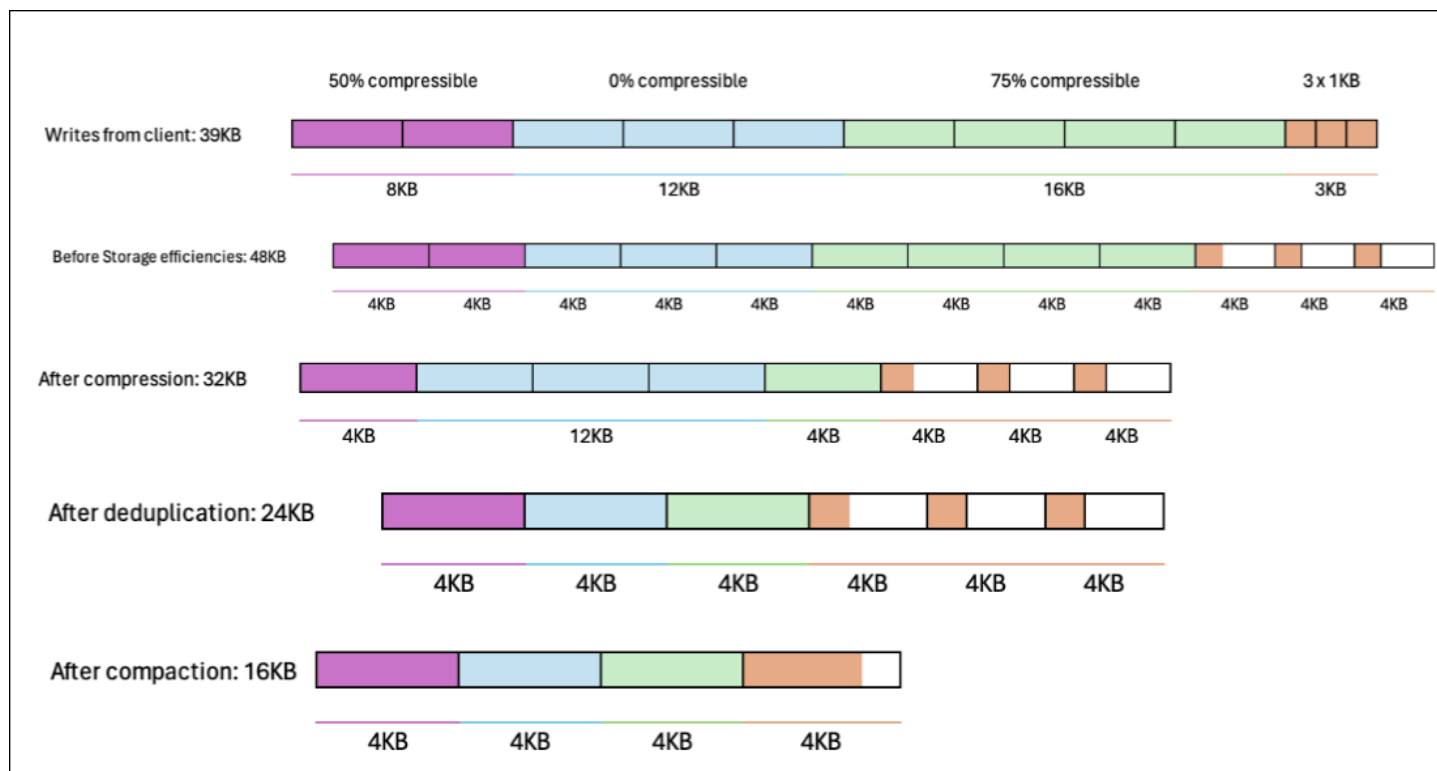
Secara default, data dipadatkan sebaris untuk mengoptimalkan tata letak data seperti yang ditulis ke disk untuk meminimalkan overhead penyimpanan, mengurangi fragmentasi, dan meningkatkan kinerja baca.

Gambar berikut menggambarkan penghematan penyimpanan yang dapat dicapai dengan pemadatan.



Contoh: efisiensi penyimpanan

Gambar berikut menggambarkan bagaimana efisiensi penyimpanan diterapkan pada data.



Mengaktifkan autosizing

Volume autosizing sehingga volume akan secara otomatis tumbuh ke ukuran tertentu ketika mencapai ambang ruang yang digunakan. Anda dapat melakukan ini untuk tipe FlexVol volume (tipe volume default FSx untuk ONTAP) menggunakan perintah ONTAP [volume autosize](#) CLI.

Untuk mengaktifkan autosizing volume (ONTAP CLI)

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Gunakan `volume autosize` perintah seperti yang ditunjukkan, menggantikan nilai-nilai berikut:
 - Ganti *svm_name* dengan nama SVM tempat volume dibuat.
 - Ganti *vol_name* dengan nama volume yang ingin Anda ubah ukurannya.
 - Ganti *grow_threshold* dengan nilai persentase spasi yang digunakan (seperti 90) di mana volume akan secara otomatis meningkat dalam ukuran (hingga *max_size* nilai).
 - Ganti *max_size* dengan ukuran maksimum yang volumenya bisa bertambah. Gunakan formatnya *integer*[KB|MB|GB|TB|PB]; misalnya, 300TB. Ukuran maksimumnya adalah 300 TB. Defaultnya adalah 120% dari ukuran volume.
 - Ganti *min_size* dengan ukuran minimum yang volume akan menyusut. Gunakan format yang sama seperti untuk *max_size*.
 - Ganti *shrink_threshold* dengan persentase ruang yang digunakan di mana volume akan secara otomatis menyusut ukurannya.

```
::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -  
grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-  
percent shrink_threshold -minimum-size min_size
```

3. Untuk menampilkan pengaturan ukuran otomatis saat ini, jalankan perintah berikut. Ganti *svm_name* dan *vol_name* dengan informasi Anda.

```
::> volume autosize -vserver svm_name -volume vol_name
```

Mengaktifkan mode tulis cloud

Gunakan perintah `volume modify` ONTAP CLI untuk mengaktifkan atau menonaktifkan mode tulis cloud untuk volume yang ada. Untuk informasi selengkapnya, lihat [volume modify](#) di Pusat Dokumentasi NetApp ONTAP.

Prasyarat untuk mengatur mode tulis cloud adalah:

- Volume harus berupa volume yang ada. Anda hanya dapat mengaktifkan fitur pada volume yang ada.
- Volume harus berupa volume baca-tulis (RW).
- Volume harus memiliki kebijakan All tiering. Untuk informasi selengkapnya tentang memodifikasi kebijakan tingkatan volume, lihat [Memperbarui kebijakan tiering](#)

Mode tulis cloud sangat membantu untuk kasus-kasus seperti migrasi, misalnya, di mana sejumlah besar data ditransfer ke sistem file menggunakan protokol NFS.

Untuk mengatur mode tulis cloud volume (ONTAP CLI)

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Masukkan mode lanjutan CLI ONTAP menggunakan perintah berikut.

```
FSx::> set -privilege advanced
```

```
Warning: These advanced commands are potentially dangerous; use them only when  
directed to do so by NetApp personnel.
```

```
Do you want to continue? {y|n}: y
```

3. Gunakan perintah berikut untuk mengatur mode tulis cloud volume, menggantikan nilai berikut:

- Ganti `svm_name` dengan nama SVM tempat volume dibuat.
- Ganti `vol_name` dengan nama volume yang Anda atur mode tulis cloud.
- Ganti `vol_cw_mode` dengan salah satu `true` untuk mengaktifkan mode tulis cloud pada volume atau `false` untuk menonaktifkannya.

```
FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-enabled vol_cw_mode
```

Sistem merespons sebagai berikut untuk permintaan yang berhasil.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Memperbarui kapasitas penyimpanan

Anda dapat mengelola kapasitas penyimpanan volume dengan menambah atau mengurangi ukuran volume secara manual menggunakan Konsol Manajemen AWS, AWS CLI dan API, dan CLI ONTAP. Anda juga dapat mengaktifkan autosizing volume sehingga ukuran volume secara otomatis tumbuh atau menyusut ketika mencapai ambang batas kapasitas penyimpanan bekas tertentu. Anda menggunakan CLI ONTAP untuk mengelola autosizing volume.

Untuk mengubah kapasitas penyimpanan volume (konsol)

- Anda dapat menambah atau mengurangi kapasitas penyimpanan volume menggunakan FSx konsol Amazon, AWS CLI, dan API. Untuk informasi selengkapnya, lihat [Memperbarui volume](#).

Anda juga dapat menggunakan ONTAP CLI untuk memodifikasi kapasitas penyimpanan volume menggunakan perintah. [volume modify](#)

Untuk memodifikasi ukuran volume (ONTAP CLI)

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti `management_endpoint_ip` dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

- Gunakan perintah `volume modify` ONTAP CLI untuk memodifikasi kapasitas penyimpanan volume. Jalankan perintah berikut, menggunakan data Anda sebagai pengganti nilai-nilai berikut:
 - Ganti `svm_name` dengan nama mesin virtual penyimpanan (SVM) tempat volume dibuat.
 - Ganti `vol_name` dengan nama volume yang ingin Anda ubah ukurannya.
 - Ganti `vol_size` dengan ukuran volume baru dalam format `integer`[KB|MB|GB|TB|PB]; misalnya, `100GB` untuk meningkatkan ukuran volume menjadi 100 gigabyte.

```
::> volume modify -vserver svm_name -volume vol_name -size vol_size
```

Memperbarui kebijakan tiering

Anda dapat mengubah kebijakan tingkatan volume menggunakan Konsol Manajemen AWS, AWS CLI dan API, dan CLI ONTAP.

Untuk mengubah kebijakan tingkatan data volume (konsol)

Gunakan prosedur berikut untuk memodifikasi kebijakan tingkat data volume menggunakan. Konsol Manajemen AWS

- Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
- Pilih Volume di panel navigasi kiri, lalu pilih volume ONTAP yang ingin Anda ubah kebijakan tingkat data.
- Pilih Perbarui volume dari menu tarik-turun Tindakan. Jendela Perbarui volume muncul.
- Untuk kebijakan tingkatan kumpulan Kapasitas, pilih kebijakan baru untuk volume tersebut. Untuk informasi selengkapnya, lihat [Kebijakan tingkatan volume](#).
- Pilih Perbarui untuk menerapkan kebijakan baru ke volume.

Untuk menetapkan kebijakan tingkatan volume (CLI)

- Ubah kebijakan tiering volume menggunakan perintah CLI [update-volume](#) (`UpdateVolume` adalah tindakan Amazon API yang setara). FSx Contoh perintah CLI berikut menetapkan kebijakan tingkat data volume ke. `SNAPSHOT_ONLY`


```
aws fsx update-volume \
  --volume-id fsxvol-abcde0123456789f
  --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

Untuk permintaan yang berhasil, sistem merespons dengan deskripsi volume.

```
{
  "Volume": {
    "CreationTime": "2021-10-05T14:27:44.332000-04:00",
    "FileSystemId": "fs-abcde0123456789f",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "OntapConfiguration": {
      "FlexCacheEndpointType": "NONE",
      "JunctionPath": "/vol1",
      "SecurityStyle": "UNIX",
      "SizeInMegabytes": 1048576,
      "StorageEfficiencyEnabled": true,
      "StorageVirtualMachineId": "svm-abc0123de456789f",
      "StorageVirtualMachineRoot": false,
      "TieringPolicy": {
        "CoolingPeriod": 2,
        "Name": "SNAPSHOT_ONLY"
      },
      "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
      "OntapVolumeType": "RW"
    },
    "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcde0123456789f/fsvol-abc012def3456789a",
    "VolumeId": "fsvol-abc012def3456789a",
    "VolumeType": "ONTAP"
  }
}
```

Untuk mengubah kebijakan tingkatan volume (ONTAP CLI)

Anda menggunakan perintah `volume modify` ONTAP CLI untuk menyetel kebijakan tiering volume. Untuk informasi selengkapnya, lihat [volume modify](#) di Pusat Dokumentasi NetApp ONTAP.

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Masukkan mode lanjutan CLI ONTAP menggunakan perintah berikut.

```
FSx::> set adv
```

```
Warning: These advanced commands are potentially dangerous; use them only when  
directed to do so by NetApp personnel.
```

```
Do you want to continue? {y|n}: y
```

3. Gunakan perintah berikut untuk mengubah kebijakan tingkat data volume, menggantikan nilai berikut:
 - Ganti *svm_name* dengan nama SVM tempat volume dibuat.
 - Ganti *vol_name* dengan nama volume yang Anda setel kebijakan data-tiering.
 - Ganti *tiering_policy* dengan kebijakan yang diinginkan. Nilai yang valid adalah snapshot-only, auto, all, atau none. Untuk informasi selengkapnya, lihat [Kebijakan tingkatan volume](#).

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-  
policy tiering_policy
```

Memperbarui hari pendinginan minimum

Hari pendinginan minimum untuk volume mengatur ambang batas yang digunakan untuk menentukan data mana yang hangat dan data mana yang dingin. Anda dapat mengatur hari pendinginan minimum volume menggunakan AWS CLI dan API, dan CLI ONTAP.

Untuk mengatur hari pendinginan minimum volume (CLI)

- Ubah konfigurasi volume dengan menggunakan perintah CLI [update-volume](#) ([UpdateVolume](#) adalah tindakan API Amazon FSx yang setara). Contoh perintah CLI berikut menetapkan volume CoolingPeriod untuk 104 hari.

```
aws fsx update-volume \
  --volume-id fsxvol-abcde0123456789f
  --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration
  TieringPolicy={CoolingPeriod=104}
```

Sistem merespons dengan deskripsi volume untuk permintaan yang berhasil.

```
{
  "Volume": {
    "CreationTime": "2021-10-05T14:27:44.332000-04:00",
    "FileSystemId": "fs-abcde0123456789f",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "OntapConfiguration": {
      "FlexCacheEndpointType": "NONE",
      "JunctionPath": "/vol1",
      "SecurityStyle": "UNIX",
      "SizeInMegabytes": 1048576,
      "StorageEfficiencyEnabled": true,
      "StorageVirtualMachineId": "svm-abc0123de456789f",
      "StorageVirtualMachineRoot": false,
      "TieringPolicy": {
        "CoolingPeriod": 104,
        "Name": "SNAPSHOT_ONLY"
      },
      "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
      "OntapVolumeType": "RW"
    },
    "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
    "VolumeId": "fsvol-abc012def3456789a",
    "VolumeType": "ONTAP"
  }
}
```

Untuk mengatur hari pendinginan minimum volume (ONTAP CLI)

Gunakan perintah `volume modify` ONTAP CLI untuk mengatur jumlah minimum hari pendinginan untuk volume yang ada. Untuk informasi selengkapnya, lihat [volume modify](#) di Pusat Dokumentasi NetApp ONTAP.

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Masukkan mode lanjutan CLI ONTAP menggunakan perintah berikut.

```
FSx::> set adv
```

```
Warning: These advanced commands are potentially dangerous; use them only when  
directed to do so by NetApp personnel.  
Do you want to continue? {y|n}: y
```

3. Gunakan perintah berikut untuk mengubah hari pendinginan minimum tingkat volume Anda, menggantikan nilai-nilai berikut:
 - Ganti *svm_name* dengan nama SVM tempat volume dibuat.
 - Ganti *vol_name* dengan nama volume yang Anda atur hari pendinginan.
 - Ganti *cooling_days* dengan yang diinginkan, bilangan bulat antara 2-183.

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-  
days cooling_days
```

Sistem merespons sebagai berikut untuk permintaan yang berhasil.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Memperbarui kebijakan pengambilan cloud volume

Gunakan perintah `volume modify` ONTAP CLI untuk menyetel kebijakan pengambilan cloud untuk volume yang ada. Untuk informasi selengkapnya, lihat [volume modify](#) di Pusat Dokumentasi NetApp ONTAP.

Untuk menyetel kebijakan pengambilan cloud volume (ONTAP CLI)

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Masukkan mode lanjutan CLI ONTAP menggunakan perintah berikut.

```
FSx::> set adv
```

```
Warning: These advanced commands are potentially dangerous; use them only when  
directed to do so by NetApp personnel.  
Do you want to continue? {y|n}: y
```

3. Gunakan perintah berikut untuk menyetel kebijakan pengambilan cloud volume, menggantikan nilai berikut:
 - Ganti *svm_name* dengan nama SVM tempat volume dibuat.
 - Ganti *vol_name* dengan nama volume yang Anda setel kebijakan pengambilan cloud.
 - Ganti *retrieval_policy* dengan nilai yang diinginkan, baik `default`, `on-read`, `never`, atau `promote`.

```
FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-  
policy retrieval_policy
```

Sistem merespons sebagai berikut untuk permintaan yang berhasil.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Memperbarui jumlah maksimum file pada volume

FSx untuk volume ONTAP dapat kehabisan kapasitas file ketika jumlah inode yang tersedia, atau pointer file, habis.

Untuk meningkatkan jumlah maksimum file pada volume (ONTAPCLI)

Anda menggunakan perintah `volume modify` ONTAP CLI untuk meningkatkan jumlah maksimum file pada volume. Untuk informasi selengkapnya, lihat [volume modify](#) di Pusat NetApp ONTAP Dokumentasi.

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti `management_endpoint_ip` dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Lakukan salah satu langkah berikut sesuai dengan kasus penggunaan Anda. Ganti `svm_name` dan `vol_name` dengan nilai-nilai Anda.
 - Untuk mengonfigurasi volume agar selalu memiliki jumlah maksimum file (inode) yang tersedia, lakukan hal berikut:

1. Masuk ke mode lanjutan di CLI ONTAP dengan menggunakan perintah berikut.

```
::> set adv
```

2. Setelah menjalankan perintah ini, Anda akan melihat output ini. Masuk y untuk melanjutkan.

```
Warning: These advanced commands are potentially dangerous; use them only
when
directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

3. Masukkan perintah berikut untuk selalu menggunakan jumlah maksimum file pada volume:

```
::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
```

- Untuk secara manual menentukan jumlah total file yang diizinkan pada volume $\text{max\_number\_files} = (\text{current\_size\_of\_volume}) \times (1 \text{ file} \div 4 \text{ KiB})$, dengan, hingga nilai maksimum yang mungkin 2 miliar, gunakan perintah berikut:

```
::> volume modify -vserver svm_name -volume vol_name -files max_number_files
```

Memantau kapasitas penyimpanan volume

Anda dapat melihat penyimpanan volume yang tersedia dan distribusi penyimpanannya di Konsol Manajemen AWS, AWS CLI, dan CLI NetApp ONTAP.

Untuk memantau kapasitas penyimpanan volume (konsol)

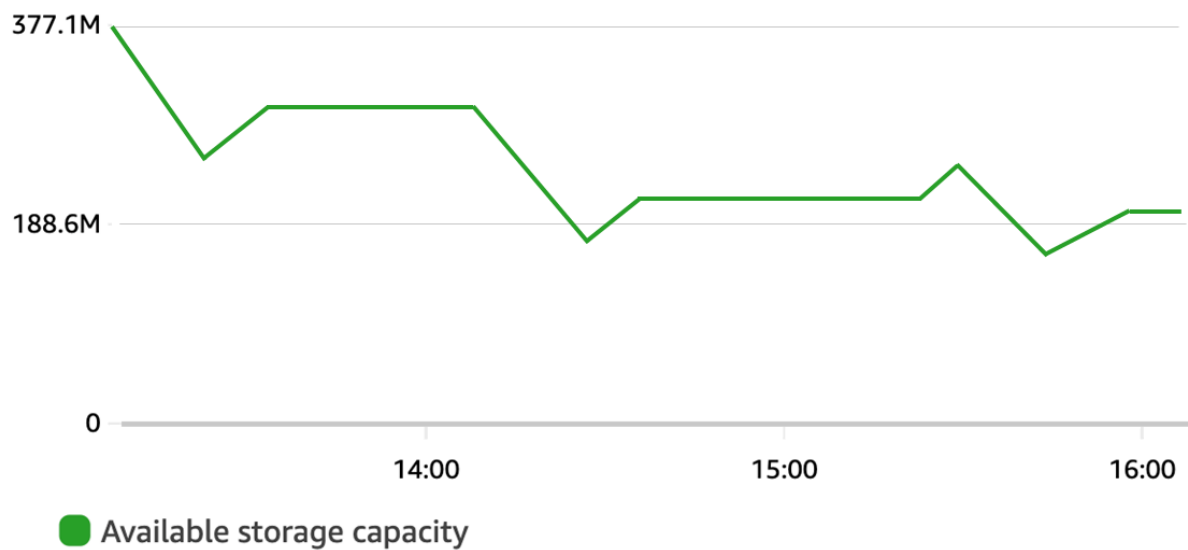
Grafik penyimpanan yang tersedia menampilkan jumlah kapasitas penyimpanan gratis pada volume dari waktu ke waktu. Grafik distribusi Storage menunjukkan bagaimana kapasitas penyimpanan volume saat ini didistribusikan pada 4 kategori:

- Data pengguna
- Data snapshot
- Kapasitas volume yang tersedia
- Data lainnya

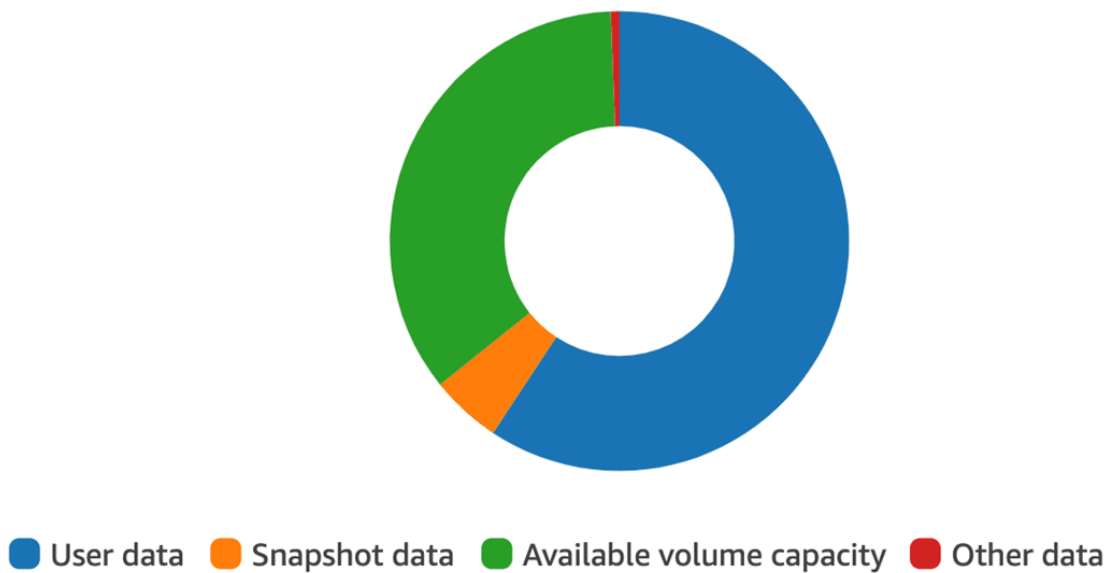
1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Pilih Volume di kolom navigasi kiri, lalu pilih volume ONTAP yang ingin Anda lihat informasi kapasitas penyimpanan. Halaman detail volume muncul.
3. Di panel kedua, pilih tab Monitoring. Grafik distribusi Penyimpanan dan Penyimpanan yang Tersedia ditampilkan, bersama dengan beberapa grafik lainnya.

Available storage capacity

No unit



Storage distribution



Untuk memantau kapasitas penyimpanan volume (ONTAPCLI)

Anda dapat memantau bagaimana kapasitas penyimpanan volume Anda dikonsumsi dengan menggunakan perintah `volume show-space` ONTAP CLI. Untuk informasi selengkapnya, lihat [volume show-space](#) di Pusat NetApp ONTAP Dokumentasi.

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Lihat penggunaan kapasitas penyimpanan volume dengan mengeluarkan perintah berikut, mengganti nilai berikut:
 - Ganti *svm_name* dengan nama SVM tempat volume dibuat.
 - Ganti *vol_name* dengan nama volume yang Anda setel kebijakan data-tiering.

```
::> volume show-space -vserver svm_name -volume vol_name
```

Jika perintah berhasil, Anda akan melihat output yang mirip dengan berikut ini:

```
Vserver : svm_name
Volume  : vol_name
```

Feature	Used	Used%
-----	-----	-----
User Data	140KB	0%
Filesystem Metadata	164.4MB	1%
Inodes	10.28MB	0%
Snapshot Reserve	563.2MB	5%
Deduplication	12KB	0%
Snapshot Spill	9.31GB	85%
Performance Metadata	668KB	0%
 Total Used	 10.03GB	 91%
Total Physical Used	10.03GB	91%

Output dari perintah ini menunjukkan jumlah ruang fisik yang ditempati berbagai jenis data pada volume ini. Ini juga menunjukkan persentase kapasitas total volume yang dikonsumsi setiap jenis data. Dalam contoh ini, Snapshot Spill dan Snapshot Reserve mengkonsumsi gabungan 90 persen dari kapasitas volume.

Snapshot Reservemenunjukkan jumlah ruang disk yang disediakan untuk menyimpan salinan Snapshot. Jika penyimpanan salinan Snapshot melebihi ruang cadangan, itu tumpah ke sistem file dan jumlah ini ditampilkan di bawah. Snapshot Spill

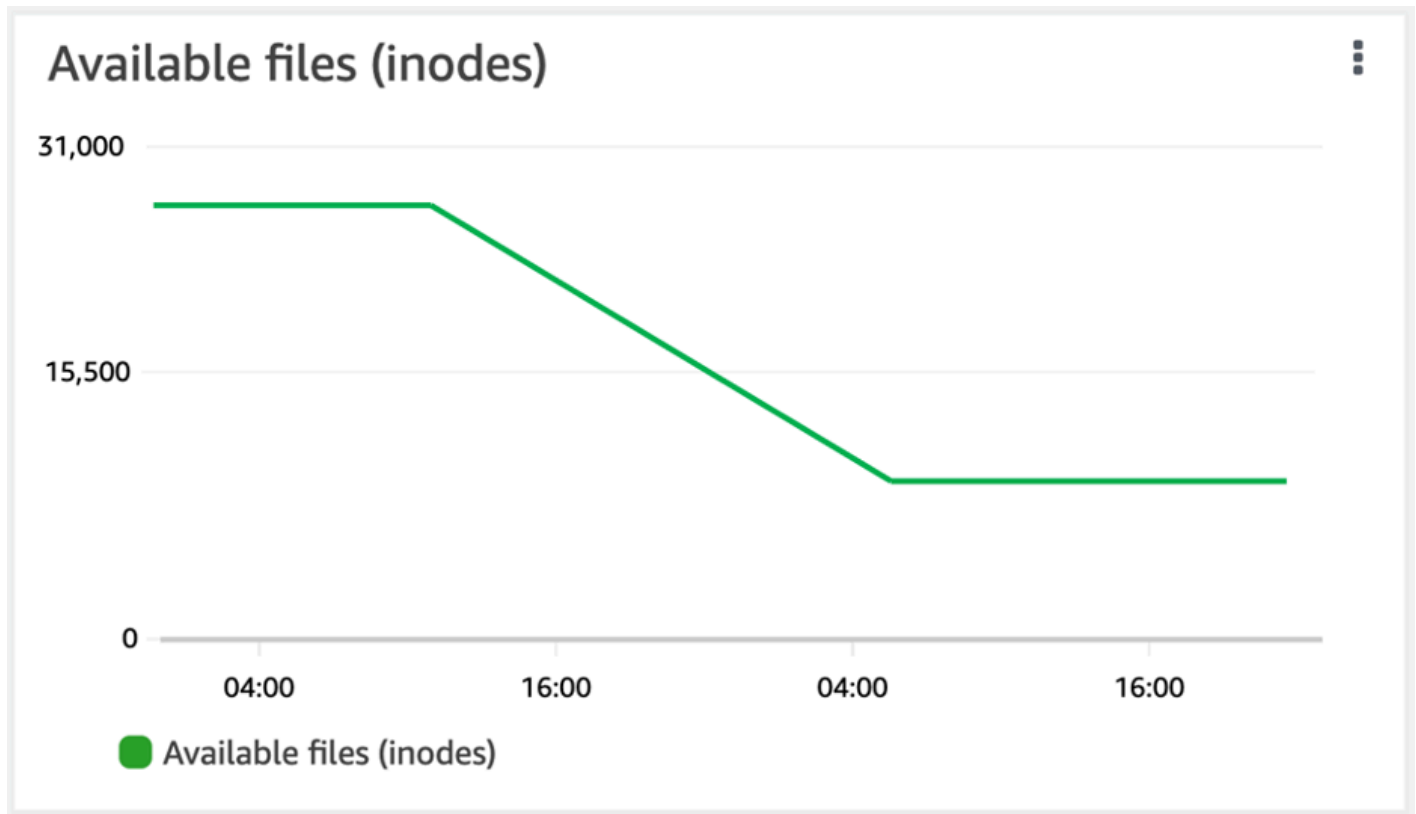
Untuk menambah jumlah ruang yang tersedia, Anda dapat [meningkatkan ukuran](#) volume, atau Anda dapat [menghapus snapshot](#) yang tidak Anda gunakan, seperti yang ditunjukkan dalam prosedur berikut.

Untuk tipe FlexVol volume (tipe volume default FSx untuk volume ONTAP), Anda juga dapat mengaktifkan [autosizing volume](#). Ketika Anda mengaktifkan autosizing, ukuran volume secara otomatis meningkat ketika mencapai ambang tertentu. Anda juga dapat menonaktifkan snapshot otomatis. Kedua fitur ini dijelaskan di bagian berikut.

Memantau kapasitas file volume

Anda dapat menggunakan salah satu metode berikut untuk melihat jumlah maksimum file yang diizinkan dan jumlah file yang sudah digunakan pada volume.

- Metrik CloudWatch volume FilesCapacity danFilesUsed.
- Di FSx konsol Amazon, navigasikan ke bagan File yang tersedia (inode) di tab Pemantauan volume Anda. Gambar berikut menunjukkan file yang tersedia (inode) pada volume menurun dari waktu ke waktu.



Mengelola FSx untuk sistem file ONTAP

Sistem file adalah FSx sumber daya Amazon utama, analog dengan kluster ONTAP lokal. Anda menentukan kapasitas penyimpanan solid state drive (SSD) dan kapasitas throughput untuk sistem file Anda, dan memilih virtual private cloud (VPC) untuk membuat sistem file. Setiap sistem file memiliki endpoint manajemen yang dapat Anda gunakan untuk mengelola sumber daya dan data dengan ONTAP CLI atau REST API.

Sumber daya sistem file

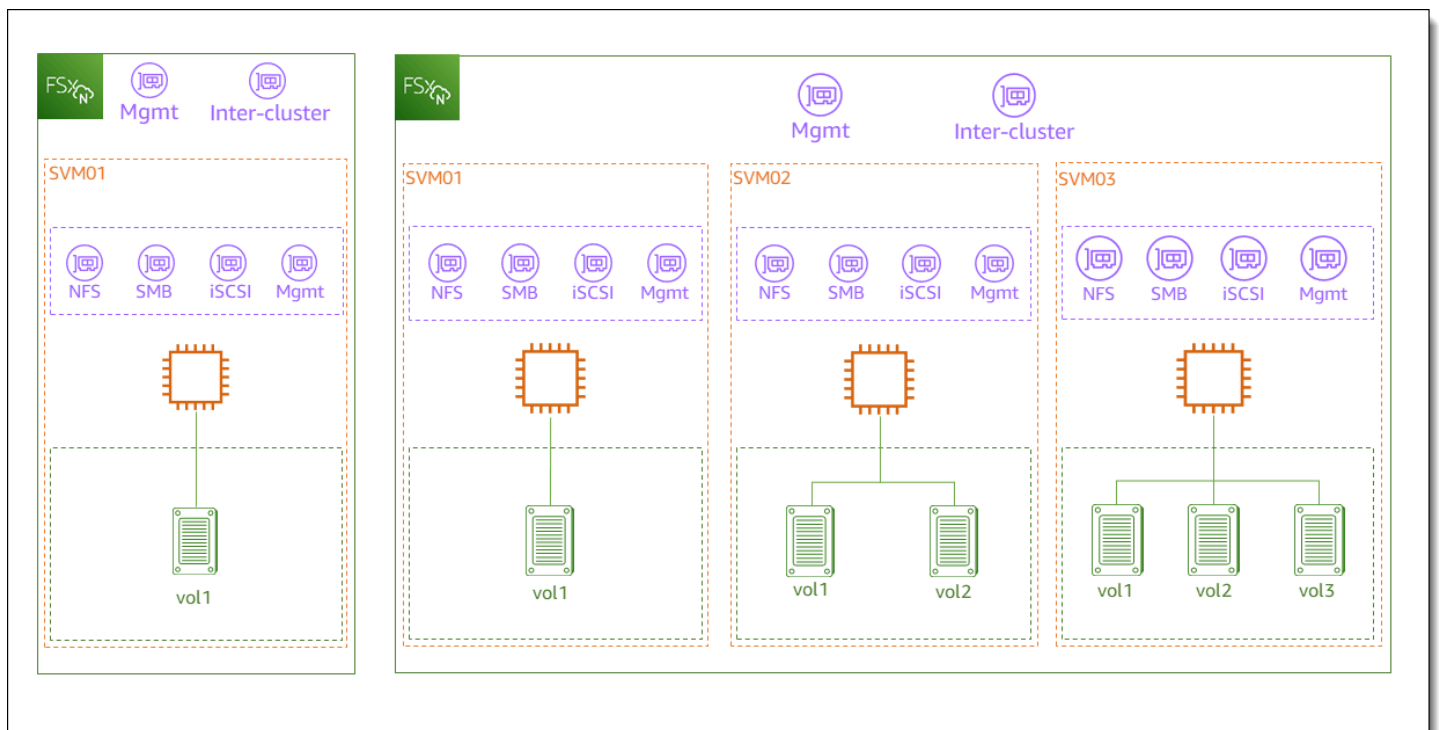
Sistem file Amazon FSx untuk NetApp ONTAP terdiri dari sumber daya utama berikut:

- Perangkat keras fisik dari sistem file itu sendiri, yang mencakup server file dan media penyimpanan.
- Satu atau lebih pasangan server file (HA) yang sangat tersedia, yang menghosting mesin virtual penyimpanan Anda (SVMs). Sistem file generasi pertama dan sistem file generasi kedua multi-AZ memiliki satu pasangan HA, dan sistem file single-AZ generasi kedua memiliki hingga 12 pasang

HA. Setiap pasangan HA memiliki kolom penyimpanan yang disebut agregat. Kumpulan agregat di semua pasangan HA membentuk tingkat penyimpanan SSD Anda.

- Satu atau lebih SVMs yang meng-host volume sistem file dan memiliki kredensialnya sendiri dan manajemen akses.
- Satu atau lebih volume yang secara virtual mengatur data Anda dan dipasang oleh klien Anda.

Gambar berikut mengilustrasikan arsitektur generasi pertama FSx untuk sistem file ONTAP dengan satu pasangan HA, dan hubungan antara sumber daya utamanya. Sistem file FSx untuk ONTAP di sebelah kiri adalah sistem file paling sederhana, dengan satu SVM dan satu volume. Sistem file di sebelah kanan memiliki banyak SVMs, dengan beberapa SVMs memiliki beberapa volume. Sistem file dan SVMs masing-masing memiliki beberapa titik akhir manajemen, dan SVMs juga memiliki titik akhir akses data.



Saat membuat sistem file FSx untuk ONTAP, Anda menentukan properti berikut:

- Jenis penyebaran — Jenis penyebaran sistem file Anda (Multi-AZ atau Single-AZ). Sistem file single-AZ mereplikasi data Anda dan menawarkan failover otomatis dalam satu Availability Zone. Sistem file Single-AZ generasi pertama mendukung satu pasangan HA. Sistem file Single-AZ generasi kedua mendukung hingga 12 pasang HA. Sistem file multi-AZ memberikan ketahanan tambahan dengan juga mereplikasi data Anda dan mendukung failover di beberapa Availability

Zone dalam hal yang sama. Wilayah AWS Sistem file Multi-AZ generasi pertama dan generasi kedua keduanya mendukung satu pasangan HA.

 Note

Anda tidak dapat mengubah jenis penerapan sistem file setelah pembuatan. Jika Anda ingin mengubah jenis penerapan (misalnya, untuk berpindah dari Single-AZ 1 ke Single-AZ 2), Anda dapat mencadangkan data Anda dan mengembalikannya pada sistem file baru. Anda juga dapat memigrasikan data Anda dengan NetApp SnapMirror, dengan AWS DataSync, atau dengan alat penyalinan data pihak ketiga. Untuk informasi selengkapnya, lihat [Migrasi ke FSx untuk ONTAP menggunakan NetApp SnapMirror](#) dan [Migrasi ke FSx untuk ONTAP menggunakan AWS DataSync](#).

- Kapasitas penyimpanan — Ini adalah jumlah penyimpanan SSD, hingga 192 tebibytes (TiB) untuk sistem file generasi pertama, 512 TiB untuk sistem file multi-AZ generasi kedua, dan 1 pebibyte (PiB) untuk sistem file single-AZ generasi kedua.
- SSD IOPS — Secara default, setiap gigabyte penyimpanan SSD mencakup tiga IOPS SSD (hingga maksimum yang didukung oleh konfigurasi sistem file Anda). Anda dapat secara opsional menyediakan IOPS SSD tambahan sesuai kebutuhan.
- Kapasitas throughput — Kecepatan berkelanjutan di mana server file dapat melayani data.
- Networking — VPC dan subnet untuk endpoint manajemen dan akses data yang dibuat oleh sistem file Anda. Untuk sistem file multi-AZ, Anda juga menentukan rentang alamat IP dan tabel rute.
- Enkripsi — Kunci AWS Key Management Service (AWS KMS) yang digunakan untuk mengenkripsi data sistem file saat istirahat.
- Akses administratif — Anda dapat menentukan kata sandi untuk `fsxadmin` pengguna. Anda dapat menggunakan pengguna ini untuk mengelola sistem file dengan menggunakan NetApp ONTAP CLI dan REST API.

Anda dapat mengelola FSx sistem file ONTAP dengan menggunakan NetApp ONTAP CLI atau REST API. Anda juga dapat mengatur SnapMirror atau SnapVault hubungan antara sistem FSx file Amazon dan penyebaran ONTAP lainnya (termasuk sistem FSx file Amazon lainnya). Masing-masing FSx untuk sistem file ONTAP memiliki titik akhir sistem file berikut yang menyediakan akses ke NetApp aplikasi:

- Manajemen — Gunakan endpoint ini untuk mengakses NetApp ONTAP CLI melalui Secure Shell (SSH), atau untuk menggunakan NetApp ONTAP REST API dengan sistem file Anda.

- Intercluster — Gunakan titik akhir ini saat mengatur replikasi menggunakan NetApp SnapMirror atau menggunakan caching. NetApp FlexCache

Untuk informasi selengkapnya, lihat [Mengelola FSx sumber daya ONTAP menggunakan aplikasi NetApp](#) dan [Mereplikasi data Anda menggunakan NetApp SnapMirror](#).

Membuat sistem file

Bagian ini menjelaskan cara membuat sistem file ONTAP FSx untuk menggunakan FSx konsol Amazon, AWS CLI, atau Amazon FSx API. Anda dapat membuat sistem file di cloud pribadi virtual (VPC) yang Anda miliki, atau di VPC yang Akun AWS telah dibagikan orang lain dengan Anda. Ada pertimbangan saat membuat sistem file multi-AZ di VPC di mana Anda adalah peserta. Pertimbangan ini dijelaskan dalam topik ini.

Secara default, saat Anda membuat sistem file baru dari FSx konsol Amazon, Amazon FSx secara otomatis membuat sistem file dengan mesin virtual penyimpanan tunggal (SVM) dan satu volume, memungkinkan akses cepat ke data dari instance Linux melalui protokol Network File System (NFS). Saat membuat sistem file, Anda dapat secara opsional menggabungkan SVM ke Active Directory untuk mengaktifkan akses dari klien Windows dan macOS melalui protokol Server Message Block (SMB). Setelah sistem file Anda dibuat, Anda dapat membuat tambahan SVMs dan volume sesuai kebutuhan.

Untuk membuat sistem file (konsol)

Prosedur ini menggunakan opsi pembuatan pembuatan Standar FSx untuk membuat sistem file ONTAP dengan konfigurasi yang Anda sesuaikan untuk kebutuhan Anda. Untuk informasi tentang menggunakan opsi Pembuatan cepat untuk membuat sistem file dengan cepat dengan set parameter konfigurasi default, lihat [Buat Amazon FSx untuk sistem file NetApp ONTAP](#).

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di dasbor, pilih Buat sistem file.
3. Pada halaman Pilih jenis sistem file, untuk opsi sistem File, pilih Amazon FSx untuk NetApp ONTAP, lalu pilih Berikutnya.
4. Di bagian Metode pembuatan, pilih Standar buat.
5. Di bagian Detail sistem berkas, berikan informasi berikut:
 - Untuk nama sistem File - opsional, masukkan 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 putih, dan angka, ditambah karakter khusus ini: + - =. _:/

- Untuk jenis Deployment pilih Multi-AZ 2, Single-AZ 2, Multi-AZ 1, atau Single-AZ 1.
 - Sistem file multi-AZ mereplikasi data Anda dan mendukung failover di beberapa Availability Zone secara bersamaan. Wilayah AWS Multi-AZ 1 adalah generasi pertama FSx untuk sistem file ONTAP. Multi-AZ 2 adalah sistem file generasi kedua. Keduanya mendukung satu pasangan ketersediaan tinggi (HA).
 - Sistem file single-AZ mereplikasi data Anda dan menawarkan failover otomatis dalam satu Availability Zone. Single-AZ 1 adalah generasi pertama FSx untuk sistem file ONTAP yang mendukung satu pasangan HA. Single-AZ 2 adalah sistem file generasi kedua yang mendukung hingga 12 pasang HA. Untuk informasi selengkapnya, lihat [Mengelola pasangan ketersediaan tinggi \(HA\)](#).

Untuk informasi selengkapnya tentang jenis penerapan, lihat [Opsi ketersediaan, daya tahan, dan penerapan](#).

 Note

Anda tidak dapat mengubah jenis penerapan sistem file setelah pembuatan. Jika Anda ingin mengubah jenis penerapan (misalnya, untuk berpindah dari Single-AZ 1 ke Single-AZ 2), Anda dapat mencadangkan data Anda dan mengembalikannya pada sistem file baru. Anda juga dapat memigrasikan data Anda dengan NetApp SnapMirror, dengan AWS DataSync, atau dengan alat penyalinan data pihak ketiga. Untuk informasi selengkapnya, lihat [Migrasi ke FSx untuk ONTAP menggunakan NetApp SnapMirror](#) dan [Migrasi ke FSx untuk ONTAP menggunakan AWS DataSync](#).

- Untuk kapasitas penyimpanan SSD, masukkan kapasitas penyimpanan sistem file Anda, dalam gibibytes (GiB). Masukkan bilangan bulat dalam kisaran 1.048-1.048.576 GiB (hingga 1 pebibyte [PiB]).

Anda dapat meningkatkan jumlah kapasitas penyimpanan sesuai kebutuhan setiap saat setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat [Mengelola kapasitas penyimpanan](#).

- Untuk Provisioned SSD IOPS, Anda memiliki dua opsi untuk menyediakan jumlah IOPS untuk sistem file Anda:

- Pilih Otomatis (default) jika Anda FSx ingin Amazon secara otomatis menyediakan 3 IOPS per GiB penyimpanan SSD.
- Pilih User-provisioned jika Anda ingin menentukan jumlah IOPS. Anda dapat menyediakan maksimum 200.000 IOPS SSD per sistem file.

 Note

Anda dapat meningkatkan IOPS SSD yang disediakan setelah Anda membuat sistem file. Perlu diingat bahwa tingkat maksimum SSD IOPS yang dapat dicapai sistem file Anda juga ditentukan oleh kapasitas throughput sistem file Anda bahkan ketika menyediakan IOPS SSD tambahan. Untuk informasi selengkapnya, lihat [Dampak kapasitas throughput terhadap performa](#) dan [Mengelola kapasitas penyimpanan](#).

- Untuk kapasitas Throughput, Anda memiliki dua opsi untuk menentukan kapasitas throughput Anda dalam megabyte per detik (): MBps
- Pilih Kapasitas throughput yang disarankan jika Anda FSx ingin Amazon secara otomatis memilih kapasitas throughput berdasarkan jumlah kapasitas penyimpanan yang Anda pilih.
- Pilih Tentukan kapasitas throughput jika Anda ingin menentukan jumlah kapasitas throughput. Jika Anda memilih opsi ini, dropdown kapasitas Throughput akan muncul dan diisi berdasarkan jenis penerapan yang Anda pilih. Anda juga dapat memilih jumlah pasangan HA (hingga 12). Untuk informasi selengkapnya, lihat [Mengelola pasangan ketersediaan tinggi \(HA\)](#).

Kapasitas throughput adalah kecepatan berkelanjutan di mana server file yang menyimpan sistem file Anda dapat melayani data. Untuk informasi selengkapnya, lihat [Amazon FSx untuk kinerja NetApp ONTAP](#).

6. Di bagian Jaringan, berikan informasi berikut:

- Untuk Virtual Private Cloud (VPC), pilih VPC yang ingin Anda kaitkan dengan sistem file Anda.
- Untuk Grup Keamanan VPC, Anda dapat memilih grup keamanan untuk dikaitkan dengan antarmuka jaringan sistem file Anda. Jika Anda tidak menentukannya, Amazon FSx akan mengaitkan grup keamanan default VPC dengan sistem file Anda.
- (Hanya multi-AZ) Untuk subnet Pilihan, pilih nilai apa pun dari daftar subnet yang tersedia. Juga pilih subnet Siaga untuk server file siaga.
- (Hanya Single-AZ) Untuk Subnet, pilih nilai apa pun dari daftar subnet yang tersedia.

- (Hanya multi-AZ) Untuk tabel rute VPC, tentukan tabel rute VPC untuk membuat titik akhir sistem file Anda. Pilih semua tabel rute VPC yang terkait dengan subnet tempat klien Anda berada. Secara default, Amazon FSx memilih tabel rute default VPC Anda. Untuk informasi selengkapnya, lihat [Mengakses data dari luar VPC penyebaran](#).

 Note

Amazon FSx mengelola tabel rute ini untuk sistem file multi-AZ menggunakan otentikasi berbasis tag. Tabel rute ini ditandai dengan `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Saat membuat FSx untuk sistem file ONTAP Multi-AZ menggunakan CloudFormation kami sarankan Anda menambahkan `Key: AmazonFSx; Value: ManagedByAmazonFSx` tag secara manual.

- Untuk jenis Jaringan, pilih IPv4(hanya untuk IPv4 dukungan) atau Dual-stack (untuk keduanya IPv4 dan IPv6 dukungan). Anda dapat mengubah jenis jaringan dari sistem file yang ada kapan saja. Untuk informasi selengkapnya, lihat [Mengubah jenis jaringan](#).

 Note

Jika Anda bermaksud membuat sistem file ONTAP FSx untuk yang menggunakan mode dual-stack, Anda harus terlebih dahulu menetapkan IPv6 blok CIDR yang disediakan Amazon ke VPC dan subnet Anda. Untuk informasi selengkapnya, lihat [IPv6 Menambahkan dukungan untuk VPC Anda](#) di Panduan Pengguna Amazon Virtual Private Cloud.

- (Hanya multi-AZ) Rentang IPv4 alamat titik akhir menentukan rentang IPv4 alamat di mana titik akhir untuk mengakses sistem file Anda dibuat.

Anda memiliki tiga opsi untuk rentang IPv4 alamat titik akhir:

- Rentang IPv4 alamat yang tidak dialokasikan dari VPC Anda — FSx Amazon memilih 64 alamat IP terakhir dari rentang CIDR utama VPC untuk digunakan sebagai rentang alamat titik akhir untuk sistem file. IPv4 Rentang ini dibagi di beberapa sistem file jika Anda memilih opsi ini beberapa kali.

 Note

Opsi ini berwarna abu-abu jika salah satu dari 64 alamat IP terakhir dalam rentang CIDR utama VPC digunakan oleh subnet. Dalam hal ini, Anda masih dapat memilih

rentang alamat in-VPC (yaitu, rentang yang tidak berada di akhir rentang CIDR utama Anda atau rentang yang ada di CIDR sekunder VPC Anda) dengan memilih opsi Masukkan rentang alamat IP.

- Rentang IPv4 alamat mengambang di luar VPC Anda - Amazon FSx memilih rentang alamat 198.19.x.0/24 yang belum digunakan oleh sistem file lain dengan VPC dan tabel rute yang sama.
- Masukkan rentang IPv4 alamat — Anda dapat memberikan rentang CIDR yang Anda pilih sendiri. Rentang IPv4 alamat yang Anda pilih dapat berada di dalam atau di luar rentang alamat IP VPC, asalkan tidak tumpang tindih dengan subnet apa pun.

 Note

Jangan memilih rentang apa pun yang termasuk dalam rentang CIDR berikut, karena tidak kompatibel dengan FSx ONTAP:

- 0.0.0.0/8
- 127.0.0.0/8
- 198.19.0.0/20
- 224.0.0.0/4
- 240.0.0.0/4
- 255.255.255.255/32

- (Hanya multi-AZ dan dual-stack) Rentang IPv6 alamat titik akhir menentukan rentang IPv6 alamat tempat titik akhir untuk mengakses sistem file Anda dibuat. Anda memiliki dua opsi untuk rentang IPv6 alamat titik akhir:
 - Rentang IPv6 alamat yang tidak dialokasikan dari VPC Anda — FSx Amazon memilih blok 1024 alamat yang IPv6 tersedia dari salah satu rentang CIDR VPC IPv6 untuk digunakan sebagai rentang alamat titik akhir untuk sistem file. IPv6
 - Masukkan rentang IPv6 alamat — Anda dapat memberikan rentang IPv6 CIDR yang Anda pilih sendiri. Rentang IPv6 alamat yang Anda pilih dapat berada di dalam atau di luar rentang IPv6 alamat VPC, asalkan tidak tumpang tindih dengan subnet apa pun.
7. Di bagian Enkripsi, untuk kunci Enkripsi, pilih kunci enkripsi AWS Key Management Service (AWS KMS) yang melindungi data sistem file Anda saat istirahat.
 8. Untuk kata sandi administratif sistem file, masukkan kata sandi aman untuk `fsxadmin` pengguna. Konfirmasikan kata sandi.

Anda dapat menggunakan `fsxadmin` pengguna untuk mengelola sistem file Anda menggunakan ONTAP CLI dan REST API. Untuk informasi selengkapnya tentang `fsxadmin` pengguna, lihat [Mengelola sistem file dengan ONTAP CLI](#).

9. Di bagian konfigurasi mesin virtual penyimpanan default, berikan informasi berikut:

- Di bidang nama mesin virtual Penyimpanan, berikan nama untuk mesin virtual penyimpanan. Anda dapat menggunakan maksimal 47 karakter alfanumerik, ditambah karakter khusus garis bawah (`_`).
- Untuk kata sandi administratif SVM, Anda dapat memilih Tentukan kata sandi dan berikan kata sandi untuk pengguna SVM. `vsadmin` Anda dapat menggunakan `vsadmin` pengguna untuk mengelola SVM menggunakan ONTAP CLI atau REST API. Untuk informasi selengkapnya tentang `vsadmin` pengguna, lihat [Mengelola SVMs dengan ONTAP CLI](#).

Jika Anda memilih Jangan tentukan kata sandi (default), Anda masih dapat menggunakan `fsxadmin` pengguna sistem file untuk mengelola sistem file Anda menggunakan ONTAP CLI atau REST API, tetapi Anda tidak dapat menggunakan pengguna SVM Anda untuk melakukan `vsadmin` hal yang sama.

- Untuk gaya keamanan Volume, pilih antara Unix (Linux) dan NTFS untuk volume. Untuk informasi selengkapnya, lihat [Gaya keamanan volume](#).
- Di bagian Active Directory, Anda dapat bergabung dengan Active Directory ke SVM. Untuk informasi selengkapnya, lihat [Bekerja dengan Microsoft Active Directory FSx untuk ONTAP](#).

Jika Anda tidak ingin bergabung dengan SVM Anda ke Active Directory, pilih Jangan bergabung dengan Active Directory.

Jika Anda ingin menggabungkan SVM Anda ke domain Active Directory yang dikelola sendiri, pilih Bergabung dengan Active Directory, dan berikan detail berikut untuk Active Directory Anda:

- Nama NetBIOS dari objek komputer Active Directory yang akan dibuat untuk SVM Anda. Nama NetBIOS tidak boleh melebihi 15 karakter.
- Nama domain yang memenuhi syarat dari Direktori Aktif Anda. Nama domain tidak boleh melebihi 255 karakter.
- Alamat IP server DNS — IPv4 atau IPv6 alamat server Domain Name System (DNS) untuk domain Anda.
- Kredensi akun layanan - Pilih cara memberikan kredensi akun layanan Anda:

- Opsi 1: AWS Secrets Manager rahasia ARN - Rahasia yang berisi nama pengguna dan kata sandi untuk akun layanan di domain Direktori Aktif Anda. Untuk informasi selengkapnya, lihat [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).
- Opsi 2: Kredensi Plaintext
 - Nama pengguna akun layanan — Nama pengguna akun layanan di Microsoft Active Directory yang ada. Jangan sertakan awalan atau akhiran domain. Misalnya, untuk `EXAMPLE\ADMIN`, gunakan saja `ADMIN`.
 - Kata sandi akun layanan — Kata sandi untuk akun layanan.
 - Konfirmasi kata sandi — Kata sandi untuk akun layanan.
- (Opsional) Unit Organisasi (OU) - Nama jalur yang dibedakan dari unit organisasi tempat Anda ingin bergabung dengan sistem file Anda.
- Grup administrator sistem file yang didelegasikan — Nama grup di Direktori Aktif Anda yang dapat mengelola sistem file Anda.

Jika Anda menggunakan AWS Managed Microsoft AD, Anda perlu menentukan grup seperti Administrator Delegasi, FSx Administrator AWS AWS Delegasi, atau grup kustom dengan izin yang didelegasikan ke OU.

Jika Anda bergabung dengan iklan yang dikelola sendiri, gunakan nama grup di iklan Anda. Grup defaultnya adalah `Domain Admins`.

10. Di bagian konfigurasi volume default, berikan informasi berikut untuk volume default yang dibuat dengan sistem file Anda:

- Di bidang Nama volume, berikan nama untuk volume. Anda dapat menggunakan hingga 203 karakter alfanumerik atau garis bawah (`_`).
- (Sistem file dengan satu pasangan HA saja) Untuk gaya Volume, pilih salah satu FlexVol atau FlexGroup. FlexVol volume adalah volume tujuan umum yang dapat mencapai 300 tebibytes (TiB) dalam ukuran. FlexGroup volume ditujukan untuk beban kerja berkinerja tinggi dan dapat berukuran hingga 20 PiB.
- Untuk ukuran Volume, masukkan bilangan bulat apa pun dalam kisaran 20—314.572.800 mebibytes (MiB) untuk FlexVol volume atau 800 gibibyte (GiB) —2.400 TiB per pasangan HA untuk volume. FlexGroup Misalnya, sistem file dengan 12 pasangan HA akan memiliki ukuran volume minimum 9.600 GiB dan ukuran maksimum 20.480 TiB.

- Untuk tipe Volume, pilih Read-Write (RW) untuk membuat volume yang dapat dibaca dan ditulis atau Perlindungan Data (DP) untuk membuat volume yang hanya-baca dan dapat digunakan sebagai tujuan hubungan atau. NetApp SnapMirror SnapVault Untuk informasi selengkapnya, lihat [Tipe volume](#).
- Untuk jalur Junction, masukkan lokasi di dalam sistem file untuk me-mount volume. Nama harus memiliki garis miring ke depan, misalnya/vol3.
- Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur efisiensi penyimpanan ONTAP (deduplikasi, kompresi, dan pemadatan). Untuk informasi selengkapnya, lihat [Efisiensi penyimpanan](#).
- Untuk kebijakan Snapshot, pilih kebijakan snapshot untuk volume. Untuk informasi selengkapnya tentang kebijakan snapshot, lihat [Kebijakan snapshot](#).

Jika memilih Kebijakan khusus, Anda harus menentukan nama kebijakan di bidang kebijakan khusus. Kebijakan kustom harus sudah ada di SVM atau di sistem file. Anda dapat membuat kebijakan snapshot khusus dengan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat [Membuat Kebijakan Snapshot di Dokumentasi](#) Produk NetApp ONTAP.

11. Di bagian Tingkatan penyimpanan volume default, untuk kebijakan tingkatan kumpulan Kapasitas, pilih kebijakan tiering kumpulan penyimpanan untuk volume, yang dapat berupa Otomatis (default), Hanya Snapshot, Semua, atau Tidak Ada. Untuk informasi selengkapnya tentang kebijakan tingkatan kumpulan kapasitas, lihat [Kebijakan tingkatan volume](#).

Untuk periode pendinginan kebijakan Tiering, jika Anda telah menetapkan tingkat penyimpanan ke salah satu kebijakan Auto dan Snapshot-only kebijakan. Nilai yang valid adalah 2-183 hari. Periode pendinginan kebijakan tingkat volume menentukan jumlah hari sebelum data yang belum diakses ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas.

12. Di bagian SnapLock Konfigurasi Volume Default, untuk SnapLockKonfigurasi, pilih antara Diaktifkan dan Dinonaktifkan. Untuk informasi selengkapnya tentang mengonfigurasi volume SnapLock Kepatuhan atau volume SnapLock Perusahaan, lihat [Memahami SnapLock Kepatuhan](#) dan [Memahami SnapLock Perusahaan](#). Untuk informasi selengkapnya tentang SnapLock, lihat [Melindungi data Anda dengan SnapLock](#).

13. Di Backup dan pemeliharaan - opsional, Anda dapat mengatur opsi berikut:

- Untuk pencadangan otomatis harian, pilih Diaktifkan untuk pencadangan harian otomatis. Pengaturan ini diaktifkan secara default.
- Untuk jendela pencadangan otomatis Harian, atur 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.

- Untuk periode retensi cadangan otomatis, tetapkan periode dari 1—90 hari yang ingin Anda pertahankan pencadangan otomatis.
- Untuk jendela pemeliharaan Mingguan, Anda dapat mengatur waktu dalam seminggu yang Anda inginkan untuk memulai jendela pemeliharaan. 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.

14. Untuk Tag - opsional, Anda dapat memasukkan 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.

Pilih Selanjutnya.

15. Tinjau konfigurasi sistem file yang ditampilkan pada halaman Buat sistem file. Untuk referensi Anda, perhatikan pengaturan sistem file mana yang dapat Anda modifikasi setelah sistem file dibuat.
16. Pilih Buat sistem file.

Untuk membuat sistem file (CLI)

- FSx Untuk membuat sistem file ONTAP, gunakan perintah [create-file-system](#) CLI (atau operasi API yang [CreateFileSystem](#) setara), seperti yang ditunjukkan pada contoh berikut.

 Note

Anda tidak dapat mengubah jenis penerapan sistem file setelah pembuatan. Jika Anda ingin mengubah jenis penerapan (misalnya, untuk berpindah dari Single-AZ 1 ke Single-AZ 2), Anda dapat mencadangkan data Anda dan mengembalikannya pada sistem file baru. Anda juga dapat memigrasikan data Anda dengan NetApp SnapMirror, dengan AWS DataSync, atau dengan alat penyalinan data pihak ketiga. Untuk informasi selengkapnya, lihat [Migrasi ke FSx untuk ONTAP menggunakan NetApp SnapMirror](#) dan [Migrasi ke FSx untuk ONTAP menggunakan AWS DataSync](#).

```
aws fsx create-file-system \  
  --file-system-type ONTAP \  
  --availability-zone us-east-1a \  
  --size 1000 \  
  --subnet-id subnet-12345678 \  
  --tags Key=Value
```

```
--storage-capacity 1024 \
--storage-type SSD \
--security-group-ids security-group-id \

--subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
--ontap-configuration DeploymentType=MULTI_AZ_1,
    ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

Setelah berhasil membuat sistem file, Amazon FSx mengembalikan deskripsi sistem file dalam format JSON seperti yang ditunjukkan pada contoh berikut.

```
{
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJa1rXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
```

```
        "Mode": "AUTOMATIC",
        "Iops": 3072
    },
    "PreferredSubnetId": "subnet-abcdef1234567890b",
    "RouteTableIds": [
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
    ],
    "ThroughputCapacity": 512,
    "WeeklyMaintenanceStartTime": "4:10:00"
}
}
```

Note

Berbeda dengan proses pembuatan sistem file di konsol, perintah `create-file-system` CLI dan operasi `CreateFileSystem` API tidak membuat SVM atau volume default. Untuk membuat SVM, lihat [Membuat mesin virtual penyimpanan \(SVM\)](#); untuk membuat volume, lihat [Membuat volume](#).

Membuat FSx untuk sistem file ONTAP di subnet bersama

Berbagi VPC memungkinkan beberapa Akun AWS untuk membuat sumber daya menjadi cloud pribadi virtual bersama yang dikelola secara terpusat (). VPCs Dalam model ini, akun yang memiliki VPC (pemilik) berbagi satu atau lebih subnet dengan akun lain (peserta) yang termasuk dalam organisasi yang sama dari AWS Organizations

Akun peserta dapat membuat FSx untuk sistem file ONTAP Single-AZ dan Multi-AZ dalam subnet VPC yang telah dibagikan oleh akun pemilik dengan mereka. Agar akun peserta dapat membuat sistem file multi-AZ, akun pemilik juga perlu memberikan FSx izin Amazon untuk mengubah tabel rute di subnet bersama atas nama akun peserta. Untuk informasi selengkapnya, lihat [Mengelola dukungan VPC bersama untuk sistem file multi-AZ](#).

Note

Merupakan tanggung jawab akun peserta untuk berkoordinasi dengan pemilik VPC untuk mencegah pembuatan subnet VPC berikutnya yang akan tumpang tindih dengan CIDR

in-VPC dari sistem file peserta. Jika subnet tumpang tindih, lalu lintas ke sistem file dapat terganggu.

Persyaratan dan pertimbangan subnet bersama

Saat membuat FSx untuk sistem file ONTAP ke subnet bersama, perhatikan hal berikut:

- Pemilik subnet VPC harus berbagi subnet dengan akun peserta sebelum akun tersebut dapat membuat sistem file FSx untuk ONTAP di dalamnya.
- Anda tidak dapat meluncurkan sumber daya menggunakan grup keamanan default untuk VPC karena milik pemilik. Selain itu, akun peserta tidak dapat meluncurkan sumber daya menggunakan grup keamanan yang dimiliki oleh peserta lain atau pemilik.
- Dalam subnet bersama, peserta dan pemilik secara terpisah mengontrol grup keamanan dalam setiap akun masing-masing. Akun pemilik dapat melihat grup keamanan yang dibuat oleh peserta, tetapi tidak dapat melakukan tindakan apa pun pada mereka. Jika akun pemilik ingin menghapus atau memodifikasi grup keamanan ini, peserta yang membuat grup keamanan harus mengambil tindakan.
- Akun peserta dapat melihat, membuat, memodifikasi, dan menghapus sistem file Single-AZ dan sumber daya terkait mereka dalam subnet yang telah dibagikan oleh akun pemilik dengan mereka.
- Akun peserta dapat membuat, melihat, memodifikasi, dan menghapus sistem file multi-AZ dan sumber daya terkait mereka dalam subnet yang telah dibagikan oleh akun pemilik dengan mereka. Selain itu, akun pemilik juga harus memberikan izin FSx layanan Amazon untuk mengubah tabel rute di subnet bersama atas nama akun peserta. Untuk informasi selengkapnya, lihat [Mengelola dukungan VPC bersama untuk sistem file multi-AZ](#)
- Pemilik VPC bersama tidak dapat melihat, memodifikasi, atau menghapus sumber daya yang dibuat peserta di subnet bersama. Ini merupakan tambahan dari sumber daya VPC yang setiap akun memiliki akses berbeda. Untuk informasi selengkapnya, lihat [Tanggung jawab dan izin untuk pemilik dan peserta](#) di Panduan Pengguna Amazon VPC.

Untuk informasi selengkapnya, lihat [Berbagi VPC Anda dengan akun lain](#) di Panduan Pengguna Amazon VPC.

Saat berbagi subnet VPC

Saat membagikan subnet Anda dengan akun peserta yang akan dibuat FSx untuk sistem file ONTAP di subnet bersama, Anda perlu melakukan hal berikut:

- Pemilik VPC perlu menggunakan AWS Resource Access Manager untuk berbagi VPCs dan subnet dengan aman dengan yang lain. Akun AWS Untuk informasi selengkapnya, lihat [Berbagi AWS sumber daya Anda](#) di Panduan AWS Resource Access Manager Pengguna.
- Pemilik VPC perlu berbagi satu atau lebih VPCs dengan akun peserta. Untuk informasi selengkapnya, lihat [Berbagi VPC Anda dengan akun lain](#) di Panduan Pengguna Amazon Virtual Private Cloud.
- Agar akun peserta dapat dibuat FSx untuk sistem file ONTAP Multi-AZ, pemilik VPC juga harus memberikan izin FSx layanan Amazon untuk membuat dan memodifikasi tabel rute di subnet bersama atas nama akun peserta. Ini karena FSx untuk sistem file Multi-AZ ONTAP menggunakan alamat IP mengambang sehingga klien yang terhubung dapat dengan mulus bertransisi antara server file pilihan dan siaga selama acara failover. Ketika peristiwa failover terjadi, Amazon FSx memperbarui semua rute di semua tabel rute yang terkait dengan sistem file untuk menunjuk ke server file yang sedang aktif.

Mengelola dukungan VPC bersama untuk sistem file multi-AZ

Akun pemilik dapat mengelola apakah akun peserta dapat membuat Multi-AZ FSx untuk sistem file ONTAP di subnet VPC yang telah dibagikan pemilik dengan peserta menggunakan,, dan API Konsol Manajemen AWS AWS CLI, seperti yang dijelaskan di bagian berikut.

Untuk mengelola berbagi VPC untuk sistem file Multi-AZ (konsol)

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

1. Pada panel navigasi, silakan pilih Pengaturan.
2. Temukan pengaturan VPC bersama Multi-AZ di halaman Pengaturan.
 - Untuk mengaktifkan berbagi VPC untuk sistem file multi-AZ di subnet VPC yang Anda bagikan, pilih Aktifkan pembaruan tabel rute dari akun peserta.
 - Untuk menonaktifkan berbagi VPC untuk sistem file multi-AZ di semua VPCs yang Anda miliki, pilih Nonaktifkan pembaruan tabel rute dari akun peserta. Layar konfirmasi ditampilkan.

Important

Kami sangat menyarankan agar sistem file Multi-AZ yang dibuat oleh peserta di VPC bersama dihapus sebelum Anda menonaktifkan fitur ini. Setelah fitur dinonaktifkan,

sistem file ini akan memasuki MISCONFIGURED status dan akan berisiko menjadi tidak tersedia.

3. Masuk **confirm** dan pilih Konfirmasi untuk menonaktifkan fitur.

Untuk mengelola berbagi VPC untuk sistem file Multi-AZ ()AWS CLI

1. Untuk melihat pengaturan saat ini untuk berbagi VPC multi-AZ, gunakan perintah [describe-shared-vpc-configuration](#)CLI, atau perintah API yang [DescribeSharedVpcConfiguration](#)setara, ditampilkan sebagai berikut:

```
$ aws fsx describe-shared-vpc-configuration
```

Layanan menanggapi permintaan yang berhasil sebagai berikut:

```
{
  "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

2. Untuk mengelola konfigurasi VPC bersama Multi-AZ, gunakan perintah [update-shared-vpc-configuration](#)CLI, atau perintah API yang setara. [UpdateSharedVpcConfiguration](#) Contoh berikut memungkinkan berbagi VPC untuk sistem file Multi-AZ.

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
```

Layanan menanggapi permintaan yang berhasil sebagai berikut:

```
{
  "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
}
```

3. Untuk menonaktifkan fitur, atur `EnableFsxRouteTableUpdatesFromParticipantAccounts` ke `false`, seperti yang ditunjukkan pada contoh berikut.

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts false
```

Layanan menanggapi permintaan yang berhasil sebagai berikut:

```
{  
  "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"  
}
```

Memperbarui sistem file

Topik ini menjelaskan properti sistem file yang ada yang dapat Anda perbarui, dan menyediakan prosedur untuk melakukannya menggunakan FSx konsol Amazon dan CLI. Anda dapat memperbarui properti sistem file ONTAP berikut FSx menggunakan FSx konsol Amazon, AWS CLI, dan API:

- Pencadangan harian otomatis. Mengaktifkan atau menonaktifkan pencadangan harian otomatis, memodifikasi jendela cadangan dan periode retensi cadangan. Untuk informasi selengkapnya, lihat [Pencadangan harian otomatis](#).
- Jendela pemeliharaan mingguan. Menetapkan hari dalam seminggu dan waktu Amazon FSx melakukan pemeliharaan dan pembaruan sistem file. Untuk informasi selengkapnya, lihat [Mengoptimalkan kinerja dengan jendela FSx pemeliharaan Amazon](#).
- Kata sandi administrasi sistem file. Mengubah kata sandi untuk fsxadmin pengguna sistem file. Anda dapat menggunakan fsxadmin pengguna untuk mengelola sistem file Anda menggunakan ONTAP CLI dan REST API. Untuk informasi selengkapnya tentang fsxadmin pengguna, lihat [Mengelola sistem file dengan ONTAP CLI](#).
- Tabel rute Amazon VPC. Dengan sistem file Multi-AZ FSx untuk ONTAP, titik akhir yang Anda gunakan untuk mengakses data melalui NFS atau SMB dan titik akhir manajemen untuk mengakses CLI ONTAP, API, dan Konsol menggunakan alamat IP NetApp mengambang di tabel rute VPC Amazon yang Anda kaitkan dengan sistem file Anda. Anda dapat mengaitkan tabel rute baru yang Anda buat dengan sistem file multi-AZ yang ada—memungkinkan Anda mengonfigurasi klien mana yang dapat mengakses data Anda bahkan saat jaringan Anda berkembang. Anda juga dapat memisahkan (menghapus) tabel rute yang ada dari sistem file Anda.

Note

Amazon FSx mengelola tabel rute VPC untuk sistem file multi-AZ menggunakan otentikasi berbasis tag. Tabel rute ini ditandai dengan `Key: AmazonFSx`; `Value: ManagedByAmazonFSx`. Saat membuat atau memperbarui FSx untuk sistem file ONTAP

Multi-AZ menggunakan CloudFormation kami sarankan Anda menambahkan Key : AmazonFSx; Value: ManagedByAmazonFSx tag secara manual.

Untuk memperbarui sistem file (konsol)

Prosedur berikut memberi Anda petunjuk tentang cara membuat pembaruan ke sistem file ONTAP FSx yang sudah ada menggunakan file. Konsol Manajemen AWS

Untuk memperbarui backup harian otomatis

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Untuk menampilkan halaman detail sistem file, di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file FSx untuk ONTAP yang ingin Anda perbarui.
3. Pilih tab Backup di panel kedua pada halaman.
4. Pilih Perbarui.
5. Ubah pengaturan cadangan harian otomatis untuk sistem file ini.
6. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk memperbarui jendela pemeliharaan mingguan

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Untuk menampilkan halaman detail sistem file, di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file FSx untuk ONTAP yang ingin Anda perbarui.
3. Pilih tab Administrasi di panel kedua pada halaman.
4. Di panel Pemeliharaan, pilih Perbarui.
5. Ubah kapan jendela pemeliharaan mingguan terjadi untuk sistem file ini.
6. Pilih Simpan untuk menyimpan perubahan Anda.

Untuk mengubah kata sandi administrasi sistem file

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Untuk menampilkan halaman detail sistem file, di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file FSx untuk ONTAP yang ingin Anda perbarui.
3. Pilih tab Administrasi.

4. Di panel administrasi ONTAP, pilih Perbarui di bawah kata sandi administrator ONTAP.
5. Di kotak dialog Perbarui kredensi administrator ONTAP, masukkan kata sandi baru di bidang kata sandi administratif ONTAP.
6. Gunakan kolom Konfirmasi kata sandi untuk mengonfirmasi kata sandi.
7. Pilih Perbarui kredensi untuk menyimpan perubahan Anda.

 Note

Jika Anda menerima kesalahan yang menyatakan bahwa kata sandi baru tidak memenuhi persyaratan kata sandi, Anda dapat menggunakan perintah [security login role config show](#) ONTAPCLI untuk melihat pengaturan persyaratan kata sandi pada sistem file. Untuk informasi selengkapnya, termasuk petunjuk tentang cara mengubah setelan kata sandi, lihat [Gagal memperbarui kata sandi fsxadmin akun](#).

Untuk memperbarui tabel rute VPC pada sistem file Multi-AZ

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Untuk menampilkan halaman detail sistem file, di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file FSx untuk ONTAP yang ingin Anda perbarui.
3. Untuk Tindakan, pilih Perbarui sistem file > Perbarui tabel rute. Atau, di panel Jaringan & keamanan, pilih Kelola di sebelah tabel Route sistem file.
4. Dalam kotak dialog Kelola tabel rute. lakukan salah satu hal berikut:
 - Untuk mengaitkan tabel rute VPC baru, pilih tabel rute dari daftar tarik-turun Tabel rute baru Associate, lalu pilih Associate.
 - Untuk memisahkan tabel rute VPC yang ada, pilih tabel rute dari panel Tabel rute saat ini, lalu pilih Pisahkan.
5. Pilih Tutup.

Untuk memperbarui sistem file (CLI)

Prosedur berikut menggambarkan cara membuat pembaruan ke sistem file ONTAP FSx yang ada menggunakan file. AWS CLI

1. Untuk memperbarui konfigurasi FSx untuk sistem file ONTAP, gunakan perintah [update-file-system](#) CLI (atau operasi API yang [UpdateFileSystem](#) setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --ontap-configuration
    AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
    WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
    FsxAdminPassword=new-fsx-admin-password
```

2. Untuk menonaktifkan backup harian otomatis, atur AutomaticBackupRetentionDays properti ke 0.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --ontap-configuration AutomaticBackupRetentionDays=0
```

Mengelola pasangan ketersediaan tinggi (HA)

Masing-masing FSx untuk sistem file ONTAP didukung oleh satu atau lebih pasangan server file ketersediaan tinggi (HA) dalam konfigurasi siaga aktif. Dalam konfigurasi ini, ada server file pilihan yang secara aktif melayani lalu lintas dan server file sekunder yang mengambil alih jika server aktif tidak tersedia. FSx untuk sistem file generasi pertama ONTAP didukung oleh satu pasangan HA, yang memberikan hingga 4 kapasitas throughput GBps dan 160.000 SSD. IOPs FSx untuk ONTAP sistem file multi-AZ generasi kedua didukung oleh satu pasangan HA juga, dan mereka memberikan hingga 6 kapasitas throughput dan 200.000 GBps IOPS SSD. FSx untuk sistem file Single-AZ generasi kedua ONTAP didukung oleh hingga 12 pasang HA, yang dapat menghasilkan hingga 72 GBps kapasitas throughput dan 2.400.000 IOPS SSD (6 GBps kapasitas throughput dan 200.000 IOPS SSD per pasangan HA).

Saat Anda membuat sistem file dari FSx konsol Amazon, Amazon FSx merekomendasikan jumlah pasangan HA yang harus Anda gunakan berdasarkan penyimpanan SSD yang Anda inginkan. Anda juga dapat secara manual memilih jumlah pasangan HA berdasarkan beban kerja dan persyaratan kinerja Anda. Kami menyarankan Anda menggunakan satu pasangan HA jika persyaratan sistem file Anda dipenuhi hingga 6 GBps kapasitas throughput dan 200.000 SSD IOPs, dan beberapa pasangan HA jika beban kerja Anda membutuhkan tingkat skalabilitas kinerja yang lebih tinggi.

Setiap pasangan HA memiliki satu agregat, yang merupakan kumpulan disk fisik yang logis.

 Note

Anda dapat menambahkan pasangan HA ke sistem file Single-AZ generasi kedua. Untuk informasi selengkapnya, lihat [Menambahkan pasangan ketersediaan tinggi \(HA\)](#). Jika tidak, Anda dapat memigrasikan data antar sistem file (dengan pasangan HA yang berbeda) menggunakan SnapMirror AWS DataSync, atau dengan memulihkan data Anda dari cadangan ke sistem file baru.

Menambahkan pasangan ketersediaan tinggi (HA)

FSx untuk sistem file ONTAP terdiri dari satu atau lebih pasangan HA dari server file. Sistem file generasi pertama dan sistem file multi-AZ generasi kedua mendukung satu pasangan HA sedangkan sistem file single-AZ generasi kedua mendukung hingga 12 pasang HA. Anda juga dapat menambahkan lebih banyak pasangan HA setelah membuat sistem file Single-AZ generasi kedua (hingga maksimum 12). Menambahkan pasangan HA tidak mengganggu dan biasanya hanya membutuhkan beberapa menit untuk menyelesaikannya.

Pertimbangkan poin-poin berikut saat menambahkan pasangan HA ke sistem file Anda:

- Menambahkan pasangan HA ke sistem file Anda memperkenalkan server file baru dengan penyimpanannya sendiri (atau agregat). Pasangan HA baru memiliki kapasitas throughput dan kapasitas penyimpanan yang sama dengan pasangan HA sistem file Anda yang ada. Misalnya, asumsikan bahwa sistem file Anda memiliki dua pasang HA dengan total 12 GBps kapasitas throughput dan 2 tebibytes (TiB) penyimpanan SSD. Jika Anda menambahkan satu pasangan HA baru, maka sistem file Anda akan memiliki 18 GBps kapasitas throughput dan 3 TiB penyimpanan SSD.
- Untuk mendapatkan keuntungan dari kinerja tambahan pasangan HA baru, Anda perlu memindahkan beberapa volume yang ada ke pasangan HA baru dan memasang kembali klien untuk terhubung dengannya. Untuk informasi selengkapnya, lihat [Menyeimbangkan beban kerja di seluruh pasangan HA](#).
- Anda tidak dapat mengubah kapasitas throughput sistem file, kapasitas penyimpanan SSD, atau IOPS SSD yang disediakan saat menambahkan pasangan HA atau saat pembaruan untuk menambahkan pasangan HA sedang berlangsung.
- Anda tidak dapat menghapus pasangan HA setelah Anda menambahkannya. Kami merekomendasikan untuk menskalakan kapasitas throughput sistem file Anda jika Anda membutuhkan lebih banyak kinerja sementara (dengan asumsi bahwa sistem file Anda tidak pada

kapasitas throughput tertinggi). Ini meningkatkan kapasitas throughput pasangan HA sistem file Anda yang ada.

- Protokol iSCSI tersedia pada sistem file yang memiliki enam atau lebih sedikit pasangan ketersediaan tinggi (pasangan HA). NVMe/TCP Protokol ini tersedia pada sistem file generasi kedua yang memiliki enam atau lebih sedikit pasangan HA. Untuk informasi selengkapnya, lihat [Mengakses data FSx ONTAP Anda](#).
- Saat Anda menambahkan pasangan HA baru ke sistem file Anda, NVMe cache diaktifkan secara default untuk node sistem file baru. Kami merekomendasikan untuk menonaktifkannya untuk beban kerja yang berat. Untuk informasi selengkapnya, lihat [Mengelola NVMe cache](#).

Untuk menambahkan pasangan HA

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Untuk menampilkan halaman detail sistem file, di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file FSx untuk ONTAP yang ingin Anda perbarui.
3. Pada panel Ringkasan, untuk Jumlah pasangan HA, pilih Perbarui.
4. Dari tarik-turun HA Pairs, pilih jumlah pasangan HA yang ingin Anda tambahkan ke sistem file Anda.
5. Pilih tombol Perbarui.

Setelah Anda menambahkan pasangan HA, penting untuk menyeimbangkan kembali data Anda yang ada untuk memastikan bahwa I/O sisa-sisa Anda didistribusikan secara merata di seluruh pasangan HA sistem file Anda. Untuk informasi selengkapnya, lihat [Menyeimbangkan beban kerja di seluruh pasangan HA](#).

Menyeimbangkan beban kerja di seluruh pasangan HA

Jika Anda memiliki sistem file dengan beberapa pasangan ketersediaan tinggi (HA), maka throughput dan penyimpanannya tersebar di setiap pasangan HA Anda. FSx untuk ONTAP secara otomatis menyeimbangkan file Anda saat ditulis ke sistem file Anda, tetapi data beban kerja dan I/O Anda tidak lagi seimbang setelah Anda menambahkan pasangan HA. Selain itu, dalam kasus yang jarang terjadi, data beban kerja atau I/O Anda dapat menjadi tidak seimbang di seluruh pasangan HA sistem file Anda yang ada, yang dapat memengaruhi kinerja keseluruhan beban kerja Anda. Jika beban kerja Anda tidak seimbang, Anda dapat menyeimbangkannya kembali di setiap pasangan HA sistem file Anda (dan server dan agregat file yang sepadan — kumpulan penyimpanan yang membentuk tingkat penyimpanan utama Anda).

Topik

- [Saldo pemanfaatan penyimpanan primer](#)
- [Ketidakseimbangan pemanfaatan kinerja file server dan disk](#)
- [Memetakan CloudWatch dimensi ke sumber daya ONTAP CLI dan REST API](#)
- [Menyeimbangkan kembali klien](#)
- [Menyeimbangkan kembali volume](#)

Saldo pemanfaatan penyimpanan primer

Kapasitas penyimpanan utama sistem file Anda dibagi secara merata di antara masing-masing pasangan HA Anda di kumpulan penyimpanan yang disebut agregat. Setiap pasangan HA memiliki satu agregat. Kami menyarankan Anda mempertahankan pemanfaatan rata-rata tidak lebih dari 80% untuk tingkat penyimpanan utama Anda secara berkelanjutan. Untuk sistem file dengan beberapa pasangan HA, kami menyarankan Anda mempertahankan pemanfaatan rata-rata hingga 80% untuk setiap agregat.

Mempertahankan pemanfaatan 80% memastikan ada ruang kosong untuk data baru yang masuk, dan mempertahankan overhead yang sehat untuk operasi pemeliharaan yang sementara dapat mengklaim ruang kosong pada agregat Anda.

Jika Anda melihat bahwa agregat Anda tidak seimbang, Anda dapat meningkatkan kapasitas penyimpanan utama sistem file Anda (sepadan meningkatkan kapasitas penyimpanan setiap agregat), atau Anda dapat memindahkan volume Anda antar agregat. Untuk informasi selengkapnya, lihat [Memindahkan volume antar agregat](#).

Ketidakseimbangan pemanfaatan kinerja file server dan disk

Kemampuan kinerja total sistem file Anda (seperti throughput jaringan, file server ke throughput disk dan IOPS, dan IOPS disk) dibagi secara merata di antara pasangan HA sistem file Anda. Kami menyarankan Anda mempertahankan pemanfaatan rata-rata di bawah 50% (dan pemanfaatan puncak maksimum di bawah 80%) untuk semua batas kinerja secara berkelanjutan — ini berlaku untuk pemanfaatan keseluruhan sumber daya server file sistem file Anda di semua pasangan HA, serta pada basis server per file.

Jika Anda melihat bahwa pemanfaatan kinerja server file Anda tidak seimbang—dan server file di mana beban kerja Anda tidak seimbang memiliki pemanfaatan berkelanjutan lebih dari 80% —Anda dapat menggunakan ONTAP CLI dan REST API untuk mendiagnosis lebih lanjut

penyebab ketidakseimbangan kinerja dan memperbaikinya. Berikut ini adalah tabel indikator ketidakseimbangan yang mungkin dan langkah selanjutnya untuk diagnosis lebih lanjut.

Jika sistem file Anda...	Maka...
Throughput disk server file atau IOPS disk server file tidak seimbang	Anda mungkin mengalami hotspotting I/O pada subset pasangan HA (subset volume Anda yang berisi sejumlah besar data yang diakses) yang dapat membatasi kinerja keseluruhan beban kerja Anda karena terhambat terhadap subset pasangan HA. Untuk setiap server file yang sangat digunakan, periksa volume yang paling banyak digunakan untuk melihat volume mana yang memiliki aktivitas paling banyak dalam agregat. Untuk informasi lebih lanjut tentang prosedur ini, lihat Menyeimbangkan kembali volume .
Throughput jaringan tidak seimbang, tetapi throughput disk server file Anda, IOPS disk server file, atau IOPS disk Anda tidak seimbang	Data Anda didistribusikan secara merata di seluruh pasangan HA, tetapi klien Anda tidak. Untuk server file yang memiliki lebih banyak pemanfaatan throughput jaringan daripada yang lain, periksa klien teratas untuk setiap server file, kemudian menyeimbangkan kembali klien tersebut dengan melepas volume apa pun dari klien tersebut dan mengatur ulang mereka menggunakan titik akhir yang berbeda pada pasangan HA yang berbeda. Untuk informasi lebih lanjut tentang prosedur ini, lihat Menyeimbangkan kembali klien .

Memetakan CloudWatch dimensi ke sumber daya ONTAP CLI dan REST API

Sistem file generasi kedua Anda memiliki CloudWatch metrik Amazon dengan dimensi atau. FileServer Aggregate Untuk mendiagnosis lebih lanjut kasus ketidakseimbangan, Anda perlu memetakan nilai dimensi ini ke server file tertentu (atau node) dan agregat di ONTAP CLI atau REST API.

- Untuk server file, setiap nama server file memetakan ke nama server file (atau node) di ONTAP (misalnya, FsxId01234567890abcdef-01). Server file bernomor ganjil adalah server file yang disukai (yaitu, mereka melayani lalu lintas kecuali sistem file gagal ke server file sekunder), sedangkan server file bernomor genap adalah server file sekunder (yaitu, mereka melayani lalu lintas hanya ketika mitra mereka tidak tersedia). Karena itu, server file sekunder biasanya akan menunjukkan pemanfaatan yang lebih sedikit daripada server file pilihan.

- Untuk agregat, setiap nama agregat memetakan ke agregat di ONTAP (misalnya,). aggr1 Ada satu agregat untuk setiap pasangan HA, artinya agregat aggr1 dibagikan oleh server file FsxId01234567890abcdef-01 (server file aktif) dan FsxId01234567890abcdef-02 (server file sekunder) dalam pasangan HA, agregat aggr2 dibagikan oleh server file FsxId01234567890abcdef-03 dan FsxId01234567890abcdef-04, dan seterusnya.

Anda dapat melihat pemetaan antara semua agregat dan server file menggunakan CLI ONTAP.

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna [Menggunakan CLI NetApp ONTAP](#) Amazon FSx untuk NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Gunakan perintah [show agregat penyimpanan](#), tentukan parameternya-fields node.

```
::> storage aggregate show -fields node
aggregate          node
-----
aggr1              FsxId01234567890abcdef-01
aggr2              FsxId01234567890abcdef-03
aggr3              FsxId01234567890abcdef-05
aggr4              FsxId01234567890abcdef-07
aggr5              FsxId01234567890abcdef-09
aggr6              FsxId01234567890abcdef-11
6 entries were displayed.
```

Menyeimbangkan kembali klien

Setelah menambahkan pasangan HA atau jika Anda mengalami ketidakseimbangan I/O di seluruh server file (khususnya dengan pemanfaatan throughput jaringan), Anda dapat menyeimbangkan kembali klien Anda. Jika Anda menyeimbangkan kembali klien setelah menambahkan pasangan HA, Anda dapat melompat ke [Remounting klien](#). Jika tidak, Anda harus terlebih dahulu mengidentifikasi klien dengan lalu lintas tinggi yang ingin Anda pindahkan untuk menyeimbangkan kembali I/O beban kerja Anda.

Jika Anda mengalami ketidakseimbangan I/O di seluruh server file (khususnya dengan pemanfaatan throughput Jaringan), klien I/O yang tinggi mungkin menjadi penyebabnya. Untuk mengidentifikasi klien dengan lalu lintas tinggi, gunakan ONTAP CLI.

Identifikasi klien dengan lalu lintas tinggi

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna [Menggunakan CLI NetApp ONTAP](#) Amazon FSx untuk NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Untuk melihat klien dengan lalu lintas tertinggi, gunakan [statistik klien teratas yang menunjukkan perintah CLI ONTAP](#). Anda dapat secara opsional menentukan `-node` parameter untuk hanya melihat klien teratas untuk server file tertentu. Jika Anda mendiagnosis ketidakseimbangan untuk server file tertentu, gunakan `-node` parameter, ganti `node_name` dengan nama server file (misalnya, `FsxId01234567890abcdef-01`).

Anda dapat menambahkan `-interval` parameter secara opsional, memberikan interval untuk mengukur (dalam detik) sebelum setiap laporan dikeluarkan. Meningkatkan interval (misalnya, hingga maksimum 300 detik) memberikan sampel jangka panjang untuk jumlah lalu lintas yang didorong ke setiap volume. Defaultnya adalah 5 (detik).

```
::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
```

Dalam output, klien teratas ditunjukkan oleh alamat IP dan port mereka.

Client	Vserver	Node	*Total Ops	Total (Bps)
172.17.236.53:938	svm01	FsxId01234567890abcdef-01	2143	140443648
172.17.236.160:898	svm02	FsxId01234567890abcdef-01	812	53215232

Remounting klien

- Anda dapat menyeimbangkan kembali klien ke pasangan HA lainnya. Untuk melakukannya, lepaskan volume dari klien dan pasang kembali menggunakan nama DNS untuk titik akhir NFS/SMB SVM—ini mengembalikan titik akhir acak yang sesuai dengan pasangan HA acak.

Kami menyarankan Anda menggunakan kembali nama DNS, tetapi Anda memiliki opsi untuk secara eksplisit memilih pasangan HA mana yang dipasang klien tertentu. Untuk menjamin bahwa Anda memasang klien ke titik akhir yang berbeda, Anda dapat menentukan alamat IP titik

akhir yang berbeda dari yang sesuai dengan server file yang mengalami lalu lintas tinggi. Anda dapat melakukannya dengan menjalankan perintah berikut:

```
::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
address,curr-node
vserver    lif                address            curr-node
-----
svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
svm01 nfs_smb_management_3 172.31.8.112  FsxId01234567890abcdef-03
2 entries were displayed.
```

Menurut contoh output untuk `statistics top client show` perintah, klien 172.17.236.53 mengarahkan lalu lintas tinggi ke FsxId01234567890abcdef-01. Output dari `network interface show` perintah menunjukkan ini adalah alamatnya 172.31.15.89. Untuk me-mount ke titik akhir yang berbeda, pilih alamat lain (dalam contoh ini, satu-satunya alamat lainnya adalah 172.31.8.112, sesuai dengan FsxId01234567890abcdef-03).

Menyeimbangkan kembali volume

Jika Anda mengalami ketidakseimbangan I/O di seluruh volume atau agregat, Anda dapat menyeimbangkan kembali volume untuk mendistribusikan kembali lalu lintas I/O di seluruh volume Anda.

Note

Jika Anda mengalami ketidakseimbangan pemanfaatan penyimpanan di seluruh agregat Anda, umumnya tidak ada dampak kinerja kecuali pemanfaatan yang tinggi digabungkan dengan ketidakseimbangan I/O. Meskipun Anda dapat memindahkan volume antar agregat untuk menyeimbangkan pemanfaatan penyimpanan, kami sarankan hanya memindahkan volume jika Anda melihat dampak kinerja, karena volume bergerak dapat berdampak buruk pada kinerja jika Anda juga tidak mempertimbangkan I/O yang didorong ke setiap volume yang Anda pertimbangkan untuk dipindahkan.

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna [Menggunakan CLI NetApp ONTAP](#) Amazon FSx untuk NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

- Gunakan perintah [statistik volume show](#) ONTAP CLI untuk melihat volume lalu lintas tertinggi untuk agregat tertentu, dengan perubahan berikut:

- Ganti *aggregate_name* dengan nama agregat (misalnya, *aggr1*).
- Anda dapat menambahkan `-interval` parameter secara opsional, memberikan interval untuk mengukur (dalam detik) sebelum setiap laporan dikeluarkan. Meningkatkan interval (misalnya, hingga maksimum 300 detik) memberikan sampel jangka panjang untuk jumlah lalu lintas yang didorong ke setiap volume. Defaultnya adalah 5 (detik).

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval [5,300]]
```

Tergantung pada interval yang Anda pilih, dibutuhkan waktu hingga 5 menit untuk menampilkan data. Perintah menunjukkan semua volume dalam agregat, bersama dengan jumlah lalu lintas yang didorong ke setiap agregat.

Volume	Vserver	Aggregate	*Total Ops	Read Ops	Write Ops	Other Ops	Read (Bps)	Write (Bps)	Latency (us)
vol1__0007	svm1	aggr1	4078	4078	0	0	267255808	0	1092
vol1__0005	svm1	aggr1	4078	4078	0	0	267255808	0	1086
vol1__0003	svm1	aggr1	4077	4077	0	0	267223040	0	1086
vol1__0001	svm1	aggr1	4077	4077	0	0	267239424	0	1087
vol1__0008	svm1	aggr2	2314	2314	0	0	151650304	0	1112
vol1__0006	svm1	aggr2	2144	2144	0	0	140509184	0	1104
vol1__0002	svm1	aggr2	2183	2183	0	0	143065088	0	1106
vol1__0004	svm1	aggr2	2183	2183	0	0	143065088	0	1103

Statistik volume ditampilkan berdasarkan per-konstituen (misalnya, *vol1__0015* adalah konstituen ke-15 untuk FlexGroup *vol1*). Anda dapat melihat dari contoh output, konstituen untuk lebih banyak *aggr1* digunakan daripada konstituen untuk *aggr2*. Untuk menyeimbangkan lalu lintas antar agregat, Anda dapat memindahkan volume konstituen antar agregat sehingga lalu lintas lebih merata.

3. Jika Anda telah menambahkan pasangan HA baru, maka Anda harus memindahkan volume yang ada ke agregat baru. Lihat informasi yang lebih lengkap di [Memindahkan volume antar agregat](#).

Mengelola NVMe cache

NVMe Cache diaktifkan secara default pada sistem file generasi kedua Anda. Jika sistem file generasi kedua Anda memiliki beban kerja yang berat, Anda dapat menonaktifkan cache untuk meningkatkan kinerja. NVMe Prosedur berikut menjelaskan cara mengaktifkan, menonaktifkan, dan memvalidasi NVMe cache sistem file Anda.

Untuk mengelola NVMe cache

1. SSH ke dalam sistem ONTAP file Anda. Untuk informasi selengkapnya, lihat [the section called “Menggunakan CLI NetApp ONTAP”](#).

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Gunakan [system node external-cache modify](#) ONTAP CLI command. Pilih **true** untuk mengaktifkan NVMe cache atau **false** menonaktifkannya.

```
::> system node external-cache modify -node * -is-enabled [true|false]
```

3. Gunakan perintah [system node external-cache show](#) ONTAP CLI untuk memeriksa apakah NVMe cache diaktifkan atau dinonaktifkan.

```
::> system node external-cache show -node * -fields is-enabled
```

NVMe Cache diaktifkan atau dinonaktifkan pada basis per-node. Saat Anda menambahkan pasangan ketersediaan tinggi (HA) baru ke sistem file Anda, setiap node baru memiliki perilaku default yang sama dengan node sistem file baru. Oleh karena itu, NVMe cache akan diaktifkan untuk setiap node baru pada sistem file bahkan jika node yang ada menonaktifkannya. Untuk informasi selengkapnya, lihat [Menambahkan pasangan ketersediaan tinggi \(HA\)](#).

Mengelola jenis jaringan

Saat Anda membuat sistem file FSx untuk ONTAP, Anda harus menentukan jenis jaringan, yang harus menjadi salah satu opsi berikut:

- IPv4 memungkinkan sistem file Anda untuk berkomunikasi hanya menggunakan Internet Protocol versi 4 (IPv4).
- Dual-stack memungkinkan sistem file Anda untuk berkomunikasi menggunakan Internet Protocol versi 6 (IPv6) dan IPv4.

Anda dapat mengubah jenis jaringan yang ada FSx untuk sistem file ONTAP kapan saja menggunakan Amazon FSx Management Console, AWS CLI, AWS API, atau salah satu AWS SDKs. Misalnya, jika subnet Anda mendukung keduanya IPv4 dan IPv6 pengalamatan, Anda dapat memperbarui sistem file yang ada dari IPv4 -only ke mode dual-stack, Anda juga dapat memperbarui sistem file dual-stack Anda ke -only. IPv4

Menggunakan mode dual-stack

Anda harus menggunakan mode dual-stack jika Anda perlu mengakses dan mengelola sistem FSx file Amazon Anda secara native dari klien. IPv6 Dengan mengonfigurasi sistem FSx file Amazon untuk menggunakan pengalamatan dual-stack, Anda dapat mengakses data file dari IPv6 klien, serta IPv4 klien, di VPC Amazon yang sama, di VPC lain, atau di jaringan Akun AWS lokal Anda. Misalnya, dengan sistem FSx file Amazon yang dikonfigurasi untuk menggunakan dual-stack, Anda dapat memiliki IPv4 klien yang ada dan IPv6 klien baru yang mengakses data file Anda yang disimpan di sistem file Anda.

Secara default, Amazon FSx dan Amazon VPC menggunakan protokol IPv4 pengalamatan. Jadi sebagai prasyarat untuk menggunakan IPv6, Anda harus terlebih dahulu menetapkan blok IPv6 Classless Inter-Domain Range (CIDR) yang disediakan Amazon ke VPC dan subnet Anda sebelum dapat digunakan dengan sistem file Amazon Anda. IPv6 FSx Untuk informasi tentang mengaktifkan VPC, [lihat IPv6 Menambahkan dukungan IPv6 untuk VPC Anda di Panduan Pengguna](#) Amazon Virtual Private Cloud.

Saat membuat FSx untuk sistem file ONTAP diatur ke mode dual-stack, Anda dapat menentukan rentang IPv6 alamat, selain rentang IPv4 alamat yang ada, di mana titik akhir untuk mengakses sistem file Anda akan dibuat. Secara default, Amazon FSx memilih blok 1024 alamat IP dari salah satu rentang IPv6 CIDR VPC untuk digunakan sebagai rentang IPv6 alamat titik akhir untuk sistem file.

Mengubah jenis jaringan

Anda dapat mengubah jenis jaringan sistem file menggunakan FSx konsol Amazon, AWS Command Line Interface (AWS CLI), atau Amazon FSx API.

Untuk mengubah jenis jaringan sistem file (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Arahkan ke sistem File, dan pilih sistem file ONTAP FSx untuk yang ingin Anda ubah jenis jaringannya.
3. Untuk Tindakan, pilih Perbarui jenis jaringan. Atau, di panel Jaringan & keamanan, pilih Kelola di samping jenis Jaringan sistem file.

Jendela Perbarui jenis jaringan muncul.

4. Untuk jenis jaringan yang diinginkan, pilih salah satu IPv4 atau Dual-stack.
 - Jika Anda memilih IPv4, tidak diperlukan konfigurasi lebih lanjut.
 - Jika Anda memilih Dual-stack, tentukan rentang IPv6 alamat yang akan digunakan titik akhir sistem file Anda:
 - Rentang IPv6 alamat yang tidak dialokasikan dari VPC Anda - FSx Amazon memilih rentang alamat IP /118 yang tersedia dari salah satu rentang CIDR VPC untuk digunakan IPv6 sebagai rentang alamat titik akhir untuk sistem file. IPv6
 - Masukkan rentang IPv6 alamat — Anda dapat memberikan rentang IPv6 CIDR yang Anda pilih sendiri. Rentang alamat IP yang Anda pilih dapat berada di dalam atau di luar rentang alamat IP VPC, asalkan tidak tumpang tindih dengan subnet apa pun.
5. Pilih Perbarui.

Untuk memodifikasi tipe jaringan sistem file (CLI)

- Untuk memodifikasi jenis jaringan sistem file, gunakan perintah [update-file-system](#) CLI (atau operasi [UpdateFileSystem](#) API yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --network-type DUAL
```

Memantau detail sistem file

Anda dapat melihat informasi konfigurasi terperinci untuk sistem file ONTAP Anda FSx menggunakan FSx konsol Amazon AWS CLI, API, dan didukung AWS SDKs.

Untuk melihat informasi sistem file rinci:

- Menggunakan konsol — Pilih sistem file untuk melihat halaman detail sistem File. Panel Ringkasan menunjukkan ID sistem file, status siklus hidup, jenis penerapan, kapasitas penyimpanan SSD, kapasitas throughput, IOPS yang disediakan, Availability Zone, dan waktu pembuatan.

Tab berikut menyediakan informasi konfigurasi terperinci dan pengeditan untuk properti yang dapat dimodifikasi:

- Jaringan & keamanan - Menampilkan informasi administrasi sistem file berikut:
 - VPC Amazon standar
 - Tabel rute Amazon VPC yang terkait dengan sistem file Multi-AZ
 - Jenis jaringan sistem file (IPv4-only atau dual-stack)
 - Titik akhir IPv4 atau rentang IPv6 alamat
 - ID kunci AWS Key Management Service (AWS KMS)
- Pemantauan & kinerja - Menampilkan CloudWatch alarm yang telah Anda buat, serta metrik dan peringatan untuk kategori berikut:
 - Ringkasan — ringkasan tingkat tinggi dari metrik aktivitas sistem file
 - Kapasitas penyimpanan sistem file
 - Server file dan kinerja disk

Untuk informasi selengkapnya, lihat [Pemantauan CloudWatch dengan Amazon](#).

- Administrasi - Menampilkan informasi administrasi sistem file berikut:
 - DNSNama dan IP alamat manajemen sistem file dan titik akhir antar-cluster.
 - Nama pengguna ONTAP administrator.
 - Opsi untuk memperbarui kata sandi ONTAP administrator.
- Daftar sistem file SVMs
- Daftar volume sistem file
- Pengaturan Backup — mengubah pengaturan backup harian otomatis sistem file.
- Pembaruan - menunjukkan status pembaruan yang dimulai pengguna yang dibuat untuk konfigurasi sistem file.
- Tag - lihat, edit, tambahkan, hapus tag Kunci: Pasangan nilai.
- Menggunakan CLI atau API - Gunakan perintah [describe-file-systems](#) CLI atau operasi API.

FSx untuk status sistem file ONTAP

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
AVAILABLE	Sistem file telah berhasil dibuat dan tersedia untuk digunakan.
CREATING	Amazon FSx sedang membuat sistem file baru.
DELETING	Amazon FSx menghapus sistem file yang ada.
SALAH KONFIGURASI	Sistem file berada dalam keadaan salah konfigurasi tetapi dapat dipulihkan.
FAILED	1. Sistem file telah gagal dan Amazon tidak FSx dapat memulihkannya. 2. Saat membuat sistem file baru, Amazon FSx tidak dapat membuat sistem file baru.

Menghapus sistem file

Anda dapat menghapus sistem file FSx untuk ONTAP menggunakan FSx konsol Amazon, FSx API AWS CLI, dan Amazon dan SDKs.

Untuk menghapus sistem file:

- Menggunakan konsol — Ikuti prosedur yang dijelaskan di [Membersihkan sumber daya](#).
- Menggunakan CLI atau API — Pertama hapus semua volume dan SVMs pada sistem file Anda. Kemudian gunakan perintah [delete-file-system](#) CLI atau operasi [DeleteFileSystem](#) API.

Mengelola FSx mesin virtual penyimpanan ONTAP

FSx Untuk ONTAP, volume di-host di server file virtual yang disebut storage virtual machines (SVMs). SVM adalah server file terisolasi dengan kredensi administratifnya sendiri dan titik akhir

untuk mengelola dan mengakses data. Saat Anda mengakses data FSx untuk ONTAP, klien dan workstation Anda memasang volume, berbagi SMB, atau iSCSI LUN yang dihosting oleh SVM menggunakan titik akhir SVM (alamat IP).

Amazon FSx secara otomatis membuat SVM default pada sistem file Anda saat Anda membuat sistem file menggunakan. Konsol Manajemen AWS Anda dapat membuat tambahan SVMs pada sistem file Anda kapan saja menggunakan konsol, AWS CLI, atau Amazon FSx API dan SDKs. Anda tidak dapat membuat SVMs menggunakan ONTAP CLI atau REST API.

Anda dapat bergabung dengan Microsoft Active Directory untuk otentikasi dan otorisasi akses file. SVMs Untuk informasi selengkapnya, lihat [Bekerja dengan Microsoft Active Directory FSx untuk ONTAP](#).

Jumlah maksimum SVMs per sistem file

Tabel berikut mencantumkan jumlah maksimum SVMs yang dapat Anda buat untuk sistem file. [Jumlah maksimum SVMs tergantung pada jumlah kapasitas throughput yang disediakan dalam megabyte per detik \(MBps\), dan juga pada jenis jaringan sistem file.](#)

Pasangan ketersediaan tinggi (HA)	Jumlah kapasitas throughput () MBps	Jumlah maksimum SVMs per sistem file (mode IPv4 -only)	Jumlah maksimum SVMs per sistem file (mode dual-stack)
1 pasangan HA	128	6	6
	256	6	6
	384	6	6
	512	14	11
	768	14	11
	1,024	14	11
	1,536	14	11
	2,048	24	11
	3,072	24	11

Pasangan ketersediaan tinggi (HA)	Jumlah kapasitas throughput () MBps	Jumlah maksimum SVMs per sistem file (mode IPv4 -only)	Jumlah maksimum SVMs per sistem file (mode dual-stack)
	4,096	24	11
	6,144	24	11
2—12 pasangan HA	Setiap	11	11

Topik

- [Membuat mesin virtual penyimpanan \(SVM\)](#)
- [Memperbarui penyimpanan mesin virtual \(SVM\)](#)
- [Mengelola konfigurasi SVM Microsoft Active Directory](#)
- [Mengaudit akses file](#)
- [Menyiapkan server SMB di workgroup](#)
- [Memantau detail konfigurasi mesin virtual penyimpanan \(SVM\)](#)
- [Menghapus penyimpanan mesin virtual \(SVM\)](#)

Membuat mesin virtual penyimpanan (SVM)

Anda dapat membuat FSx untuk ONTAP SVM menggunakan Konsol Manajemen AWS, AWS CLI, dan API.

Jumlah maksimum yang dapat SVMs Anda buat untuk sistem file tergantung pada jenis penyebaran sistem file Anda, jenis jaringan, dan jumlah kapasitas throughput yang disediakan. Untuk informasi selengkapnya, lihat [Jumlah maksimum SVMs per sistem file](#).

Properti SVM

Saat membuat SVM, Anda menentukan properti berikut:

- Sistem file FSx untuk ONTAP yang dimilikinya.
- Konfigurasi Microsoft Active Directory (AD) — Anda dapat secara opsional menggabungkan SVM Anda ke AD yang dikelola sendiri untuk otentikasi dan kontrol akses klien Windows dan macOS. Untuk informasi selengkapnya, lihat [Bekerja dengan Microsoft Active Directory FSx untuk ONTAP](#).

- Gaya keamanan volume root - Atur gaya keamanan volume root (Unix atau NTFS) agar selaras dengan jenis klien yang Anda gunakan untuk mengakses data Anda dalam SVM. Untuk informasi selengkapnya, lihat [Gaya keamanan volume](#).
- Kata sandi administratif SVM — Anda dapat mengatur kata sandi untuk pengguna SVM secara opsional. `vsadmin` Untuk informasi selengkapnya, lihat [Mengelola SVMs dengan ONTAP CLI](#).

Untuk membuat penyimpanan mesin virtual (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Storage virtual machines.
3. Pilih Buat mesin virtual penyimpanan baru.
4. Untuk sistem File, pilih sistem file untuk membuat mesin virtual penyimpanan.
5. Di bidang nama mesin virtual Penyimpanan, berikan nama untuk mesin virtual penyimpanan. Anda dapat menggunakan maksimal 47 karakter alfanumerik, ditambah karakter khusus garis bawah (_).
6. Untuk kata sandi administratif SVM, Anda dapat memilih Tentukan kata sandi dan berikan kata sandi untuk pengguna SVM ini. `vsadmin` Anda dapat menggunakan `vsadmin` pengguna untuk mengelola SVM menggunakan ONTAP CLI atau REST API. Untuk informasi selengkapnya tentang `vsadmin` pengguna, lihat [Mengelola SVMs dengan ONTAP CLI](#).

Jika Anda memilih Jangan tentukan kata sandi (default), Anda masih dapat menggunakan `fsxadmin` pengguna sistem file untuk mengelola sistem file Anda menggunakan ONTAP CLI atau REST API, tetapi Anda tidak dapat menggunakan pengguna SVM Anda untuk melakukan `vsadmin` hal yang sama.

7. Untuk Active Directory, Anda memiliki opsi berikut:
 - Jika Anda tidak bergabung dengan sistem file Anda ke Active Directory (AD), pilih Jangan bergabung dengan Active Directory.
 - Jika Anda bergabung dengan SVM Anda ke domain AD yang dikelola sendiri, pilih Bergabung dengan Direktori Aktif, dan berikan detail berikut untuk iklan Anda. Untuk informasi selengkapnya, lihat [Prasyarat untuk bergabung dengan SVM ke Microsoft AD yang dikelola sendiri](#).
 - Nama NetBIOS dari objek komputer Active Directory yang akan dibuat untuk SVM Anda. Nama NetBIOS tidak boleh melebihi 15 karakter. Ini adalah nama SVM ini di Active Directory.

- Nama domain yang sepenuhnya memenuhi syarat (FQDN) dari Direktori Aktif Anda. FQDN tidak dapat melebihi 255 karakter.
- Alamat IP server DNS — IPv4 atau IPv6 alamat server DNS untuk domain Anda.
- Kredensi akun layanan - Pilih cara memberikan kredensi akun layanan Anda:
 - Opsi 1: AWS Secrets Manager rahasia ARN - Rahasia yang berisi nama pengguna dan kata sandi untuk akun layanan di domain Direktori Aktif Anda. Untuk informasi selengkapnya, lihat [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).
 - Opsi 2: Kredensi Plaintext
 - Nama pengguna akun layanan — Nama pengguna akun layanan di Microsoft Active Directory yang ada. Jangan sertakan awalan atau akhiran domain. Misalnya, untuk EXAMPLE\ADMIN, gunakan saja ADMIN.
 - Kata sandi akun layanan — Kata sandi untuk akun layanan.
 - Konfirmasi kata sandi — Kata sandi untuk akun layanan.
- (Opsional) Unit Organisasi (OU) - Nama jalur yang dibedakan dari unit organisasi tempat Anda ingin bergabung dengan sistem file Anda.
- Grup administrator sistem file yang didelegasikan — Nama grup di AD Anda yang dapat mengelola sistem file Anda.

Jika Anda menggunakan AWS Managed Microsoft AD, Anda harus menentukan grup seperti Administrator AWS Delegasi, FSx Administrator AWS Delegasi, atau grup kustom dengan izin yang didelegasikan ke OU.

Jika Anda bergabung dengan iklan yang dikelola sendiri, gunakan nama grup di iklan Anda. Grup default adalah Domain Admins.

8. Untuk gaya keamanan volume root SVM, pilih gaya keamanan untuk SVM tergantung pada jenis klien yang mengakses data Anda. Pilih Unix (Linux) jika Anda terutama mengakses data Anda menggunakan klien Linux; pilih NTFS jika Anda terutama mengakses data Anda menggunakan klien Windows. Untuk informasi selengkapnya, lihat [Gaya keamanan volume](#).
9. Pilih Konfirmasi untuk membuat mesin virtual penyimpanan.

Anda dapat memantau kemajuan pembaruan pada halaman detail sistem file, di kolom Status panel mesin virtual Penyimpanan. Mesin virtual penyimpanan siap digunakan saat statusnya Dibuat.

Untuk membuat mesin virtual penyimpanan (CLI)

- FSx Untuk membuat mesin virtual penyimpanan ONTAP (SVM), gunakan perintah [create-storage-virtual-machine](#) CLI (atau operasi [CreateStorageVirtualMachine](#) API yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx create-storage-virtual-machine \
  --file-system-id fs-0123456789abcdef0 \
  --name svm1 \
  --svm-admin-password password \
  --active-directory-configuration
SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
\
UserName="FSxService",Password="password", \
  DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Setelah berhasil membuat mesin virtual penyimpanan, Amazon FSx mengembalikan deskripsinya dalam format JSON, seperti yang ditunjukkan pada contoh berikut.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddresses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddresses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddresses": ["198.19.0.5", "198.19.0.6"]
      }
    }
  }
}
```

```

    "Iscsi": {
      "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
      "IpAddresses": ["198.19.0.7", "198.19.0.8"]
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}

```

Memperbarui penyimpanan mesin virtual (SVM)

Anda dapat memperbarui properti konfigurasi mesin virtual penyimpanan (SVM) berikut menggunakan FSx konsol Amazon AWS CLI, dan Amazon FSx API:

- Kata sandi akun administratif SVM.
- Konfigurasi SVM Active Directory (AD) — Anda dapat menggabungkan SVM ke AD, atau memodifikasi konfigurasi AD dari SVM yang sudah bergabung dengan AD. Untuk informasi selengkapnya, lihat [Mengelola konfigurasi SVM Microsoft Active Directory](#).

Untuk memperbarui kredensi akun administrator SVM (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Pilih SVM yang akan diperbarui sebagai berikut:
 - Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file ONTAP yang ingin Anda perbarui SVM.
 - Pilih tab Storage Virtual Machines.

—Atau—

 - Untuk menampilkan daftar semua yang SVMs tersedia Akun AWS di Anda saat ini Wilayah AWS, perluas ONTAP dan pilih Storage mesin virtual.
3. Pilih mesin virtual penyimpanan yang ingin Anda perbarui.
4. Pilih Tindakan > Perbarui kata sandi administrator. Jendela Perbarui kredensi administratif SVM muncul.
5. Masukkan kata sandi baru untuk vsadmin pengguna, dan konfirmasi.
6. Pilih Perbarui kredensi untuk menyimpan kata sandi baru.

Untuk memperbarui kredensi akun administrator SVM (CLI)

- Untuk memperbarui konfigurasi FSx untuk ONTAP SVM, gunakan perintah [update-storage-virtual-machine](#) CLI (atau operasi [UpdateStorageVirtualMachine](#) API yang setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

Setelah berhasil membuat mesin virtual penyimpanan, Amazon FSx mengembalikan deskripsinya dalam format JSON, seperti yang ditunjukkan pada contoh berikut.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
```

```

    "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
    "IpAddresses": ["198.19.0.4"]
  },
  "Nfs": {
    "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
    "IpAddresses": ["198.19.0.4"]
  },
  "Smb": {
    "DnsName": "amznfsx12345",
    "IpAddresses": ["198.19.0.4"]
  },
  "SmbWindowsInterVpc": {
    "IpAddresses": ["198.19.0.5", "198.19.0.6"]
  },
  "Iscsi": {
    "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
    "IpAddresses": ["198.19.0.7", "198.19.0.8"]
  }
},
"FileSystemId": "fs-0123456789abcdef0",
"Lifecycle": "CREATING",
"Name": "vol1",
"ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
"StorageVirtualMachineId": "svm-abcdef01234567890",
"Subtype": "default",
"Tags": [],
"ActiveDirectoryConfiguration": {
  "NetBiosName": "amznfsx12345",
  "SelfManagedActiveDirectoryConfiguration": {
    "UserName": "Admin",
    "DnsIps": [
      "10.0.1.3",
      "10.0.91.97"
    ],
    "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
    "DomainName": "customer-ad.example.com"
  }
}
}
}

```

}

Mengelola konfigurasi SVM Microsoft Active Directory

Anda dapat menggabungkan SVM ke Microsoft Active Directory atau memodifikasi konfigurasi Microsoft Active Directory dari SVM yang sudah bergabung dengan Microsoft Active Directory. FSx untuk ONTAP terintegrasi dengan AWS Secrets Manager untuk mengelola kredensial akun layanan bergabung domain Anda dengan aman.

Untuk memperbarui konfigurasi SVM Microsoft Active Directory (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Pilih SVM yang akan diperbarui sebagai berikut:
 - Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem ONTAP file yang ingin Anda perbarui SVM.
 - Pilih tab Storage Virtual Machines.

—Atau—

 - Untuk menampilkan daftar semua yang SVMs tersedia Akun AWS di Anda saat ini Wilayah AWS, perluas ONTAP dan pilih Storage mesin virtual.
3. Pilih mesin virtual penyimpanan yang ingin Anda perbarui.
4. Pilih Tindakan > Perbarui konfigurasi Microsoft Active Directory. Jendela konfigurasi Perbarui Microsoft Active Directory muncul.
5. Untuk kredensial akun layanan bergabung dengan Domain, pilih Dikelola di Secrets Manager (disarankan) untuk menggunakan Secrets Manager untuk pengelolaan kredensial yang aman.

Note

Menggunakan Secrets Manager menghilangkan kebutuhan untuk menyimpan kredensial teks biasa dan menyediakan manajemen kredensial terpusat. Untuk informasi selengkapnya, lihat [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).

6. Untuk Rahasia, pilih rahasia yang ada dari Secrets Manager yang berisi kredensial akun layanan bergabung domain Anda yang diperbarui, atau pilih Buat rahasia baru untuk membuatnya.

7. Perbarui bidang konfigurasi Microsoft Active Directory lainnya sesuai kebutuhan untuk lingkungan Anda.
8. Pilih Perbarui konfigurasi untuk menyimpan perubahan.

Untuk memperbarui konfigurasi SVM Microsoft Active Directory (CLI)

- Untuk memperbarui konfigurasi Microsoft Active Directory FSx untuk ONTAP SVM, gunakan perintah [update-storage-virtual-machine](#) CLI dengan `--active-directory-configuration` parameter, seperti yang ditunjukkan pada contoh berikut.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--active-directory-configuration DomainJoinServiceAccountSecret=secret-arn
```

Mengaudit akses file

Amazon FSx untuk NetApp ONTAP mendukung audit akses pengguna akhir ke file dan direktori di mesin virtual penyimpanan (SVM).

Topik

- [Gambaran umum audit akses file](#)
- [Ikhtisar tugas untuk mengatur audit akses file](#)

Gambaran umum audit akses file

Audit akses file memungkinkan Anda merekam akses pengguna akhir dari masing-masing file dan direktori berdasarkan kebijakan audit yang Anda tentukan. Audit akses file dapat membantu Anda meningkatkan keamanan sistem Anda dan mengurangi risiko akses tidak sah ke data sistem Anda. Audit akses file membantu organisasi Anda tetap mematuhi persyaratan perlindungan data, mengidentifikasi potensi ancaman sejak dini, dan mengurangi risiko pelanggaran data.

Di seluruh akses file dan direktori, Amazon FSx mendukung pencatatan upaya yang berhasil (seperti pengguna dengan izin yang cukup berhasil mengakses file), upaya gagal, atau keduanya. Anda juga dapat menonaktifkan audit akses file kapan saja.

Secara default, log peristiwa audit disimpan dalam format EVT file, yang memungkinkan Anda melihatnya menggunakan Microsoft Event Viewer.

Acara akses SMB yang dapat diaudit

Tabel berikut mencantumkan file SMB dan peristiwa akses folder dapat diaudit.

ID Acara (EVT/EVTX)	Peristiwa	Deskripsi	Kategori
560/4656	Buka Objek/Buat Objek	OBJECT ACCESS: Objek (file atau direktori) terbuka	Akses Berkas
563/4659	Buka Object dengan Intent to Delete	AKSES OBJEK: Pegangan ke objek (file atau direktori) diminta dengan Intent to Delete	Akses Berkas
564/4660	Hapus Objek	AKSES OBJEK: Hapus Objek (file atau direktori). ONTAP menghasilkan acara ini ketika klien Windows mencoba menghapus objek (file atau direktori)	Akses Berkas
567/4663	Baca Atribut Object/Write Object/Get Object Attributes/Set Objek	AKSES OBJEK: Upaya akses objek (baca, tulis, dapatkan atribut, atur atribut).  Note Untuk acara ini, ONTAP hanya mengaudit operasi baca SMB pertama	Akses Berkas

ID Acara (EVT/EVTX)	Peristiwa	Deskripsi	Kategori
		dan SMB tulis pertama (sukses atau gagal) pada suatu objek. Ini mencegah ONTAP membuat entri log yang berlebihan ketika satu klien membuka objek dan melakukan banyak operasi baca atau tulis berturut-turut ke objek yang sama.	
N/A/4664	Tautan keras	OBJECT ACCESS: Upaya dibuat untuk membuat hard link	Akses Berkas
ID Acara N/A/N/A ONTAP 9999	Ganti Nama Objek	OBJECT ACCESS: Object berganti nama. Ini adalah acara ONTAP. Saat ini tidak didukung oleh Windows sebagai satu acara.	Akses Berkas

ID Acara (EVT/EVTX)	Peristiwa	Deskripsi	Kategori
ID Acara N/A/N/A ONTAP 9998	Putuskan Tautan Objek	OBJECT ACCESS: Objek tidak ditautkan . Ini adalah acara ONTAP. Saat ini tidak didukung oleh Windows sebagai satu acara.	Akses Berkas

Acara akses NFS yang dapat diaudit

Peristiwa akses file dan folder NFS berikut dapat diaudit.

- MEMBACA
- BUKA
- TUTUP
- READDIR
- MENULIS
- SETATTR
- CREATE
- PRANALA
- OPENATTR
- REMOVE (HAPUS)
- GETATTR
- MEMVERIFIKASI
- NVERIFIKASI
- GANTI NAMA

Ikhtisar tugas untuk mengatur audit akses file

FSx Menyiapkan ONTAP untuk audit akses file melibatkan tugas-tugas tingkat tinggi berikut:

1. [Biasakan diri Anda](#) dengan persyaratan dan pertimbangan audit akses file.

2. [Buat konfigurasi audit](#) pada SVM tertentu.
3. [Aktifkan audit](#) pada SVM itu.
4. [Konfigurasi kebijakan audit](#) pada file dan direktori Anda.
5. [Lihat log peristiwa audit](#) setelah ONTAP FSx memancarkannya.

Rincian tugas disediakan dalam prosedur berikut.

Ulangi tugas untuk SVM lain di sistem file Anda yang ingin Anda aktifkan audit akses file.

Persyaratan audit

Sebelum Anda mengonfigurasi dan mengaktifkan audit pada SVM, Anda harus mengetahui persyaratan dan pertimbangan berikut.

- Audit NFS mendukung audit Access Control Entries (ACEs) yang ditetapkan sebagai tipeu, yang menghasilkan entri log audit saat akses dicoba pada objek. Untuk audit NFS, tidak ada pemetaan antara bit mode dan audit. ACEs Saat mengonversi ACLs ke bit mode, audit ACEs dilewati. Saat mengonversi bit mode ke ACLs, audit tidak ACEs dihasilkan.
- Audit tergantung pada memiliki ruang yang tersedia dalam volume pementasan. (Volume pementasan adalah volume khusus yang dibuat oleh ONTAP untuk menyimpan file pementasan, yang merupakan file biner perantara pada node individu di mana catatan audit disimpan sebelum konversi ke format file EVTX atau XML.) Anda harus memastikan bahwa ada ruang yang cukup untuk volume pementasan dalam agregat yang berisi volume yang diaudit.
- Audit tergantung pada memiliki ruang yang tersedia dalam volume yang berisi direktori tempat log peristiwa audit yang dikonversi disimpan. Anda harus memastikan bahwa ada cukup ruang dalam volume yang digunakan untuk menyimpan log peristiwa. Anda dapat menentukan jumlah log audit yang akan disimpan di direktori audit dengan menggunakan `-rotate-limit` parameter saat membuat konfigurasi audit, yang dapat membantu memastikan bahwa ada cukup ruang yang tersedia untuk log audit dalam volume.

Membuat konfigurasi audit pada SVMs

Sebelum Anda dapat mulai mengaudit peristiwa file dan direktori, Anda harus membuat konfigurasi audit pada Storage Virtual Machine (SVM). Setelah Anda membuat konfigurasi audit, Anda harus mengaktifkannya di SVM.

Sebelum Anda menggunakan `vserver audit create` perintah untuk membuat konfigurasi audit, pastikan Anda telah membuat direktori untuk digunakan sebagai tujuan untuk log, dan direktori tidak memiliki symlink. Anda menentukan direktori tujuan dengan `-destination` parameter.

Anda dapat membuat konfigurasi audit yang memutar log audit berdasarkan ukuran log atau jadwal, sebagai berikut:

- Untuk memutar log audit berdasarkan ukuran log, gunakan perintah ini:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

Contoh berikut membuat konfigurasi audit untuk SVM bernama `svm1` yang mengaudit operasi file dan peristiwa logon dan logoff CIFS (SMB) (default) menggunakan rotasi berbasis ukuran. Format log adalah EVTX (default), log disimpan dalam `/audit_log` direktori, dan Anda akan memiliki satu file log pada satu waktu (hingga 200MB dalam ukuran).

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- Untuk memutar log audit berdasarkan jadwal, gunakan perintah ini:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]  
[-rotate-limit integer] [-rotate-schedule-month chron_month]  
[-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-  
day chron_dayofmonth]  
[-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

`-rotate-schedule-minute` Parameter diperlukan jika Anda mengonfigurasi rotasi log audit berbasis waktu.

Contoh berikut membuat konfigurasi audit untuk SVM bernama `svm2` menggunakan rotasi berbasis waktu. Format log adalah EVTX (default) dan log audit diputar setiap bulan, pada pukul 12:30 pada semua hari dalam seminggu.

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB -  
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -  
rotate-schedule-minute 30
```

Anda dapat menggunakan `-format` parameter untuk menentukan apakah log audit dibuat dalam EVTX format yang dikonversi (default) atau dalam format XML file. EVTXFormat ini memungkinkan Anda untuk melihat file log dengan Microsoft Event Viewer.

Secara default, kategori peristiwa yang akan diaudit adalah peristiwa akses file (baik SMB dan NFS), peristiwa logon dan logoff CIFS (SMB), dan peristiwa perubahan kebijakan otorisasi. Anda dapat memiliki kontrol yang lebih besar atas peristiwa mana yang akan dicatat oleh `-events` parameter, yang memiliki format berikut:

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-account|authorization-policy-change|security-group}
```

Misalnya, menggunakan `-events file-share` mengaktifkan audit peristiwa berbagi file.

Untuk informasi selengkapnya tentang `vserver audit create` perintah, lihat [Membuat konfigurasi audit](#).

Mengaktifkan audit pada SVM

Setelah Anda selesai menyiapkan konfigurasi audit, Anda harus mengaktifkan audit pada SVM. Untuk melakukannya, gunakan perintah berikut:

```
vserver audit enable -vserver svm_name
```

Misalnya, gunakan perintah berikut untuk mengaktifkan audit pada SVM bernama. `svm1`

```
vserver audit enable -vserver svm1
```

Anda dapat menonaktifkan audit akses kapan saja. Misalnya, gunakan perintah berikut untuk mematikan audit pada SVM bernama. `svm4`

```
vserver audit disable -vserver svm4
```

Saat Anda menonaktifkan audit, konfigurasi audit tidak akan dihapus di SVM, yang berarti Anda dapat mengaktifkan kembali audit pada SVM tersebut kapan saja.

Mengkonfigurasi kebijakan audit file dan folder

Anda perlu mengonfigurasi kebijakan audit pada file dan folder yang ingin diaudit untuk upaya akses pengguna. Anda dapat mengonfigurasi kebijakan audit untuk memantau upaya akses yang berhasil dan gagal.

Anda dapat mengonfigurasi kebijakan audit SMB dan NFS. Kebijakan audit SMB dan NFS memiliki persyaratan konfigurasi dan kemampuan audit yang berbeda berdasarkan gaya keamanan volume.

Kebijakan audit pada file dan direktori gaya keamanan NTFS

Anda dapat mengonfigurasi kebijakan audit NTFS dengan menggunakan tab Keamanan Windows atau CLI ONTAP.

Untuk mengkonfigurasi kebijakan audit NTFS (tab Keamanan Windows)

Anda mengonfigurasi kebijakan audit NTFS dengan menambahkan entri ke NTFS SACLs yang terkait dengan deskriptor keamanan NTFS. Deskriptor keamanan kemudian diterapkan ke file dan direktori NTFS. Tugas-tugas ini secara otomatis ditangani oleh GUI Windows. Deskriptor keamanan dapat berisi daftar kontrol akses diskresioner (DACLS) untuk menerapkan izin akses file dan folder, SACLs untuk audit file dan folder, atau keduanya dan. SACLs DACLS

1. Dari menu Tools di Windows Explorer, pilih Map network drive.
2. Lengkapi kotak Map Network Drive:
 - a. Pilih huruf Drive.
 - b. Di kotak Folder, ketik nama server SMB (CIFS) yang berisi share, memegang data yang ingin Anda audit dan nama share.
 - c. Pilih Selesai.

Drive yang Anda pilih sudah terpasang dan siap dengan jendela Windows Explorer yang menampilkan file dan folder yang terdapat dalam share.

3. Pilih file atau direktori yang ingin Anda aktifkan akses auditing.
4. Klik kanan file atau direktori, lalu pilih Properties.
5. Pilih tab Security.
6. Klik Advanced.
7. Pilih tab Audit.

8. Lakukan tindakan yang diinginkan:

Jika Anda ingin...	Lakukan hal berikut
Menyiapkan audit untuk pengguna atau grup baru	1. Pilih Tambahkan. 2. Dalam kotak Masukkan nama objek untuk dipilih, ketikkan nama pengguna atau grup yang ingin Anda tambahkan. 3. Pilih OK.
Menghapus audit dari pengguna atau grup	1. Di kotak Masukkan nama objek untuk dipilih, pilih pengguna atau grup yang ingin Anda hapus. 2. Pilih Hapus. 3. Pilih OK. 4. Lewati sisa prosedur ini.
Mengubah audit untuk pengguna atau grup	1. Di kotak Masukkan nama objek untuk dipilih, pilih pengguna atau grup yang ingin Anda ubah. 2. Pilih Edit. 3. Pilih OK.

Jika Anda menyiapkan audit pada pengguna atau grup atau mengubah audit pada pengguna atau grup yang ada, kotak Entri Audit untuk **object** terbuka.

9. Di kotak Terapkan ke, pilih cara Anda ingin menerapkan entri audit ini.

Jika Anda menyiapkan audit pada satu file, kotak Terapkan ke tidak aktif, karena defaultnya hanya untuk objek ini.

10. Di kotak Akses, pilih apa yang ingin diaudit dan apakah Anda ingin mengaudit peristiwa yang berhasil, peristiwa kegagalan, atau keduanya.

- Untuk mengaudit peristiwa yang berhasil, pilih kotak Sukses.
- Untuk mengaudit peristiwa kegagalan, pilih kotak Kegagalan.

Pilih tindakan yang perlu Anda pantau untuk memenuhi persyaratan keamanan Anda. Untuk informasi selengkapnya tentang peristiwa yang dapat diaudit ini, lihat dokumentasi Windows Anda. Anda dapat mengaudit peristiwa berikut:

- Kontrol penuh
 - Melintasi folder/jalankan file
 - Daftar folder/baca data
 - Baca atribut
 - Baca atribut yang diperluas
 - Buat file/tulis data
 - Buat folder/tambahkan data
 - Tulis atribut
 - Tulis atribut yang diperluas
 - Hapus subfolder dan file
 - Hapus
 - Baca izin
 - Ubah izin
 - Ambil kepemilikan
11. Jika Anda tidak ingin setelan audit menyebar ke file dan folder berikutnya dari wadah asli, pilih kotak Terapkan entri audit ini ke objek dan/atau wadah dalam wadah ini saja.
12. Pilih Terapkan.
13. Setelah selesai menambahkan, menghapus, atau mengedit entri audit, pilih OK.

Entri Audit untuk **object** kotak ditutup.

14. Di kotak Audit, pilih pengaturan warisan untuk folder ini. Pilih hanya level minimal yang menyediakan acara audit yang memenuhi persyaratan keamanan Anda.

Anda dapat memilih salah satu dari yang berikut ini:

- Pilih kotak Sertakan entri audit yang dapat diwariskan dari kotak induk objek ini.
- Pilih kotak Ganti semua entri audit warisan yang ada pada semua turunan dengan entri audit yang dapat diwariskan dari objek ini.
- Pilih kedua kotak.
- Pilih kotak mana pun.

Jika Anda menyetel SACLs pada satu file, kotak Ganti semua entri audit warisan yang ada pada semua turunan dengan entri audit yang dapat diwariskan dari objek ini tidak ada di kotak Audit.

15. Pilih OK.

Untuk mengonfigurasi kebijakan audit NTFS (ONTAP CLI)

Dengan menggunakan CLI ONTAP, Anda dapat mengonfigurasi kebijakan audit NTFS tanpa perlu terhubung ke data menggunakan berbagi SMB pada klien Windows.

- Anda dapat mengonfigurasi kebijakan audit NTFS dengan menggunakan keluarga perintah [direktori file keamanan vservers ntfs sacl add](#).

Misalnya, perintah berikut membuat kebijakan keamanan yang p1 dinamai SVM bernama vs0.

```
vservers security file-directory policy create -policy-name p1 -vservers vs0
```

Kemudian, perintah berikut menerapkan kebijakan p1 keamanan ke vs0 SVM.

```
vservers security file-directory apply -vservers vs0 -policy-name p1
```

Kebijakan audit pada file dan direktori gaya keamanan UNIX

Anda mengonfigurasi audit untuk file dan direktori bergaya keamanan UNIX dengan menambahkan audit ACEs (ekspresi kontrol akses) ke NFS v4.x (daftar kontrol akses). ACLs ini memungkinkan Anda untuk memantau peristiwa akses file dan direktori NFS tertentu untuk tujuan keamanan.

Note

Untuk NFS v4.x, baik diskresioner dan sistem disimpan dalam ACL ACEs yang sama. Oleh karena itu, Anda harus berhati-hati saat menambahkan audit ACEs ke ACL yang ada untuk menghindari penimpaan dan kehilangan ACL yang ada. Urutan di mana Anda menambahkan audit ACEs ke ACL yang ada tidak masalah.

Untuk mengonfigurasi kebijakan audit UNIX

1. Ambil ACL yang ada untuk file atau direktori dengan menggunakan perintah `nfs4_getfacl` atau setara.
2. Tambahkan audit ACEs yang diinginkan.
3. Terapkan ACL yang diperbarui ke file atau direktori dengan menggunakan perintah `nfs4_setfacl` atau setara.

Contoh ini menggunakan `-a` opsi untuk memberikan izin baca pengguna (bernamatestuser) ke file bernamafile1.

```
nfs4_setfacl -a "A::testuser@example.com:R" file1
```

Melihat log peristiwa audit

Anda dapat melihat log peristiwa audit yang disimpan dalam format XML file EVTX atau.

- EVTXformat file - Anda dapat membuka log peristiwa EVTX audit yang dikonversi sebagai file yang disimpan menggunakan Microsoft Event Viewer.

Ada dua opsi yang dapat Anda gunakan saat melihat log peristiwa menggunakan Event Viewer:

- Tampilan umum: Informasi yang umum untuk semua peristiwa ditampilkan untuk catatan acara. Data khusus peristiwa untuk catatan peristiwa tidak ditampilkan. Anda dapat menggunakan tampilan detail untuk menampilkan data khusus acara.
- Tampilan detil: Tampilan ramah dan tampilan XHTML tersedia. Tampilan ramah dan tampilan XHTML menampilkan informasi yang umum untuk semua peristiwa dan data khusus peristiwa untuk catatan peristiwa.
- XMLformat file - Anda dapat melihat dan memproses log peristiwa audit XMLpada aplikasi pihak ketiga yang mendukung format file XML. Alat tampilan XHTML dapat digunakan untuk melihat log audit asalkan Anda memiliki skema XHTML dan informasi tentang definisi untuk bidang XHTML.

Menyiapkan server SMB di workgroup

Anda dapat mengonfigurasi server Blok Pesan Server (SMB) di workgroup sebagai alternatif untuk menggabungkan [SVM ke Microsoft Active Directory](#) ketika infrastruktur domain Microsoft Active

Directory tidak tersedia. Workgroup adalah peer-to-peer jaringan yang menggunakan protokol SMB, dan hanya memiliki akun dan grup lokal.

Proses pengaturan server SMB sebagai anggota dalam workgroup terdiri dari yang berikut:

- Membuat server SMB pada mesin virtual penyimpanan (SVM).
- Membuat pengguna dan grup lokal.
- Menambahkan pengguna atau grup lokal sebagai anggota workgroup.

Perlu diingat bahwa server SMB dalam mode workgroup tidak mendukung fitur SMB berikut:

- SMB3 Protokol saksi
- SMB3 Saham CA
- SQL melalui SMB
- Pengalihan Folder
- Profil Roaming
- Objek Kebijakan Grup (GPO)
- Layanan Snapshot Volume (VSS)

Juga, server SMB dalam mode workgroup hanya mendukung otentikasi NTLM dan tidak mendukung otentikasi Kerberos.

Prosedur berikut membawa Anda melalui proses menyiapkan server SMB di SVM di workgroup, membuat akun lokal, dan menambahkan akun ini ke keanggotaan workgroup. Anda akan menggunakan NetApp ONTAP CLI dari sistem file atau antarmuka manajemen SVM untuk menerapkan prosedur ini. Untuk informasi selengkapnya, lihat [Menggunakan CLI NetApp ONTAP](#).

Topik

- [Membuat server SMB di workgroup](#)
- [Membuat akun pengguna lokal di server SMB](#)
- [Membuat grup lokal di server SMB](#)
- [Menambahkan pengguna lokal ke grup lokal](#)

Membuat server SMB di workgroup

Anda dapat menggunakan [vserver cifs create](#) ONTAP CLI perintah untuk membuat server SMB di SVM dan menentukan workgroup yang menjadi miliknya.

Sebelum Anda mulai

SVM dan volume (dan antarmuka) yang Anda gunakan untuk melayani data harus telah dikonfigurasi untuk memungkinkan protokol SMB.

LIFs Harus dapat terhubung ke server DNS yang dikonfigurasi pada SVM. Lisensi CIFS mungkin diperlukan pada sistem file, namun lisensi CIFS tidak diperlukan jika server SMB akan digunakan untuk otentikasi saja.

Untuk membuat server SMB di workgroup

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Buat server SMB di workgroup:

```
FSxIdabcde123456::> vserver cifs create -vserver vserver_name -cifs-server cifs_server_name -workgroup workgroup_name [-comment workgroup_description]
```

Perintah berikut membuat server SMB smb_server01 di workgroup01 workgroup:

```
FSxIdabcde123456::> vserver cifs create -vserver svm1 -cifs-server SMB_SERVER01 -workgroup workgroup01
```

Jika Anda terhubung ke port manajemen SVM, Anda tidak perlu menentukan. -vserver

3. Verifikasi konfigurasi server SMB dengan menggunakan `vserver cifs show` perintah.

Dalam contoh berikut, output perintah menunjukkan bahwa server SMB bernama smb_server01 dibuat pada SVM svm1 di workgroup: workgroup01

```
FSxIdabcde123456:~> vserver cifs show -vserver svm1
```

```

                                Vserver: svm1
                        CIFS Server NetBIOS Name: SMB_SERVER01
NetBIOS Domain/Workgroup Name: workgroup01
                Fully Qualified Domain Name: -
                        Organizational Unit: -
Default Site Used by LIFs Without Site Membership: -
                        Workgroup Name: workgroup01
                        Authentication Style: workgroup
CIFS Server Administrative Status: up
                        CIFS Server Description:
                        List of NetBIOS Aliases: -

```

Membuat akun pengguna lokal di server SMB

Anda dapat membuat akun pengguna lokal yang dapat digunakan untuk mengotorisasi akses ke data yang terdapat dalam SVM melalui koneksi SMB. Anda juga dapat menggunakan akun pengguna lokal untuk otentikasi saat membuat sesi SMB. Fungsionalitas pengguna lokal diaktifkan secara default saat SVM dibuat. Saat Anda membuat akun pengguna lokal, Anda harus menentukan nama pengguna dan Anda harus menentukan SVM yang dapat digunakan untuk mengaitkan akun tersebut.

Untuk membuat akun pengguna lokal di server SMB

1. Buat pengguna lokal menggunakan perintah [vserver cifs users-and-groups local-user create](#) ONTAP CLI:

```
vserver cifs users-and-groups local-user create -vserver svm_name -user-  
name user_name optional_parameters
```

Parameter opsional berikut mungkin berguna:

- `-full-name` Nama lengkap pengguna.
- `-description`— Deskripsi untuk pengguna lokal.
- `-is-account-disabled {true|false}`— Menentukan apakah akun pengguna diaktifkan atau dinonaktifkan. Jika parameter ini tidak ditentukan, defaultnya adalah mengaktifkan akun pengguna.

Perintah meminta kata sandi pengguna lokal.

2. Masukkan kata sandi untuk pengguna lokal, lalu konfirmasi kata sandi.
3. Verifikasi bahwa pengguna berhasil dibuat:

```
vserver cifs users-and-groups local-user show -vserver svm_name
```

Contoh berikut membuat pengguna lokal SMB_SERVER01\sue, dengan nama lengkap Sue Chang, terkait dengan SVM svm1:

```
FSxIdabcde123456:> vserver cifs users-and-groups local-user create -vserver svm1  
-user-name SMB_SERVER01\sue -full-name "Sue Chang"
```

```
Enter the password:  
Confirm the password:
```

```
FSxIdabcde123456:> vserver cifs users-and-groups local-user show
```

Vserver	User Name	Full Name	Description
svm1	SMB_SERVER01\Administrator		Built-in administrator account
svm1	SMB_SERVER01\sue	Sue Chang	

Membuat grup lokal di server SMB

Anda dapat membuat grup lokal yang dapat digunakan untuk mengotorisasi akses ke data yang terkait dengan SVM melalui koneksi SMB. Anda juga dapat menetapkan hak istimewa yang menentukan hak atau kemampuan pengguna apa yang dimiliki anggota grup.

Fungsionalitas grup lokal diaktifkan secara default saat SVM dibuat. Saat Anda membuat grup lokal, Anda harus menentukan nama untuk grup tersebut dan Anda harus menentukan SVM yang dapat digunakan untuk mengaitkan grup tersebut. Anda dapat menentukan nama grup dengan atau tanpa nama domain lokal, dan Anda dapat menentukan deskripsi untuk grup lokal secara opsional. Anda tidak dapat menambahkan grup lokal ke grup lokal lain.

Untuk membuat grup lokal di server SMB

1. buat grup lokal menggunakan perintah [vserver cifs users-and-groups local-group create](#) ONTAP CLI.

```
vserver cifs users-and-groups local-group create -vserver svm_name -group-  
name group_name [-description local_group_description]
```

Menyertakan deskripsi untuk grup lokal berguna.

2. Verifikasi bahwa grup telah berhasil dibuat:

```
vserver cifs users-and-groups local-group show -vserver svm_name
```

Contoh berikut membuat grup lokal yang SMB_SERVER01\engineering terkait dengan SVMsvm1:

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group create -vserver svm1 -  
group-name SMB_SERVER01\engineering
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group show -vserver svm1
```

Vserver	Group Name	Description
svm1	BUILTIN\Administrators	Built-in Administrators group
svm1	BUILTIN\Backup Operators	Backup Operators group
svm1	BUILTIN\Guests	Built-in Guests group
svm1	BUILTIN\Power Users	Restricted administrative privileges
svm1	BUILTIN\Users	All users
svm1	SMB_SERVER01\engineering	

Menambahkan pengguna lokal ke grup lokal

Anda dapat mengelola keanggotaan grup lokal dengan menambahkan dan menghapus pengguna lokal atau domain, atau menambahkan dan menghapus grup domain. Ini berguna jika Anda ingin mengontrol akses ke data berdasarkan kontrol akses yang ditempatkan pada grup, atau jika Anda ingin pengguna memiliki hak istimewa yang terkait dengan grup tersebut. Jika Anda tidak lagi ingin pengguna lokal, pengguna domain, atau grup domain memiliki hak akses atau hak istimewa berdasarkan keanggotaan dalam grup, Anda dapat menghapus anggota dari grup.

Saat menambahkan anggota ke grup lokal, ingatlah hal berikut:

- Anda tidak dapat menambahkan pengguna ke grup Semua Orang khusus.
- Anda tidak dapat menambahkan grup lokal ke grup lokal lain.

- Untuk menambahkan pengguna domain atau grup ke grup lokal, ONTAP harus dapat menyelesaikan nama ke SID.

Saat menghapus anggota dari grup lokal, ingatlah hal berikut:

- Anda tidak dapat menghapus anggota dari grup Everyone khusus.
- Untuk menghapus anggota dari grup lokal, ONTAP harus dapat menyelesaikan nama mereka ke SID.

Anda harus memiliki `fsxadmin` peran untuk menjalankan perintah yang digunakan dalam prosedur ini. Untuk informasi selengkapnya, lihat [ONTAP peran dan pengguna](#).

Untuk mengelola keanggotaan grup lokal

- Tambahkan anggota ke atau hapus anggota dari grup menggunakan perintah CLI [hapus ONTAP anggota users-and-groups grup lokal vservers cifs users-and-groups local-group add-members dan vservers cifs](#).
- Untuk menambahkan anggota ke workgroup:

```
vserver cifs users-and-groups local-group add-members -vserver svm_name -group-name group_name -member-names name[,...]
```

Anda dapat menentukan daftar pengguna lokal, pengguna domain, atau grup domain yang dibatasi koma untuk ditambahkan ke grup lokal yang ditentukan.

- Untuk melihat anggota workgroup:

```
vserver cifs users-and-groups local-group show-members -vserver svm_name -group-name group_name
```

- Untuk menghapus anggota dari grup kerja:

```
vserver cifs users-and-groups local-group remove-members -vserver svm_name -group-name group_name -member-names name[,...]
```

Anda dapat menentukan daftar pengguna lokal, pengguna domain, atau grup domain yang dibatasi koma untuk dihapus dari grup lokal yang ditentukan.

Contoh berikut menambahkan pengguna lokal SMB_SERVER01\sue ke grup lokal SMB_SERVER01\engineering di SVMsvm1:

```
FSxIdabcde123456::> vservers cifs users-and-groups local-group add-members -vservers svm1
-group-name SMB_SERVER01\engineering -member-names SMB_SERVER01\sue
```

Contoh berikut menghapus pengguna lokal SMB_SERVER01\sue dan SMB_SERVER01\james dari grup lokal SMB_SERVER01\engineering di SVMsvm1:

```
FSxIdabcde123456::> vservers cifs users-and-groups local-group remove-
members -vservers svm1 -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue,SMB_SERVER01\james
```

Contoh berikut mencantumkan anggota grup lokal SMB_SERVER01\engineering:

```
FSxIdabcde123456::> vservers cifs users-and-groups local-group show-members -
vservers svm_name -group-name group_name
```

```
Vserver: svm1
Domain Name: SMB_SERVER01
Group Name: SMB_SERVER01\engineering
Member Name: SMB_SERVER01\anita
              SMB_SERVER01\james
              SMB_SERVER01\liang
```

Memantau detail konfigurasi mesin virtual penyimpanan (SVM)

Anda dapat melihat mesin virtual penyimpanan ONTAP FSx untuk yang saat ini ada di sistem file Anda menggunakan FSx konsol Amazon, FSx API Amazon AWS CLI, dan Amazon.

Untuk melihat mesin virtual penyimpanan pada sistem file Anda:

- Menggunakan konsol — Pilih sistem file untuk melihat halaman detail sistem File. Untuk membuat daftar semua mesin virtual penyimpanan pada sistem file, pilih tab Mesin virtual Penyimpanan, lalu pilih mesin virtual penyimpanan yang ingin Anda lihat.
- Menggunakan CLI atau API - Gunakan perintah [describe-storage-virtual-machines](#) CLI atau operasi API. [DescribeStorageVirtualMachines](#)

Respons sistem adalah daftar deskripsi lengkap dari semua yang ada SVMs di akun Anda di dalamnya. Wilayah AWS

Menghapus penyimpanan mesin virtual (SVM)

Anda hanya dapat menghapus FSx untuk ONTAP SVM dengan menggunakan FSx konsol Amazon, the AWS CLI, dan API. Sebelum Anda dapat menghapus SVM, Anda harus menghapus semua volume non-root yang dilampirkan ke SVM terlebih dahulu.

Important

Anda tidak dapat menghapus SVM dengan menggunakan NetApp ONTAP CLI atau API.

Note

Sebelum Anda menghapus mesin virtual penyimpanan, pastikan tidak ada aplikasi yang mengakses data di SVM, dan Anda telah menghapus semua volume non-root yang dilampirkan ke SVM.

Untuk menghapus penyimpanan mesin virtual (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Pilih SVM yang ingin Anda hapus sebagai berikut:
 - Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file ONTAP yang ingin Anda hapus SVM.
 - Pilih tab Storage Virtual Machines.

—Atau—

 - Untuk menampilkan daftar semua yang SVMs tersedia, perluas ONTAP dan pilih mesin virtual Penyimpanan.

Pilih SVM yang ingin Anda hapus dari daftar.

3. Di tab Volume, lihat daftar volume yang dilampirkan ke SVM. Jika ada volume non-root yang dilampirkan ke SVM, Anda harus menghapusnya sebelum Anda dapat menghapus SVM. Untuk informasi selengkapnya, lihat [Menghapus volume](#).
4. Pilih Hapus penyimpanan virtual machine dari menu Actions.
5. Di kotak dialog hapus konfirmasi, pilih Hapus penyimpanan virtual machine.

Untuk menghapus penyimpanan mesin virtual (CLI)

- Untuk menghapus mesin virtual penyimpanan ONTAP, gunakan perintah [delete-storage-virtual-machine](#) CLI (atau operasi API yang [DeleteStorageVirtualMachines](#) setara), seperti yang ditunjukkan pada contoh berikut. FSx

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-abcdef0123456789d
```

Mengelola FSx volume ONTAP

Setiap mesin virtual penyimpanan (SVM) pada sistem file FSx untuk ONTAP dapat memiliki satu atau lebih volume. Volume adalah wadah data terisolasi untuk file, direktori, atau unit penyimpanan logis iSCSI (). LUNs Volume tipis disediakan, artinya mereka mengkonsumsi kapasitas penyimpanan hanya untuk data yang tersimpan di dalamnya.

Anda dapat mengakses volume dari klien Linux, Windows, atau macOS melalui protokol Network File System (NFS), protokol Server Message Block (SMB), atau melalui protokol Internet Small Computer Systems Interface (iSCSI) dengan membuat iSCSI LUN (penyimpanan blok bersama). FSx untuk ONTAP juga mendukung akses multi-protokol (akses NFS dan SMB bersamaan) ke volume yang sama.

Anda dapat membuat volume dengan menggunakan Konsol Manajemen AWS, AWS CLI, Amazon FSx API, atau NetApp Console. Anda juga dapat menggunakan sistem file atau titik akhir administratif SVM untuk membuat, memperbarui, dan menghapus volume dengan menggunakan NetApp ONTAP CLI atau REST API.

Note

Anda dapat membuat 500 volume per pasangan HA, hingga 1.000 volume di semua pasangan HA. FlexGroup volume konstituen dihitung terhadap batas ini. Secara default, ada delapan volume konstituen per agregat, per. FlexGroup

Saat Anda membuat volume, Anda menentukan properti berikut:

- Gaya volume — [Gaya volume](#) dapat berupa FlexVol atau FlexGroup.
- Nama volume — Nama volume.

- Jenis volume - [Jenis volume](#) dapat berupa Read-Write (RW) atau Perlindungan data (DP). Volume DP adalah read-only dan digunakan sebagai tujuan dalam hubungan atau NetAppSnapMirror. SnapVault
- Ukuran volume — Ini adalah jumlah maksimum data yang dapat disimpan volume, terlepas dari tingkat penyimpanannya.
- Jalur persimpangan — Ini adalah lokasi di namespace SVM tempat volume dipasang.
- Efisiensi penyimpanan — Fitur [efisiensi penyimpanan](#), termasuk pemadatan data, kompresi, dan deduplikasi memberikan penghematan penyimpanan tipikal sebesar 65% untuk beban kerja berbagi file tujuan umum.
- [Gaya keamanan](#) volume (Unix atau NTFS) — Menentukan jenis izin apa yang digunakan untuk akses data pada volume saat mengotorisasi pengguna.
- Tiering data — [Kebijakan tiering](#) mendefinisikan data mana yang disimpan dalam tingkat kumpulan kapasitas yang hemat biaya.
- [Periode pendinginan kebijakan tingkat](#) — Menentukan kapan data ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas.
- Kebijakan snapshot — Kebijakan [snapshot](#) menentukan cara sistem membuat snapshot untuk volume. Anda dapat memilih dari tiga kebijakan yang telah ditentukan sebelumnya atau menggunakan kebijakan kustom. yang telah Anda buat menggunakan ONTAP CLI atau REST API.
- [Salin tag ke cadangan](#) - Amazon FSx akan secara otomatis menyalin tag apa pun dari volume Anda ke cadangan menggunakan opsi ini. Anda dapat mengatur opsi ini menggunakan AWS CLI atau Amazon FSx API.

Topik

- [Gaya volume](#)
- [Tipe volume](#)
- [Gaya keamanan volume](#)
- [Membuat volume](#)
- [Memperbarui volume](#)
- [Memindahkan volume antar agregat](#)
- [Volume pemantauan](#)
- [Menghapus volume](#)

Gaya volume

FSx untuk ONTAP menawarkan dua gaya volume yang dapat Anda gunakan untuk tujuan yang berbeda. Anda dapat membuat salah satu FlexVol atau FlexGroup volume menggunakan FSx konsol Amazon, FSx API Amazon AWS CLI, dan Amazon.

- FlexVolvolume menawarkan pengalaman paling sederhana untuk sistem file dengan satu pasangan ketersediaan tinggi (HA), sehingga mereka adalah gaya volume default untuk sistem file generasi pertama dan sistem file generasi kedua dengan satu pasangan HA. Ukuran minimum FlexVol volume adalah 20 mebibytes (MiB), dan ukuran maksimum adalah 314.572.800 MiB.
- FlexGroupvolume terdiri dari beberapa FlexVol volume konstituen, yang memungkinkannya memberikan kinerja dan skalabilitas penyimpanan yang lebih tinggi daripada FlexVol volume untuk sistem file dengan beberapa pasangan HA. FlexGroupvolume adalah gaya volume default untuk sistem file generasi kedua dengan lebih dari satu pasangan HA. Ukuran minimum FlexGroup volume adalah 100 gibibytes (GiB) per konstituen, dan ukuran maksimum adalah 20 pebibytes (PiB).

Anda dapat mengonversi volume dengan FlexVol gaya ke FlexGroup gaya dengan ONTAP CLI, yang menciptakan a FlexGroup dengan satu konstituen. Namun, kami menyarankan Anda AWS DataSync untuk memindahkan data antara FlexVol volume dan FlexGroup volume baru untuk memastikan bahwa data didistribusikan secara merata di seluruh FlexGroup's konstituen. Untuk informasi selengkapnya, lihat [FlexGroupkonstituen](#).

Note

Jika Anda ingin menggunakan ONTAP CLI untuk mengonversi FlexVol volume menjadi FlexGroup volume, pastikan Anda menghapus cadangan FlexVol volume sebelum mengonversinya. ONTAPtidak secara otomatis menyeimbangkan kembali data sebagai bagian dari konversi, sehingga data mungkin tidak seimbang di seluruh konstituen. FlexGroup

FlexGroupkonstituen

FlexGroupVolume terdiri dari konstituen, yaitu FlexVol volume. Secara default, FSx untuk ONTAP menetapkan delapan konstituen ke FlexGroup volume per pasangan HA.

Ketika Anda membuat FlexGroup volume Anda, ukurannya dibagi rata di antara konstituennya. Misalnya, jika Anda membuat FlexGroup volume 800 gigabyte (GB) dengan delapan konstituen,

masing-masing konstituen berukuran 100 GB. FlexGroupVolume dapat berukuran antara 100 GB dan 20 PiB, tetapi ukuran totalnya tergantung pada ukuran konstituen. Setiap konstituen memiliki ukuran minimum 100 GB dan ukuran maksimum 300 TiB. Misalnya, FlexGroup volume dengan delapan konstituen memiliki ukuran minimum 800 GB dan ukuran maksimum 20 PiB.

ONTAP mendistribusikan data pada tingkat file di seluruh konstituen. Anda dapat menyimpan hingga dua miliar file di setiap konstituen pada FlexGroup volume Anda.

Saat Anda memperbarui ukuran FlexGroup volume Anda, ukuran baru didistribusikan secara merata di antara konstituen yang ada.

Anda juga dapat menambahkan lebih banyak konstituen ke FlexGroup volume Anda menggunakan ONTAP CLI atau REST API. Namun, kami menyarankan Anda hanya melakukannya jika Anda membutuhkan kapasitas penyimpanan tambahan dan semua konstituen Anda sudah pada ukuran maksimumnya (300 TiB per konstituen). Menambahkan konstituen dapat menyebabkan ketidakseimbangan data dan I/O seluruh konstituen. Sampai konstituennya seimbang, mungkin saja throughput penulisan mungkin 5-10% lebih rendah dari volume seimbangFlexGroup. Ketika data baru ditulis ke FlexGroup volume, ONTAP memprioritaskan mendistribusikannya di antara konstituen baru sampai konstituen seimbang. Jika Anda menambahkan konstituen baru, kami sarankan memilih nomor genap dan tidak melebihi delapan per agregat.

Note

Jika Anda menambahkan konstituen baru, snapshot Anda yang ada menjadi snapshot sebagian; oleh karena itu, snapshot tersebut tidak dapat digunakan untuk mengembalikan FlexGroup volume Anda sepenuhnya ke status sebelumnya. Snapshot sebelumnya tidak dapat menawarkan point-in-time gambar lengkap FlexGroup volume Anda karena konstituen baru belum ada. Namun, sebagian snapshot dapat digunakan untuk memulihkan file dan direktori individual, untuk membuat volume baru, atau untuk mereplikasi dengan. SnapMirror

Tipe volume

FSx untuk ONTAP menawarkan dua jenis volume yang dapat Anda buat menggunakan FSx konsol Amazon, yaitu AWS CLI, dan Amazon FSx API.

- Volume baca-tulis (RW) digunakan dalam banyak kasus. Seperti namanya, mereka dapat dibaca.

- Volume perlindungan data (DP) adalah volume hanya-baca yang Anda gunakan sebagai tujuan suatu atau NetApp SnapMirror hubungan. SnapVault Anda harus menggunakan volume DP saat ingin [memigrasi](#) atau [melindungi](#) data satu volume.

FlexVoldan FlexGroup volume dapat berupa RW atau DP.

Note

Anda tidak dapat memperbarui jenis volume setelah volume dibuat.

Gaya keamanan volume

Saat membuat volume FSx untuk ONTAP, Anda dapat memilih dari dua gaya keamanan: Unix dan NTFS. Setiap gaya keamanan memiliki efek yang berbeda pada bagaimana izin ditangani untuk data. Anda harus memahami efek yang berbeda untuk memastikan bahwa Anda memilih gaya keamanan yang sesuai untuk tujuan Anda.

Penting untuk dipahami bahwa gaya keamanan tidak menentukan jenis klien apa yang dapat atau tidak dapat mengakses data. Gaya keamanan hanya menentukan jenis izin FSx untuk penggunaan ONTAP untuk mengontrol akses data dan jenis klien apa yang dapat memodifikasi izin ini.

Dua faktor yang Anda gunakan untuk menentukan gaya keamanan untuk volume adalah jenis administrator yang mengelola sistem file dan jenis pengguna atau layanan yang mengakses data pada volume.

Saat membuat volume di FSx konsol Amazon, CLI, dan API, gaya keamanan secara otomatis diatur ke gaya keamanan volume root. Anda dapat memodifikasi gaya keamanan volume menggunakan API AWS CLI atau. Anda dapat mengubah pengaturan ini setelah volume dibuat. Untuk informasi selengkapnya, lihat [Memperbarui volume](#).

Saat Anda mengonfigurasi gaya keamanan pada volume, pertimbangkan kebutuhan lingkungan Anda untuk memastikan bahwa Anda memilih gaya keamanan terbaik untuk menghindari masalah dalam mengelola izin. Perlu diingat bahwa gaya keamanan tidak menentukan tipe klien mana yang dapat mengakses data. Gaya keamanan menentukan izin yang digunakan untuk memungkinkan akses data dan jenis klien yang dapat mengubah izin tersebut. Berikut ini adalah pertimbangan yang dapat membantu Anda memutuskan gaya keamanan mana yang akan dipilih untuk volume:

- Unix (Linux) — Pilih gaya keamanan ini jika sistem file dikelola oleh administrator Unix, mayoritas pengguna adalah klien NFS, dan aplikasi yang mengakses data menggunakan pengguna Unix sebagai akun layanan. Hanya klien Linux yang dapat memodifikasi izin dengan gaya keamanan Unix, dan jenis izin yang digunakan pada file dan direktori adalah mode-bit atau NFS v4.x. ACLs
- NTFS — Pilih gaya keamanan ini jika sistem file dikelola oleh administrator Windows, mayoritas pengguna adalah klien SMB, dan aplikasi yang mengakses data menggunakan pengguna Windows sebagai akun layanan. Jika ada akses Windows yang diperlukan untuk volume, kami sarankan Anda menggunakan gaya keamanan NTFS. Hanya klien Windows yang dapat memodifikasi izin dengan gaya keamanan NTFS, dan jenis izin yang digunakan pada file dan direktori adalah NTFS. ACLs

Membuat volume

Anda dapat membuat FSx untuk ONTAP FlexVol atau FlexGroup volume menggunakan FSx konsol Amazon, FSx API Amazon AWS CLI, dan Amazon, selain antarmuka baris perintah NetApp ONTAP (CLI) dan REST API.

Untuk membuat FlexVol volume (konsol)

Note

Gaya keamanan volume secara otomatis diatur ke gaya keamanan volume root.

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Volume.
3. Pilih Buat volume.
4. Untuk jenis sistem File, pilih Amazon FSx untuk NetApp ONTAP.
5. Di bagian Detail sistem berkas, berikan informasi berikut:
 - Untuk sistem File, pilih sistem file untuk membuat volume aktif.
 - Untuk mesin virtual Penyimpanan, pilih mesin virtual penyimpanan (SVM) untuk membuat volume aktif.
6. Di bagian Gaya volume, pilih FlexVol.
7. Di bagian Detail volume, berikan informasi berikut:

- Di bidang Nama volume, berikan nama untuk volume. Anda dapat menggunakan hingga 203 karakter alfanumerik atau garis bawah (_).
- Untuk ukuran Volume, masukkan bilangan bulat apa pun dalam kisaran 20—314572800 untuk menentukan ukuran dalam mebibytes (MiB).
- Untuk tipe Volume, pilih Read-Write (RW) untuk membuat volume yang dapat dibaca dan ditulis atau Perlindungan Data (DP) untuk membuat volume yang hanya-baca dan dapat digunakan sebagai tujuan hubungan atau. NetApp SnapMirror SnapVault Untuk informasi selengkapnya, lihat [Tipe volume](#).
- Untuk jalur Junction, masukkan lokasi di dalam sistem file untuk me-mount volume. Nama harus memiliki garis miring ke depan, misalnya/vol3.
- Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur efisiensi penyimpanan ONTAP (deduplikasi, kompresi, dan pemadatan) pada volume ini. Untuk informasi selengkapnya, lihat [Efisiensi penyimpanan](#).
- Untuk gaya keamanan Volume, pilih antara Unix (Linux) dan NTFS untuk volume. Untuk informasi selengkapnya, lihat [Gaya keamanan volume](#).
- Untuk kebijakan Snapshot, pilih kebijakan snapshot untuk volume. Untuk informasi selengkapnya tentang kebijakan snapshot, lihat [Kebijakan snapshot](#).

Jika memilih Kebijakan khusus, Anda harus menentukan nama kebijakan di bidang kebijakan khusus. Kebijakan kustom harus sudah ada di SVM atau di sistem file. Anda dapat membuat kebijakan snapshot khusus dengan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat [Membuat Kebijakan Snapshot di Dokumentasi](#) Produk NetApp ONTAP.

8. Di bagian Storage tiering, berikan informasi berikut:

- Untuk kebijakan tingkatan kumpulan Kapasitas, pilih kebijakan tiering kumpulan penyimpanan untuk volume, yang dapat berupa Otomatis (default), Hanya Snapshot, Semua, atau Tidak Ada. Untuk informasi selengkapnya, lihat [Kebijakan tingkatan volume](#).
- Jika Anda memilih Auto atau Snapshot Only, Anda dapat mengatur periode pendinginan kebijakan Tiering untuk menentukan jumlah hari sebelum data yang belum diakses ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas. Anda dapat memberikan nilai antara 2 dan 183 hari. Pengaturan default adalah 31 hari.

9. Di bagian Lanjutan, untuk SnapLockKonfigurasi, pilih antara Diaktifkan dan Dinonaktifkan. Untuk informasi selengkapnya tentang mengonfigurasi volume SnapLock Kepatuhan atau volume SnapLock Perusahaan, lihat [Memahami SnapLock Kepatuhan](#) dan [Memahami SnapLock](#)

[Perusahaan](#). Untuk informasi selengkapnya tentang SnapLock, lihat [Melindungi data Anda dengan SnapLock](#).

10. Pilih Konfirmasi untuk membuat volume.

Anda dapat memantau kemajuan pembaruan pada halaman detail sistem file, di kolom Status panel Volume. Volume siap digunakan saat statusnya Dibuat.

Untuk membuat FlexGroup volume (konsol)

Note

Anda hanya dapat membuat FlexGroup volume untuk sistem file dengan beberapa pasangan HA menggunakan FSx konsol Amazon. Untuk membuat FlexVol volume untuk sistem file dengan beberapa pasangan HA, gunakan AWS CLI, Amazon FSx API, atau alat NetApp manajemen.

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Volume.
3. Pilih Buat volume.
4. Untuk jenis sistem File, pilih Amazon FSx untuk NetApp ONTAP.
5. Di bagian Detail sistem berkas, berikan informasi berikut:
 - Untuk sistem File, pilih sistem file untuk membuat volume aktif.
 - Untuk mesin virtual Penyimpanan, pilih mesin virtual penyimpanan (SVM) untuk membuat volume aktif.
6. Di bagian Gaya volume, pilih FlexGroup.
7. Di bagian Detail volume, berikan informasi berikut:
 - Di bidang Nama volume, berikan nama untuk volume. Anda dapat menggunakan hingga 203 karakter alfanumerik atau garis bawah (_).
 - Untuk ukuran Volume, masukkan bilangan bulat apa pun dalam kisaran 800 gibibyte (GiB) — 2.400 tebibytes (TiB) per pasangan HA. Misalnya, sistem file dengan 12 pasang ketersediaan tinggi (HA) akan memiliki ukuran volume minimum 9.600 GiB dan ukuran maksimum 20.480 TiB.

- Untuk tipe Volume, pilih Read-Write (RW) untuk membuat volume yang dapat dibaca dan ditulis atau Perlindungan Data (DP) untuk membuat volume yang hanya-baca dan dapat digunakan sebagai tujuan hubungan atau. NetApp SnapMirror SnapVault Untuk informasi selengkapnya, lihat [Tipe volume](#).
- Untuk jalur Junction, masukkan lokasi di dalam sistem file untuk me-mount volume. Nama harus memiliki garis miring ke depan, misalnya/vol3.
- Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur efisiensi penyimpanan ONTAP (deduplikasi, kompresi, dan pemadatan). Untuk informasi selengkapnya, lihat [Efisiensi penyimpanan](#).
- Untuk gaya keamanan Volume, pilih antara Unix (Linux) dan NTFS untuk volume. Untuk informasi selengkapnya, lihat [Gaya keamanan volume](#).

 Note

Gaya keamanan volume secara otomatis diatur ke gaya keamanan volume root.

- Untuk kebijakan Snapshot, pilih kebijakan snapshot untuk volume. Untuk informasi selengkapnya tentang kebijakan snapshot, lihat [Kebijakan snapshot](#).

Jika memilih Kebijakan khusus, Anda harus menentukan nama kebijakan di bidang kebijakan khusus. Kebijakan kustom harus sudah ada di SVM atau di sistem file. Anda dapat membuat kebijakan snapshot khusus dengan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat [Membuat Kebijakan Snapshot di Dokumentasi](#) Produk NetApp ONTAP.

8. Di bagian Storage tiering, berikan informasi berikut:

- Untuk kebijakan tingkatan kumpulan Kapasitas, pilih kebijakan tiering kumpulan penyimpanan untuk volume, yang dapat berupa Otomatis (default), Hanya Snapshot, Semua, atau Tidak Ada. Untuk informasi selengkapnya, lihat [Kebijakan tingkatan volume](#).
- Jika Anda memilih Auto atau Snapshot Only, Anda dapat mengatur periode pendinginan kebijakan Tiering untuk menentukan jumlah hari sebelum data yang belum diakses ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas. Anda dapat memberikan nilai antara 2-183 hari. Pengaturan default adalah 31 hari.

9. Di bagian Lanjutan, untuk SnapLockKonfigurasi, pilih antara Diaktifkan dan Dinonaktifkan. Untuk informasi selengkapnya tentang mengonfigurasi volume SnapLock Kepatuhan atau volume SnapLock Perusahaan, lihat [Memahami SnapLock Kepatuhan](#) dan [Memahami SnapLock](#)

[Perusahaan](#). Untuk informasi selengkapnya tentang SnapLock, lihat [Melindungi data Anda dengan SnapLock](#).

10. Pilih Konfirmasi untuk membuat volume.

Anda dapat memantau kemajuan pembaruan pada halaman detail sistem file, di kolom Status panel Volume. Volume siap digunakan saat statusnya Dibuat.

Untuk membuat volume (CLI)

- FSx Untuk membuat volume ONTAP, gunakan perintah CLI [create-volume](#) (atau operasi API yang [CreateVolumesetara](#)), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx create-volume \
  --volume-type ONTAP \
  --name vol1 \
  --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
  SizeInMegabytes=1024,SnapshotPolicy=default, \
  StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
  StorageEfficiencyEnabled=true
```

Setelah berhasil membuat volume, Amazon FSx mengembalikan deskripsinya dalam format JSON, seperti yang ditunjukkan pada contoh berikut.

```
{
  "Volume": {
    "CreationTime": "2022-08-12T13:03:37.625000-04:00",
    "FileSystemId": "fs-abcdef0123456789c",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "OntapConfiguration": {
      "CopyTagsToBackups": true,
      "FlexCacheEndpointType": "NONE",
      "JunctionPath": "/vol1",
      "SecurityStyle": "NTFS",
      "SizeInMegabytes": 1024,
      "SnapshotPolicy": "default",
      "StorageEfficiencyEnabled": true,
      "StorageVirtualMachineId": "svm-abcdef0123456789a",
      "StorageVirtualMachineRoot": false,
```

```
    "TieringPolicy": {
      "Name": "NONE"
    },
    "OntapVolumeType": "RW"
  },
  "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
  "VolumeId": "fsvol-abcdef0123456789b",
  "VolumeType": "ONTAP"
}
}
```

Anda juga dapat membuat volume baru dengan mengembalikan cadangan volume ke volume baru. Untuk informasi selengkapnya, lihat [Memulihkan backup ke volume baru](#).

Memperbarui volume

Anda dapat memperbarui konfigurasi FSx untuk volume ONTAP menggunakan FSx konsol Amazon, FSx API Amazon AWS CLI, dan Amazon, selain antarmuka baris perintah NetApp ONTAP (CLI) dan REST API. Anda dapat memodifikasi properti berikut dari volume ONTAP FSx yang sudah ada:

- Nama volume
- Jalur persimpangan
- Ukuran volume
- Efisiensi penyimpanan
- Kebijakan tingkatan kolam kapasitas
- Gaya keamanan volume
- Kebijakan snapshot
- Periode pendinginan kebijakan tingkat
- Salin tag ke backup (menggunakan dan AWS CLI Amazon FSx API)

Untuk informasi selengkapnya, lihat [Mengelola FSx volume ONTAP](#).

Untuk memperbarui konfigurasi volume (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.

2. Arahkan ke sistem File dan pilih sistem file ONTAP yang ingin Anda perbarui volumenya.
3. Pilih tab Volume.
4. Pilih volume yang ingin Anda perbarui.
5. Untuk Tindakan, pilih Perbarui volume.

Kotak dialog Perbarui volume ditampilkan dengan pengaturan volume saat ini.

6. Untuk jalur Junction, masukkan lokasi yang ada di dalam sistem file untuk me-mount volume. Nama harus memiliki garis miring ke depan, seperti/vol5.
7. Untuk ukuran Volume, Anda dapat menambah atau mengurangi ukuran volume dalam rentang yang ditentukan di FSx konsol Amazon. Untuk FlexVol volume, ukuran maksimum adalah 300 TiB. Untuk FlexGroup volume, ukuran maksimum adalah 300 TiB dikalikan dengan jumlah total volume konstituen yang Anda FlexGroup miliki, hingga maksimum 20 PiB.
8. Untuk [efisiensi Penyimpanan](#), pilih Diaktifkan untuk mengaktifkan fitur efisiensi penyimpanan ONTAP (deduplikasi, kompresi, dan pemadatan) pada volume, atau pilih Dinonaktifkan untuk menonaktifkannya.
9. Untuk kebijakan tingkatan kumpulan Kapasitas, pilih kebijakan tiering kumpulan penyimpanan baru untuk volume, yang dapat berupa Otomatis (default), khusus Snapshot, Semua, atau Tidak Ada. Untuk informasi selengkapnya tentang kebijakan tingkatan kumpulan kapasitas, lihat[Kebijakan tingkatan volume](#).
10. Untuk [gaya keamanan Volume](#), pilih Unix (Linux), NTFS, atau Mixed. Gaya keamanan volume menentukan apakah preferensi diberikan kepada NTFS atau UNIX ACLs untuk akses multi-protokol. Mode MIXED tidak diperlukan untuk akses multi-protokol dan hanya direkomendasikan untuk pengguna tingkat lanjut.
11. Untuk kebijakan Snapshot, pilih kebijakan snapshot untuk volume. Untuk informasi selengkapnya tentang kebijakan snapshot, lihat[Kebijakan snapshot](#).

Jika memilih Kebijakan khusus, Anda harus menentukan nama kebijakan di bidang kebijakan khusus. Kebijakan kustom harus sudah ada di SVM atau di sistem file. Anda dapat membuat kebijakan snapshot khusus dengan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat [Membuat Kebijakan Snapshot di Dokumentasi](#) Produk NetApp ONTAP.

12. Untuk periode pendinginan kebijakan Tiering, nilai yang berlaku adalah 2-183 hari. Periode pendinginan kebijakan tingkat volume menentukan jumlah hari sebelum data yang belum diakses ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas. Pengaturan ini hanya memengaruhi Snapshot-only kebijakan Auto dan kebijakan.
13. Pilih Perbarui untuk memperbarui volume.

Untuk memperbarui konfigurasi volume (CLI)

- Untuk memperbarui konfigurasi volume ONTAP, gunakan perintah CLI [update-volume](#) (atau operasi API yang [UpdateVolumesetara](#)), seperti yang ditunjukkan pada contoh berikut. FSx

```
aws fsx update-volume \  
  --volume-id fsvol-1234567890abcdefa \  
  --name new_vol \  
  --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \  
    SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \  
    StorageEfficiencyEnabled=true, \  
    TieringPolicy=all
```

Memperluas FlexGroup volume

Anda dapat menambahkan volume konstituen tambahan ke FlexGroup volume Anda dengan `volume expand` perintah di ONTAP CLI. Ini adalah praktik terbaik setelah menambahkan pasangan ketersediaan tinggi (HA) ke sistem file Anda karena memastikan FlexGroup volume Anda tetap seimbang.

Sebelum memperluas FlexGroup volume Anda, pertimbangkan hal-hal berikut:

- Semua volume FlexGroup's konstituen memiliki kapasitas penyimpanan yang sama. Ketika Anda memperluas FlexGroup volume Anda dengan konstituen tambahan, setiap konstituen memiliki ukuran yang sama dengan konstituen yang ada. Oleh karena itu, pastikan bahwa setiap agregat memiliki ruang yang cukup tersedia sebelum menambahkan konstituen.
- AWS merekomendasikan mempertahankan delapan volume konstituen per agregat untuk setiap FlexGroup volume. Delapan volume konstituen per agregat memaksimalkan paralelisme FlexGroup volume dan menawarkan kinerja paling optimal untuk beban kerja Anda. Umumnya, kami hanya menyarankan untuk memperluas FlexGroup volume Anda dengan konstituen tambahan jika Anda menambahkan pasangan HA. Ini adalah satu-satunya skenario di mana Anda perlu menambahkan konstituen untuk mempertahankan delapan konstituen per agregat.
- Jika FlexGroup volume Anda dalam suatu SnapMirror hubungan, maka FlexGroup volume sumber dan tujuan harus memiliki jumlah konstituen yang sama. Jika tidak, SnapMirror transfer akan gagal. SnapMirror beroperasi pada tingkat konstituen dan mentransfer data antara masing-masing konstituen individu. Oleh karena itu, jika Anda memperluas FlexGroup volume dengan volume konstituen tambahan, Anda juga harus secara manual memperluas volume apa pun yang ada SnapMirror hubungannya dengannya.

- Saat Anda memperluas FlexGroup volume dengan konstituen tambahan, semua salinan snapshot yang ada menjadi salinan “sebagian”. Salinan sebagian tidak dapat dipulihkan, tetapi dapat dijelajahi dan masing-masing file dapat dipulihkan. Selain itu, ini mengakibatkan hilangnya inkrementalitas apa pun untuk cadangan, FSx AWS cadangan, atau hubungan Amazon SnapMirror
- Anda tidak dapat menghapus volume konstituen setelah Anda menambahkannya.

Menambahkan konstituen FlexGroup volume

Anda dapat menggunakan ONTAP CLI untuk menambahkan volume konstituen ke volume Anda. FlexGroup

Untuk menambah konstituen FlexGroup volume

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen FSx Amazon NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Gunakan perintah [volume expand](#) ONTAP CLI untuk memperluas FlexGroup volume Anda dengan konstituen tambahan. Ganti nilai-nilai berikut:
 - *svm_name* dengan nama mesin virtual penyimpanan (SVM) yang menampung FlexGroup volume Anda (misalnya, *svm1*).
 - *vol_name* dengan nama FlexGroup volume yang ingin Anda kembangkan (misalnya, *vol1*).
 - *aggregates* dengan daftar agregat yang dipisahkan koma yang ingin Anda tambahkan volume FlexGroup konstituen. Misalnya, *aggr1* untuk agregat tunggal atau *aggr1, aggr2* untuk beberapa agregat.
 - *constituent_per_aggregated* dengan jumlah konstituen tambahan yang ingin Anda tambahkan ke masing-masing yang ditentukan *aggregates*. Anda hanya harus menambahkan konstituen yang cukup untuk memastikan bahwa FlexGroup volume Anda memiliki jumlah konstituen yang seimbang di seluruh agregat tempat ia berada.

```
::> volume expand -vserver svm_name -volume vol_name -aggr-list aggregates -aggr-list-multiplier constituents_per_aggregate
```

Important

Anda tidak dapat menghapus FlexGroup konstituen setelah Anda menambahkannya, jadi periksa input Anda sebelum menjalankan perintah sebelumnya.

Memindahkan volume antar agregat

Saat Anda menambahkan pasangan ketersediaan tinggi (HA) ke sistem file Anda, Anda perlu menyeimbangkan kembali data yang ada dengan memindahkan volume ke agregat baru. Untuk memindahkan volume antar agregat, Anda dapat menggunakan `volume move` perintah di CLI ONTAP.

Sebelum menggunakan `volume move` perintah, pertimbangkan hal-hal berikut:

- Menggunakan `volume move` perintah dapat memengaruhi kinerja karena mengkonsumsi sumber daya jaringan dan disk pada sistem file Anda. Oleh karena itu, kami merekomendasikan untuk memindahkan volume antar agregat selama periode aktivitas rendah. Atau, Anda dapat mengurangi pemanfaatan throughput jaringan dan pemanfaatan throughput disk pada sistem file Anda menjadi tidak lebih dari 50% saat memindahkan volume.
- Untuk mengurangi dampak kinerja pada sistem file Anda, sebaiknya pindahkan satu volume antara dua pasangan HA dan agregat sekaligus. Misalnya, jika sistem file Anda memiliki empat pasangan HA, sebaiknya pindahkan dua volume sekaligus (dengan asumsi pergerakan volume bukan dari atau menuju pasangan HA yang sama). ONTAP mendukung pergerakan hingga delapan volume pada setiap pasangan HA sekaligus, tetapi pergerakan volume yang lebih simultan akan mengurangi kinerja klien I/O dan pergerakan volume yang sedang berlangsung.
- Setiap data yang disimpan pada tingkat SSD pada volume yang terkena dampak secara fisik dipindahkan ke set disk yang berbeda pada server file yang berbeda. Operasi ini terjadi di latar belakang dan membutuhkan waktu. Tingkat waktu transfer tergantung pada kapasitas throughput sistem file Anda dan jumlah aktivitas pada sistem file Anda. Namun, pergerakan volume dapat dibatasi. Untuk informasi selengkapnya, lihat [Volume pelambatan bergerak](#).

- Data yang disimpan dalam kumpulan kapasitas tidak dipindahkan secara fisik karena pasangan HA berbagi penyimpanan kolam kapasitas yang sama. Sebaliknya, ONTAP memindahkan metadata yang sepenuhnya menggambarkan setiap blok dalam kumpulan kapasitas (langkah logis). Perlu diingat bahwa metadata file selalu disimpan di tingkat SSD. Untuk informasi selengkapnya, lihat [Tingkat data volume](#).

Fase memindahkan volume

Ada dua fase dalam operasi pemindahan volume: fase replikasi dan fase cutover. Selama fase replikasi, data yang ada direplikasi ke agregat baru volume. Selama fase cutover, ONTAP mencoba transfer cepat akhir ke agregat baru volume. Ini termasuk mentransfer data apa pun yang telah ditulis selama fase transfer dan mengarahkan lalu lintas baru ke agregat baru volume. Secara default, jendela cutover adalah 30 detik dan menghentikan semua volume I/O Anda. Jika ONTAP tidak dapat melakukan semua langkah ini selama jendela cutover, itu akan gagal. Secara default, ONTAP akan mencoba memotong tiga kali berturut-turut. Jika ketiga upaya berturut-turut gagal, maka ONTAP akan mencoba lagi satu jam sekali sampai berhasil. Anda dapat mengurangi beban pada sistem file Anda untuk memastikan bahwa fase cutover berhasil dengan mengurangi atau menjeda I/O lalu lintas ke volume sebelum fase cutover dimulai.

Volume awal bergerak

Untuk memulai pergerakan volume

1. Untuk mengakses CLI NetApp ONTAP, buat sesi SSH pada port manajemen FSx Amazon NetApp untuk sistem file ONTAP dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Jalankan [gerakan volume mulai perintah](#) ONTAP CLI. Ganti nilai-nilai berikut:
 - `vserver_name` dengan nama SVM yang menampung volume yang Anda pindahkan.
 - `volume_name` dengan nama konstituen volume (misalnya, `vol1__0001`).
 - `aggregate_name` dengan nama agregat tujuan untuk volume.
 - `-enforce-network-throttling` untuk membatasi total throughput volume move. Ini opsional.

```
::> volume move start -vserver svm_name -volume volume_name --destination-  
aggregate aggregate_name -foreground false  
[Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".  
Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the  
status of this operation.
```

Important

Volume bergerak mengkonsumsi sumber daya jaringan dan disk untuk server file sumber dan tujuan. Oleh karena itu, kinerja beban kerja Anda dapat dipengaruhi oleh pergerakan volume apa pun yang sedang berlangsung. Selain itu, I/O lalu lintas Anda ke volume akan dijeda sementara selama fase cutover dari pemindahan volume.

Memantau pergerakan volume

Untuk memantau pergerakan volume

- Untuk memeriksa status operasi pemindahan volume, gunakan perintah `volume move show` ONTAP CLI.

```
::> volume move show -vserver svm_name -volume volume_name
```

```
Vserver Name: svm01  
Volume Name: vol1__0001  
Actual Completion Time: -  
Bytes Remaining: 1.00TB  
Specified Action For Cutover: retry_on_failure  
Specified Cutover Time Window: 30  
Destination Aggregate: aggr2  
Destination Node: FsxId01234567890abcdef-03  
Detailed Status: Transferring data: 12.23GB sent.  
Percentage Complete: 1%  
Move Phase: replicating  
Prior Issues Encountered: -  
Estimated Remaining Duration: 00:40:25  
Replication Throughput: 434.3MB/s  
Duration of Move: 00:00:27
```

```
Source Aggregate: aggr1
Source Node: FsxId01234567890abcdef-01
Move State: healthy
```

Output perintah menunjukkan perkiraan waktu untuk menyelesaikan gerakan. Setelah selesai, Move phase akan menampilkan completed status.

Mempertahankan FlexGroup volume seimbang

Agar beban kerja Anda dapat bekerja secara optimal, FlexGroup volume Anda harus mencakup semua agregat dan memiliki jumlah volume konstituen genap per agregat. Kami merekomendasikan memiliki delapan konstituen per agregat. Pertimbangkan skenario berikut saat menyeimbangkan kembali volumeFlexGroup:

- Memindahkan FlexGroup konstituen di antara agregat yang ada: Jika Anda memindahkan volume FlexGroup's konstituen ke agregat lain yang seimbangFlexGroup, Anda kemudian harus memindahkan konstituen lain yang kurang digunakan untuk agregat asli. Ini memastikan bahwa Anda FlexGroup memiliki jumlah konstituen genap per agregat.

Memindahkan FlexGroup konstituen ke agregat baru setelah menambahkan pasangan HA: Jika Anda memindahkan volume FlexGroup's konstituen ke agregat baru setelah menambahkan pasangan HA, maka Anda harus memperluas FlexGroup dengan konstituen tambahan pada agregat yang kehilangan konstituen. Ini memastikan bahwa Anda FlexGroup memiliki jumlah konstituen genap per agregat. Untuk informasi selengkapnya, lihat [the section called “Memperluas FlexGroup volume”](#).

Volume pelambatan bergerak

Jika Anda ingin membatasi bandwidth pemindahan volume pada sistem file Anda, Anda dapat menambahkan `-enforce-network-throttling` opsi di awal operasi.

Note

Menggunakan opsi ini mempengaruhi transfer data SnapMirror replikasi masuk untuk sistem file. Lacak bagaimana Anda mengonfigurasi opsi replikasi sistem file Anda karena Anda tidak dapat melihatnya setelah mengaturnya.

Untuk membatasi pergerakan volume

1. Throttle menggunakan throttle replikasi global. Untuk mengatur throttle replikasi global, gunakan perintah berikut di CLI. ONTAP

```
::> options -option-name replication.throttle.enable on
```

2. Tentukan total bandwidth maksimum yang dapat digunakan oleh replikasi, menggantikan opsi berikut:

- `kbs_throttled` dengan throughput maksimum yang diinginkan untuk digunakan untuk replikasi apa pun (termasuk SnapMirror dan pergerakan volume), dalam Kilobyte per detik.

```
::> options -option-name replication.throttle.incoming.max_kbs kbs_throttle  
::> options -option-name replication.throttle.outgoing.max_kbs kbs_throttle
```

Volume pemantauan

Anda dapat melihat volume yang saat ini ada di sistem file Anda menggunakan FSx konsol Amazon AWS CLI, Amazon FSx API, dan Amazon SDKs.

Untuk memantau volume pada sistem file Anda:

- Menggunakan konsol — Pilih sistem file untuk melihat halaman detail sistem File. Pilih tab Volume untuk mencantumkan semua volume pada sistem file, lalu pilih volume yang ingin Anda lihat.
- Menggunakan CLI atau API - Gunakan [perintah CLI deskripsi-volume](#) atau operasi API.

[DescribeVolumes](#)

```
$ aws fsx describe-volumes  
{  
  "Volumes": [  
    {  
      "CreationTime": "2024-03-04T20:17:44+00:00",  
      "FileSystemId": "fs-abcdef0123a0bb087",  
      "Lifecycle": "CREATED",  
      "Name": "SVM8_ext_root",  
      "OntapConfiguration": {  
        "FlexCacheEndpointType": "NONE",  
        "JunctionPath": "/",
```

```

        "SecurityStyle": "NTFS",
        "SizeInMegabytes": 1024,
        "StorageEfficiencyEnabled": false,
        "StorageVirtualMachineId": "svm-01234567890abcdef",
        "StorageVirtualMachineRoot": true,
        "TieringPolicy": {
            "Name": "NONE"
        },
        "UUID": "42ce3de0-da64-11ee-a22d-7f7cdfb8d381",
        "OntapVolumeType": "RW",
        "SnapshotPolicy": "default",
        "CopyTagsToBackups": false,
        "VolumeStyle": "FLEXVOL",
        "AggregateConfiguration": {
            "Aggregates": [
                "aggr1"
            ]
        },
        "SizeInBytes": 1073741824
    },
    "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcdef0123a0bb087/fsvol-abcdef0123456789a",
    "VolumeId": "fsvol-abcdef0123456789a",
    "VolumeType": "ONTAP"
}
]
}

```

Melihat volume offline

Anda tidak dapat membuat atau menghapus cadangan volume saat volume sumber offline. Anda dapat menggunakan perintah [volume show](#) ONTAP CLI untuk menentukan status volume saat ini.

```
volume show -vserver svm-name
```

Untuk informasi tentang mengakses ONTAP CLI pada sistem file Anda, lihat. [Menggunakan CLI NetApp ONTAP](#)

```

FsxIdabc12345::> volume show -vserver vs1
Vserver  Volume      Aggregate    State      Type      Size  Available Used%
-----

```

vs1	vol1	aggr1	online	RW	2GB	1.9GB	5%
vs1	vol1_dr	aggr0_dp	online	DP	200GB	160.0GB	20%
vs1	vol2	aggr0	online	RW	150GB	110.3GB	26%
vs1	vol2_dr	aggr0_dp	online	DP	150GB	110.3GB	26%
vs1	vol3	aggr1	online	RW	150GB	120.0GB	20%
vs1	vol3_dr	aggr1_dp	online	DP	150GB	120.0GB	20%
vs1	vol4	aggr1	online	RW	200GB	159.8GB	20%

7 entries were displayed.

Untuk mengembalikan volume offline secara online, gunakan perintah [volume online](#) ONTAP CLI, seperti yang ditunjukkan pada contoh berikut. Jika hanya ada satu SVM (Vserver), Anda tidak perlu menentukan parameternya. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Menghapus volume

Anda dapat menghapus volume FSx untuk ONTAP menggunakan FSx konsol Amazon, FSx API Amazon AWS CLI, dan Amazon, selain antarmuka baris perintah NetApp ONTAP (CLI) dan REST API.

Sebelum Anda menghapus volume, pastikan tidak ada aplikasi yang mengakses data dalam volume yang ingin Anda hapus.

Important

Anda hanya dapat menghapus volume menggunakan FSx konsol Amazon, API, atau CLI jika volume telah mengaktifkan FSx cadangan Amazon.

Mengambil cadangan volume akhir

Saat Anda menghapus volume menggunakan FSx konsol Amazon, Anda memiliki opsi untuk mengambil cadangan akhir volume. Sebagai praktik terbaik, kami menyarankan Anda memilih untuk mengambil cadangan akhir. Jika Anda merasa tidak membutuhkannya setelah jangka waktu tertentu, Anda dapat menghapus ini dan cadangan volume yang dibuat secara manual lainnya. Saat Anda menghapus volume dengan menggunakan perintah `delete-volume` CLI, Amazon FSx mengambil cadangan akhir secara default.

Untuk informasi selengkapnya tentang pencadangan volume, lihat. [Melindungi data Anda dengan backup volume](#)

Untuk menghapus volume (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file ONTAP yang ingin Anda hapus volumenya.
3. Pilih tab Volume.
4. Pilih volume yang ingin Anda hapus.
5. Untuk Tindakan, pilih Hapus volume.
6. (hanya SnapLock Enterprise volume) Untuk Bypass SnapLock Enterprise Retention, pilih Ya.
7. Di kotak dialog konfirmasi, untuk Buat cadangan akhir, Anda memiliki dua opsi:
 - Pilih Ya untuk mengambil cadangan akhir volume. Nama cadangan akhir ditampilkan.
 - Pilih Tidak jika Anda tidak ingin cadangan akhir volume. Anda diminta untuk mengakui bahwa setelah volume dihapus, backup otomatis tidak lagi tersedia.
8. Konfirmasikan penghapusan volume dengan memasukkan hapus di bidang Konfirmasi hapus.
9. Pilih Hapus volume.

Untuk menghapus volume (CLI)

- Untuk menghapus volume ONTAP, gunakan perintah CLI [hapus volume](#) (atau operasi API yang [DeleteVolume](#) setara), seperti yang ditunjukkan pada contoh berikut. FSx

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Menghapus volume SnapLock

Bagian ini menjelaskan cara menghapus SnapLock volume.

Anda dapat menghapus volume SnapLock Kepatuhan jika periode retensi semua penulisan sekali, membaca banyak file (WORM) di dalamnya kedaluwarsa.

 Note

Ketika Anda menutup Akun AWS yang berisi SnapLock Enterprise atau Compliance volume, AWS dan FSx untuk ONTAP menangguhkan akun Anda selama 90 hari sehingga data Anda tetap utuh. Jika Anda tidak membuka kembali akun selama 90 hari tersebut, AWS hapus data Anda termasuk data dalam SnapLock volume terlepas dari pengaturan retensi Anda.

Anda dapat menghapus volume SnapLock Perusahaan kapan saja jika Anda memiliki izin yang diperlukan. Untuk menghapus volume SnapLock Enterprise menggunakan ONTAP CLI, Anda harus memiliki peran. `fsxadmin` Untuk informasi selengkapnya, lihat [Peran administrator sistem file dan pengguna](#).

Untuk menghapus volume SnapLock Perusahaan yang berisi data WORM dengan kebijakan retensi aktif menggunakan FSx konsol Amazon, CLI, atau Amazon FSx API, Anda harus memiliki izin `fsx:BypassSnapLockEnterpriseRetention` IAM.

 Warning

Periode retensi minimum untuk volume log SnapLock audit adalah enam bulan. Sampai periode retensi ini berakhir, Anda tidak dapat menghapus volume log SnapLock audit, mesin virtual penyimpanan (SVM), atau sistem file yang terkait dengan SVM—meskipun volume dibuat dalam mode Enterprise. SnapLock Lihat informasi yang lebih lengkap di [SnapLockvolume log audit](#).

Membuat iSCSI LUN

Proses ini menjelaskan cara membuat iSCSI LUN di FSx NetApp Amazon untuk sistem file ONTAP menggunakan perintah CLI. NetApp ONTAP lun create Untuk informasi selengkapnya, lihat [lun create](#) di Pusat NetApp ONTAP Dokumentasi.

 Note

Protokol iSCSI tidak didukung untuk sistem file dengan lebih dari enam pasangan HA.

Proses ini mengasumsikan Anda sudah memiliki volume yang dibuat pada sistem file Anda. Untuk informasi selengkapnya, lihat [Membuat volume](#).

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Buat LUN menggunakan `lun create` NetApp CLI perintah, mengganti nilai-nilai berikut:
 - **svm_name**- Nama mesin virtual penyimpanan (SVM) yang menyediakan target iSCSI. Tuan rumah menggunakan nilai ini untuk mencapai LUN.
 - **vol_name**- Nama volume hosting LUN.
 - **lun_name**- Nama yang ingin Anda tetapkan ke LUN.
 - **size**- Ukuran, dalam byte, dari LUN. Ukuran maksimum LUN yang dapat Anda buat adalah 128 TB.

 Note

Kami menyarankan Anda menggunakan volume setidaknya 5% lebih besar dari ukuran LUN Anda. Margin ini menyisakan ruang untuk snapshot volume.

- **ostype**- Sistem operasi host, baik `windows_2008` atau `linux`. Gunakan `windows_2008` untuk semua versi Windows; ini memastikan LUN memiliki offset blok yang tepat untuk sistem operasi dan mengoptimalkan kinerja.

 Note

Sebaiknya aktifkan alokasi ruang pada LUN Anda. Dengan alokasi ruang diaktifkan, ONTAP dapat menginformasikan host Anda ketika LUN kehabisan kapasitas dan dapat merebut kembali ruang saat Anda menghapus data dari LUN.

Untuk informasi selengkapnya, lihat [lun create](#) di dokumentasi CLI NetApp ONTAP.

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
ostype ostype -space-allocation enabled
```

Created a LUN of size 10g (10737418240)

3. Konfirmasikan LUN dibuat, online, dan dipetakan.

```
> lun show
```

Sistem merespons dengan output berikut:

Vserver	Path	State	Mapped	Type	Size
<i>svm_name</i>	<i>/vol/vol_name/lun_name</i>	online	unmapped	windows_2008	10GB

Langkah selanjutnya

Sekarang setelah Anda membuat iSCSI LUN, langkah selanjutnya dalam proses menggunakan iSCSI LUN sebagai penyimpanan blok adalah memetakan LUN ke file. *igroup* Untuk informasi selengkapnya, lihat [Penyediaan iSCSI untuk Linux](#) atau [Penyediaan iSCSI untuk Windows](#).

Mengoptimalkan kinerja dengan jendela FSx pemeliharaan Amazon

Sebagai layanan yang dikelola sepenuhnya, FSx untuk ONTAP secara teratur melakukan pemeliharaan dan pembaruan ke sistem file Anda. Pemeliharaan ini tidak berdampak pada sebagian besar beban kerja. Untuk beban kerja yang sensitif terhadap kinerja, pada kesempatan langka Anda mungkin melihat dampak singkat (<60 detik) pada kinerja saat pemeliharaan terjadi; Amazon FSx memungkinkan Anda menggunakan jendela pemeliharaan untuk mengontrol kapan aktivitas pemeliharaan potensial tersebut terjadi.

Patching jarang terjadi, biasanya setiap beberapa minggu sekali. Saat penambalan terjadi, setiap server file sistem file Anda ditambah satu per satu, dan setiap server file biasanya membutuhkan waktu hingga satu jam untuk ditambah. Sebelum server file apa pun ditambah dalam pasangan HA, sistem file Anda secara otomatis gagal ke mitra HA server file, yang dapat mengakibatkan jeda I/O

singkat (kurang dari 60 detik) untuk setiap I/O yang diarahkan ke pasangan HA itu. Sistem file Anda kemudian akan gagal kembali, yang dapat mengakibatkan jeda I/O singkat lainnya (kurang dari 60 detik). Anda memilih waktu mulai jendela pemeliharaan selama pembuatan sistem file. Jika Anda tidak memilih jendela, satu secara otomatis ditetapkan.

 Important

Untuk memastikan bahwa sistem file Anda dapat berhasil ditambah, FSx untuk ONTAP akan membawa online volume offline apa pun selama proses penambalan. Volume apa pun yang FSx dibawa Amazon kembali online tidak akan dapat diakses oleh klien.

FSx untuk ONTAP memungkinkan Anda menyesuaikan jendela pemeliharaan sesuai kebutuhan untuk mengakomodasi beban kerja dan persyaratan operasional Anda. Anda dapat memindahkan jendela pemeliharaan sesering yang diperlukan, asalkan jendela pemeliharaan terjadi setidaknya sekali setiap 14 hari. Jika patch dilepaskan dan jendela pemeliharaan tidak terjadi dalam 14 hari, FSx untuk ONTAP akan melanjutkan pemeliharaan pada sistem file untuk memastikan keamanan dan keandalannya.

 Note

Untuk memastikan integritas data selama aktivitas pemeliharaan, FSx untuk ONTAP menutup semua kunci oportunistik dan menyelesaikan operasi penulisan yang tertunda ke volume penyimpanan dasar yang menghosting sistem file Anda sebelum pemeliharaan dimulai.

Anda dapat menggunakan Amazon FSx Management Console AWS CLI, AWS API, atau salah satu AWS SDKs untuk mengubah jendela pemeliharaan sistem file Anda.

Untuk mengubah jendela (konsol) pemeliharaan mingguan

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. Halaman detail sistem file Ringkasan 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 sistem file.

Untuk mengubah jendela pemeliharaan mingguan menggunakan perintah [update-file-system](#) CLI, lihat [Untuk memperbarui sistem file \(CLI\)](#)

Mengelola kapasitas throughput

FSx untuk ONTAP mengonfigurasi kapasitas throughput saat Anda membuat sistem file. Anda dapat memodifikasi kapasitas throughput sistem file Anda kapan saja. Perlu diingat bahwa sistem file Anda memerlukan konfigurasi khusus untuk mencapai jumlah maksimum kapasitas throughput. Misalnya, untuk menyediakan 4 GBps kapasitas throughput untuk sistem file generasi pertama, sistem file Anda memerlukan konfigurasi dengan kapasitas penyimpanan SSD minimal 5.120 GiB dan 160.000 IOPS SSD. Untuk informasi selengkapnya, lihat [Dampak kapasitas throughput terhadap performa](#).

Kapasitas throughput adalah salah satu faktor yang menentukan kecepatan di mana server file yang menghosting sistem file dapat melayani data file. Tingkat kapasitas throughput yang lebih tinggi datang dengan tingkat jaringan yang lebih tinggi, operasi I/O baca disk per detik (IOPS), dan kapasitas caching data pada server file. Untuk informasi selengkapnya, lihat [Performa](#).

Saat Anda memodifikasi kapasitas throughput sistem file Anda, Amazon FSx mengganti server file yang memberi daya pada sistem file Anda. Sistem file Single-AZ dan Multi-AZ mengalami failover dan failback otomatis selama proses ini, yang biasanya membutuhkan waktu beberapa menit untuk menyelesaikannya. Proses failover dan failback transparan untuk klien NFS (Network File Sharing), SMB (Server Message Block), dan iSCSI (Internet Small Computer Systems Interface), memungkinkan beban kerja Anda terus berjalan tanpa gangguan atau intervensi manual. Anda ditagih untuk jumlah kapasitas throughput baru setelah tersedia untuk sistem file Anda.

Note

Untuk memastikan integritas data selama aktivitas pemeliharaan, FSx untuk ONTAP menutup semua kunci oportunistik dan menyelesaikan operasi penulisan yang tertunda ke volume penyimpanan yang mendasari yang menghosting sistem file Anda sebelum pemeliharaan dimulai. Selama jendela pemeliharaan sistem file terjadwal, modifikasi sistem (seperti modifikasi kapasitas throughput Anda) mungkin tertunda. Pemeliharaan sistem dapat

menyebabkan perubahan ini mengantri hingga diproses. Untuk informasi selengkapnya, lihat [the section called “Memperbarui jendela pemeliharaan”](#).

Topik

- [Kapan harus mengubah kapasitas throughput](#)
- [Bagaimana permintaan bersamaan ditangani](#)
- [Memperbarui kapasitas throughput](#)
- [Memantau perubahan kapasitas throughput pada konsol](#)

Kapan harus mengubah kapasitas throughput

Amazon FSx terintegrasi dengan Amazon CloudWatch, yang membantu Anda memantau tingkat penggunaan throughput sistem file yang sedang berlangsung. Kinerja throughput dan IOPS yang dapat Anda dorong melalui sistem file tergantung pada karakteristik beban kerja spesifik Anda, selain kapasitas throughput sistem file Anda. Sebagai aturan, Anda harus menyediakan kapasitas throughput yang cukup untuk mendukung throughput baca beban kerja Anda ditambah dua kali throughput penulisan beban kerja Anda. Anda dapat menggunakan CloudWatch metrik untuk menentukan dimensi mana yang akan diubah untuk meningkatkan kinerja. Untuk informasi selengkapnya, lihat [the section called “Pemantauan di FSx konsol Amazon”](#).

Bagaimana permintaan bersamaan ditangani

Untuk sistem file generasi pertama, Anda dapat meminta pembaruan kapasitas throughput tepat sebelum kapasitas penyimpanan SSD dan alur kerja pembaruan IOPS yang disediakan dimulai atau saat sedang berlangsung. Urutan bagaimana Amazon FSx menangani dua permintaan adalah sebagai berikut:

- Jika Anda mengirimkan SSD/IOPS update and throughput capacity update at the same time, both requests are accepted. The SSD/IOPS pembaruan diprioritaskan sebelum pembaruan kapasitas throughput.
- Jika Anda mengirimkan pembaruan kapasitas throughput saat diperbarui (nilai baru tersedia) dan selama langkah pengoptimalan. SSD/IOPS update is in progress, the throughput capacity update request is accepted and queued to occur after the SSD/IOPS update. The throughput capacity update starts after SSD/IOPS. Ini biasanya memakan waktu kurang dari 10 menit.

- Jika Anda mengirimkan permintaan pembaruan SSD/IOPS update while a throughput capacity update is in progress, the SSD/IOPS penyimpanan diterima dan diantrian untuk memulai setelah pembaruan kapasitas throughput selesai (kapasitas throughput baru tersedia). Ini biasanya memakan waktu 20 menit.

Pertimbangkan poin-poin berikut saat meminta pembaruan kapasitas throughput untuk sistem file generasi kedua:

- Anda harus menunggu minimal enam jam antara memperbarui kapasitas throughput untuk sistem file generasi kedua.
- Periode cooldown kapasitas throughput dibagi dengan penskalaan SSD/IOPS.
- Penskalaan kapasitas throughput dan penskalaan SSD/IOPS tidak dapat dilakukan secara simulasi atau antri saat keduanya sedang berlangsung.
- Anda tidak dapat menambahkan pasangan ketersediaan tinggi (HA) bersamaan dengan atau saat penskalaan kapasitas throughput atau penskalaan dan penskalaan kapasitas throughput SSD/IOPS scaling are in progress. However, adding HA pairs doesn't share a cooldown with SSD/IOPS. Untuk informasi selengkapnya, lihat [Menambahkan pasangan ketersediaan tinggi \(HA\)](#).

Untuk informasi selengkapnya tentang penyimpanan SSD dan pembaruan IOPS yang disediakan, lihat [Mengelola kapasitas penyimpanan](#)

Memperbarui kapasitas throughput

Anda dapat mengubah kapasitas throughput sistem file menggunakan FSx konsol Amazon, AWS Command Line Interface (AWS CLI), atau Amazon FSx API.

Note

Anda harus menunggu minimal enam jam antara memperbarui kapasitas throughput untuk sistem file generasi kedua.

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 ONTAP yang ingin Anda tingkatkan kapasitas throughputnya.

3. Untuk Tindakan, pilih Perbarui kapasitas throughput. Atau, pada panel Ringkasan, pilih Perbarui di samping Kapasitas throughput pada sistem file.
4. Pilih nilai baru untuk Kapasitas throughput dari daftar.
5. Pilih Perbarui untuk memulai pembaruan kapasitas throughput.
6. Anda dapat memantau kemajuan pembaruan pada halaman detail 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 perubahan kapasitas throughput pada konsol](#).

Untuk mengubah kapasitas throughput sistem file (CLI)

Untuk memodifikasi 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` untuk nilai yang diinginkan untuk memperbarui properti sistem file.

Anda dapat memantau kemajuan pembaruan dengan menggunakan FSx konsol Amazon, the AWS CLI, dan API. Untuk informasi selengkapnya, lihat [Memantau perubahan kapasitas throughput pada konsol](#).

Memantau perubahan kapasitas throughput pada konsol

Anda dapat memantau kemajuan modifikasi kapasitas throughput menggunakan FSx konsol Amazon, API, dan AWS CLI

Memantau perubahan kapasitas throughput pada konsol

Pada tab Pembaruan di jendela Rincian sistem file, Anda dapat melihat 10 tindakan pembaruan terbaru untuk setiap jenis tindakan pembaruan.

Untuk melakukan tindakan pembaruan kapasitas throughput, Anda dapat melihat informasi berikut.

Jenis pembaruan

Jenis yang didukung adalah Kapasitas throughput, Kapasitas penyimpanan, dan Optimisasi penyimpanan.

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.
- 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 ketika 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-systems](#) CLI 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 128 MBps, dan kapasitas throughput target 256. MBps

```
.  
.   
.   
  "ThroughputCapacity": 128,  
  "AdministrativeActions": [
```



```

{
  "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
  "RequestTime": 1581694764.757,
  "Status": "PENDING",
  "TargetFileSystemValues": {
    "OntapConfiguration": {
      "ThroughputCapacity": 256
    }
  }
}
]

```

Saat Amazon berhasil FSx 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": {
        "OntapConfiguration": {
          "ThroughputCapacity": 256
        }
      }
    }
  ]
]

```

Jika perubahan kapasitas throughput gagal, statusnya berubah menjadi **FAILED**, dan properti **FailureDetails** memberikan informasi tentang kegagalan tersebut.

Mengelola saham SMB

Untuk mengelola berbagi file SMB di sistem FSx file Amazon Anda, Anda dapat menggunakan GUI Folder Bersama Microsoft Windows. GUI Folder Bersama menyediakan lokasi pusat untuk mengelola

semua folder bersama di mesin virtual penyimpanan (SVM) Anda. Prosedur berikut merinci cara membuat, memperbarui, dan menghapus berbagi file Anda.

 Note

Anda juga dapat mengelola berbagi file SMB dengan menggunakan Manajer NetApp Sistem. Untuk informasi selengkapnya, lihat [Menggunakan NetApp System Manager dengan NetApp Console](#).

Untuk menghubungkan folder bersama ke sistem FSx file Amazon Anda

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. Untuk informasi selengkapnya, lihat [Menghubungkan ke Instans Windows Anda](#) di Panduan EC2 Pengguna Amazon.
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 DNS untuk mesin virtual penyimpanan Anda (SVM), misalnya, **netbios_name.corp.example.com**

Untuk menemukan nama DNS SVM Anda di FSx konsol Amazon, pilih Storage virtual machines, pilih SVM Anda, lalu gulir ke bawah ke Endpoints hingga Anda menemukan nama SMB DNS. Anda juga bisa mendapatkan nama DNS sebagai respons operasi [DescribeStorageVirtualMachinesAPI](#).

6. Pilih OK. 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 dengan tindakan berikut:

 Note

Kami menyarankan Anda menemukan saham SMB Anda pada volume selain volume root Anda.

- Buat berbagi file baru — Di alat Folder Bersama, pilih Berbagi di panel kiri untuk melihat pembagian aktif untuk sistem FSx file Amazon Anda. Volume ditampilkan dipasang pada jalur yang dipilih selama pembuatan volume. 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: pilih Jelajahi saat menentukan jalur folder lokal, pilih Buat folder baru untuk membuat folder lokal.
- Menggunakan baris perintah:

```
New-Item -Type Directory -Path \\netbios_name.corp.example.com\C  
$volume_path\MyNewFolder
```

- 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

Menghapus berbagi file dari GUI hanya mungkin jika Anda terhubung ke fsmgmt.msc menggunakan nama DNS dari sistem file Amazon. FSx Jika Anda terhubung menggunakan alamat IP atau nama alias DNS dari sistem file, opsi Berhenti Berbagi tidak akan bekerja dan pembagian file tidak akan dihapus.

Mengelola FSx sumber daya ONTAP menggunakan aplikasi NetApp

Selain Konsol Manajemen AWS,, dan AWS API dan AWS CLI SDKs, Anda juga dapat menggunakan alat dan aplikasi NetApp manajemen ini untuk mengelola sumber daya ONTAP Anda FSx :

Topik

- [Mendaftar untuk NetApp akun](#)
- [Menggunakan NetApp Console](#)
- [Menggunakan CLI NetApp ONTAP](#)
- [Menggunakan ONTAP REST API](#)

Important

Amazon FSx secara berkala menyinkronkan dengan ONTAP untuk memastikan konsistensi. Jika Anda membuat atau memodifikasi volume menggunakan NetApp aplikasi, mungkin diperlukan waktu hingga beberapa menit agar perubahan ini tercermin dalam Konsol Manajemen AWS,, API AWS CLI, dan SDKs.

Mendaftar untuk NetApp akun

Untuk mengunduh beberapa NetApp perangkat lunak, seperti NetApp Console, SnapCenter, dan konektor ONTAP Antivirus, Anda harus memiliki NetApp akun. Untuk mendaftar NetApp akun, lakukan langkah-langkah berikut:

1. Buka halaman [Pendaftaran NetApp Pengguna](#) dan daftar untuk akun NetApp pengguna baru.
2. Lengkapi formulir dengan informasi Anda. Pastikan untuk memilih tingkat akses NetApp Customer/End pengguna. Di bidang SERIAL NUMBER, salin dan tempel ID Sistem File untuk sistem file ONTAP Anda FSx . Lihat contoh berikut ini:

USER ACCESS LEVEL

- ☐ Guest User ☒ NetApp Customer / End User
- ☐ NetApp Reseller / Service Provider / System Integrator / Partner

Product Information (Optional)

Please enter a Serial Number or System ID to help us validate your access level.

Please note: Not providing a Serial Number or System ID may delay processing of your request.

SERIAL NUMBER

fs-0de9123abcf12368a

(Either a NetApp hardware Serial Number, often located on back of unit; or a NetApp software Serial Number.)

OR

SYSTEM ID

(Run a "sysconfig -a" command on your NetApp product. The output should list the System ID.)

NETAPP TOKEN

Apa yang diharapkan setelah Anda mendaftar

Pelanggan dengan NetApp produk yang sudah ada akan memiliki akun NSS mereka naik level ke akses Tingkat Pelanggan dalam satu hari kerja. Pelanggan baru NetApp akan onboard menggunakan praktik bisnis standar, selain memiliki akun NSS mereka yang ditingkatkan ke akses Tingkat Pelanggan. Menyediakan ID Sistem File membantu mempercepat proses ini. Anda dapat memeriksa status akun NSS Anda dengan masuk ke mysupport.netapp.com dan menavigasi ke halaman Selamat Datang. Tingkat akses akun Anda harus Akses Pelanggan.

Menggunakan NetApp Console

NetApp Console (sebelumnya NetApp BlueXP) adalah bidang kontrol terpadu yang menyederhanakan pengalaman manajemen untuk penyimpanan dan layanan data di lingkungan lokal dan cloud. NetApp Console menyediakan antarmuka pengguna terpusat untuk mengelola, memantau, dan mengotomatiskan penerapan ONTAP di dalam dan di tempat. AWS Untuk informasi

selengkapnya, lihat [dokumentasi NetApp Konsol](#) dan [dokumentasi pengelolaan Amazon FSx untuk NetApp ONTAP](#).

 Note

NetApp Console tidak didukung untuk sistem file generasi kedua dengan lebih dari satu pasangan ketersediaan tinggi (HA).

Menggunakan NetApp System Manager dengan NetApp Console

Anda dapat mengelola Amazon FSx untuk sistem file NetApp ONTAP menggunakan System Manager langsung dari NetApp Console. NetApp Console memungkinkan Anda menggunakan antarmuka Manajer Sistem yang sama dengan yang biasa Anda gunakan, sehingga Anda dapat mengelola infrastruktur multi-cloud hybrid Anda dari satu bidang kontrol. Anda juga memiliki akses ke fungsionalitas NetApp Konsol lainnya. Untuk informasi selengkapnya, lihat topik [Integrasikan Pengelola Sistem ONTAP dengan NetApp Konsol](#) di dokumentasi NetApp ONTAP.

 Note

NetApp Manajer Sistem tidak didukung untuk sistem file generasi kedua dengan lebih dari satu pasangan HA.

Menggunakan CLI NetApp ONTAP

Anda dapat mengelola Amazon FSx untuk sumber daya NetApp ONTAP menggunakan NetApp ONTAP CLI. Anda dapat mengelola sumber daya di tingkat sistem file (analog dengan cluster NetApp ONTAP), dan pada tingkat SVM.

Mengelola sistem file dengan ONTAP CLI

Anda dapat menjalankan perintah ONTAP CLI pada sistem file FSx ONTAP Anda, mirip dengan menjalankannya di cluster. NetApp ONTAP Anda mengakses ONTAP CLI pada sistem file Anda dengan membuat koneksi shell aman (SSH) ke titik akhir manajemen sistem file, dan masuk dengan nama pengguna dan kata sandi. `fsxadmin` Anda memiliki opsi untuk mengatur `fsxadmin` kata sandi saat membuat sistem file menggunakan [alur pembuatan kustom](#) atau menggunakan file AWS CLI. Jika Anda membuat sistem file menggunakan opsi Quick create, `fsxadmin` kata sandi tidak

disetel, jadi Anda harus mengaturnya untuk masuk ke ONTAP CLI. Untuk informasi selengkapnya tentang pengaturan sistem file `fsxadmin`, kata sandi, lihat [Memperbarui sistem file](#). Anda dapat menemukan nama DNS dan alamat IP titik akhir manajemen sistem file Anda di FSx konsol Amazon, di tab Administrasi halaman detail sistem file FSx untuk ONTAP.

Untuk terhubung ke endpoint manajemen sistem file dengan SSH, pertama-tama masuk ke EC2 instance di VPC yang sama dengan sistem file ONTAP FSx untuk. Setelah Anda masuk ke EC2 instance, gunakan `fsxadmin` pengguna dan kata sandi untuk SSH ke alamat IP endpoint manajemen sistem file atau nama DNS, seperti pada contoh berikut.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

Perintah SSH dengan nilai sampel:

```
ec2user $ ssh fsxadmin@198.51.100.0
```

Perintah SSH menggunakan nama DNS endpoint manajemen:

```
ec2user $ ssh fsxadmin@file-system-management-endpoint-dns-name
```

Perintah SSH menggunakan contoh nama DNS:

```
ec2user $ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com  
Password: fsxadmin_password
```

```
This is your first recorded login.  
FsxId0abcdef123456789::>
```

Lingkup perintah ONTAP CLI tersedia untuk **fsxadmin**

Tampilan administratif berada pada tingkat sistem file, yang mencakup semua SVMs dan volume dalam sistem file. `fsxadmin` melakukan peran administrator ONTAP cluster. Karena Amazon FSx untuk sistem file NetApp ONTAP sepenuhnya dikelola, `fsxadmin` peran dapat menjalankan subset dari perintah CLI yang tersedia ONTAP.

Untuk melihat daftar perintah yang `fsxadmin` dapat dijalankan, gunakan perintah [security login role show](#) ONTAP CLI berikut:

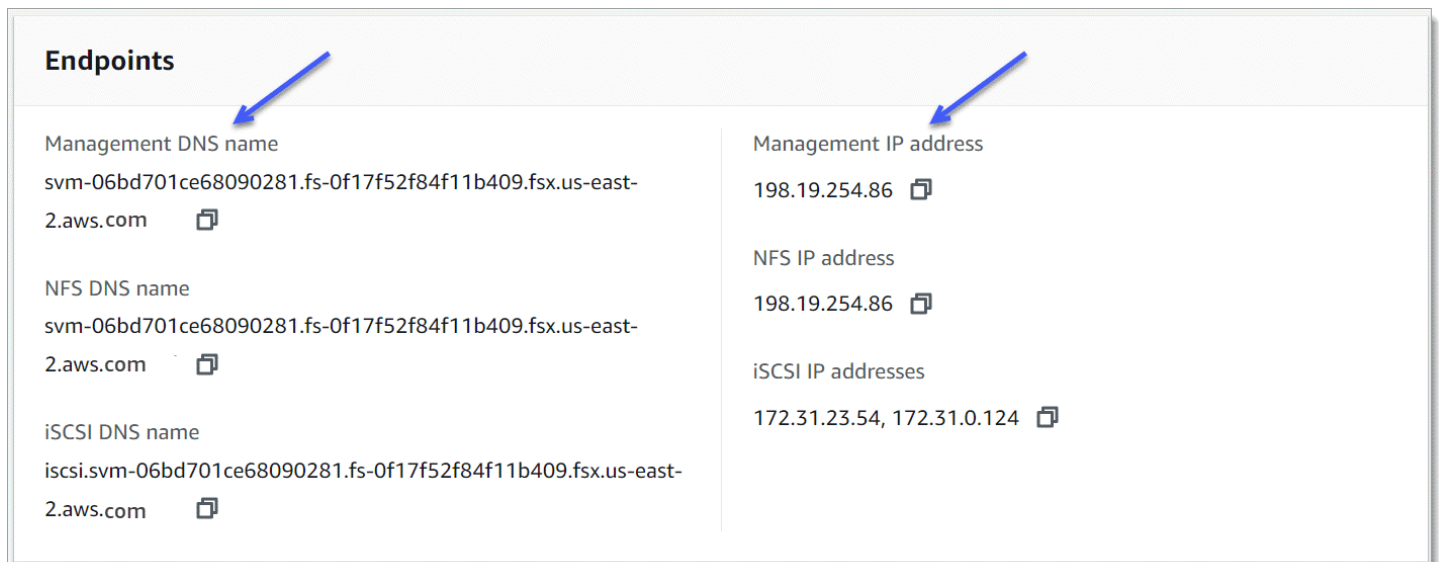
```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
```

Vserver	Role Name	Command/Directory	Query	Access Level

FsxId0abcdef123456789	fsxadmin	application		all
		cluster application-record		all
		cluster date show		readonly
		cluster ha modify		readonly
		cluster ha show		readonly
		cluster identity modify		readonly
		cluster identity show		readonly
		cluster log-forwarding	-port !55555	all
		cluster modify		readonly
		cluster peer		all
		cluster show		readonly
		cluster statistics show		readonly
		cluster time-service ntp server create		readonly
		cluster time-service ntp server delete		readonly
		cluster time-service ntp server modify		readonly
		cluster time-service ntp server show		readonly
		debug network tcpdump	-ip space !Cluster	all
		debug san lun		all
		df	-vserver !FsxId* -vserver !Cluster	readonly
		echo		all
		event catalog show		readonly
		event config		all
.				
.				
.				
378 entries were displayed.				

Mengelola SVMs dengan ONTAP CLI

Anda dapat mengakses ONTAP CLI di SVM Anda dengan membuat koneksi shell aman (SSH) ke titik akhir manajemen SVM menggunakan nama pengguna dan kata sandi. `vsadmin` Anda dapat menemukan nama DNS endpoint manajemen SVM dan alamat IP di FSx konsol Amazon, di panel Endpoints pada halaman detail mesin virtual Penyimpanan, yang ditunjukkan pada grafik berikut.



Endpoints	
Management DNS name svm-06bd701ce68090281.fs-0f17f52f84f11b409.fsx.us-east-2.aws.com	Management IP address 198.19.254.86
NFS DNS name svm-06bd701ce68090281.fs-0f17f52f84f11b409.fsx.us-east-2.aws.com	NFS IP address 198.19.254.86
iSCSI DNS name iscsi.svm-06bd701ce68090281.fs-0f17f52f84f11b409.fsx.us-east-2.aws.com	iSCSI IP addresses 172.31.23.54, 172.31.0.124

Untuk terhubung ke titik akhir manajemen SVM dengan SSH, Anda dapat menggunakan nama pengguna dan `vsadmin` kata sandi. Jika Anda tidak menetapkan kata sandi untuk `vsadmin` pengguna saat SVM dibuat, Anda dapat mengatur `vsadmin` kata sandi kapan saja. Untuk informasi selengkapnya, lihat [Memperbarui penyimpanan mesin virtual \(SVM\)](#). Anda dapat SSH ke SVM dari klien yang berada di VPC yang sama dengan sistem file, menggunakan alamat IP endpoint manajemen atau nama DNS.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

Perintah dengan nilai sampel:

```
ssh vsadmin@198.51.100.10
```

Perintah SSH menggunakan nama DNS endpoint manajemen:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

Perintah SSH menggunakan contoh nama DNS:

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

Password: *vsadmin-password*

```
This is your first recorded login.  
FsxId0abcdef123456789::>
```

Amazon FSx untuk NetApp ONTAP mendukung perintah NetApp ONTAP CLI.

Untuk referensi lengkap perintah NetApp ONTAP CLI, lihat Perintah [ONTAP: Referensi Halaman Manual](#).

Menggunakan ONTAP REST API

Saat mengakses sistem file ONTAP Anda FSx menggunakan ONTAP REST API menggunakan fsxadmin kredensial, lakukan salah satu hal berikut:

- Nonaktifkan validasi TLS.

Atau

- Percayai otoritas AWS sertifikat (CAs) - Bundel sertifikat untuk CAs di setiap wilayah dapat ditemukan di berikut ini URLs:
 - <https://fsx-aws-certificates.s3.amazonaws.com/bundle-.pem> untuk *aws-region* Publik Wilayah AWS
 - <https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle-.pem> untuk Wilayah *aws-region* AWS GovCloud
 - [https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-*aws-region*.pem](https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-aws-region.pem) untuk Wilayah Tiongkok AWS

Untuk referensi lengkap perintah NetApp ONTAP REST API, lihat [Referensi Online NetApp ONTAP REST API](#).

Menandai sumber daya Amazon FSx

Untuk membantu mengelola sistem file dan FSx sumber daya Amazon lainnya, Anda dapat menetapkan metadata Anda sendiri ke setiap sumber daya dalam bentuk tag. Dengan tag, Anda dapat mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Kategorisasi ini berguna ketika Anda memiliki banyak sumber daya dari jenis yang sama—Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang telah Anda tetapkan padanya. Topik ini menjelaskan tag dan menunjukkan cara membuatnya.

Topik

- [Dasar-dasar tag](#)
- [Pemberian tag pada sumber daya Anda](#)
- [Menyalin tag ke cadangan](#)
- [Batasan tag](#)
- [Izin dan penandaan](#)

Dasar-dasar tag

Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tag terdiri dari dua bagian yang Anda tentukan:

- Sebuah kunci tag (misalnya, CostCenter, Environment, atau Project). Kunci tag peka huruf besar dan kecil.
- Nilai tag (misalnya, 111122223333 atau Production). Seperti kunci tag, nilai tag peka huruf besar dan kecil. Nilai tag adalah opsional.

Anda dapat menggunakan tag untuk mengkategorikan AWS sumber daya Anda dengan berbagai cara, seperti, berdasarkan tujuan, pemilik, atau lingkungan. Misalnya, Anda dapat menentukan satu set tag untuk sistem FSx file Amazon akun Anda yang membantu Anda melacak setiap pemilik instans dan tingkat tumpukan.

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 [Menandai AWS sumber daya](#) di. Referensi Umum AWS

Beberapa perilaku penandaan yang perlu diingat:

- Tag tidak memiliki arti semantik ke Amazon FSx dan ditafsirkan secara ketat sebagai serangkaian karakter.
- Selain itu, tanda tidak dapat menetapkan secara otomatis ke sumber daya Anda.

- Anda dapat mengedit kunci dan nilai tanda, dan Anda dapat menghapus tanda dari sumber daya kapan pun.
- Anda dapat mengatur nilai tag ke string kosong, tetapi Anda tidak dapat mengatur nilai tag ke null.
- Jika Anda menambahkan tanda yang memiliki kunci yang sama dengan tanda yang sudah ada di sumber daya tersebut, nilai baru akan menimpa nilai lama.
- Jika sumber daya dihapus, semua tanda untuk sumber daya tersebut juga akan dihapus.
- Jika Anda menggunakan Amazon FSx API, the AWS Command Line Interface (AWS CLI), atau AWS SDK, Anda dapat melakukan hal berikut:
 - Anda dapat menggunakan tindakan TagResource API untuk menerapkan tag ke sumber daya yang ada.
 - Untuk beberapa tindakan pembuatan sumber daya, Anda dapat menentukan tag untuk sumber daya saat sumber daya dibuat. Dengan memberikan tag pada sumber daya saat pembuatan, Anda tidak perlu menjalankan skrip pemberian tag kustom setelah pembuatan sumber daya.

Jika tag tidak dapat diterapkan selama pembuatan sumber daya, FSx Amazon mengembalikan proses pembuatan sumber daya. Perilaku ini membantu memastikan bahwa sumber daya dibuat dengan tag atau tidak dibuat sama sekali, dan tidak ada sumber daya yang dibiarkan tanpa tag kapan saja.

Note

Izin tertentu AWS Identity and Access Management (IAM) diperlukan bagi pengguna untuk menandai sumber daya pada pembuatan. Untuk informasi selengkapnya, 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 Amazon 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. Namun, meskipun konsol mengatur sumber daya sesuai dengan kunci Nama, kunci ini tidak memiliki arti semantik apa pun untuk layanan Amazon. FSx

Untuk menerapkan kontrol terperinci atas pengguna dan grup yang dapat menandai sumber daya saat pembuatan, Anda dapat menerapkan izin tingkat sumber daya berbasis tag dalam kebijakan IAM Anda ke tindakan Amazon FSx API yang mendukung penandaan saat pembuatan. Dengan menggunakan izin tersebut dalam kebijakan Anda, Anda mendapatkan manfaat berikut:

- Sumber daya Anda diamankan dengan benar dari penciptaan.
- Karena tag diterapkan segera ke sumber daya Anda, izin tingkat sumber daya berbasis tag yang mengendalikan penggunaan sumber daya segera efektif.
- 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.

Untuk mengontrol kunci tag dan nilai yang ditetapkan pada sumber daya yang ada, Anda dapat menerapkan izin tingkat sumber daya ke tindakan FSx API TagResource Amazon dan UntagResource Amazon dalam kebijakan IAM Anda.

Untuk informasi selengkapnya tentang izin yang diperlukan untuk menandai FSx sumber daya Amazon saat pembuatan, lihat [Memberikan 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](#)

Untuk informasi tentang menandai sumber daya Anda untuk penagihan, lihat [Menggunakan tag alokasi biaya di Panduan Pengguna AWS Billing](#)

Menyalin tag ke cadangan

Saat Anda membuat atau memperbarui volume di Amazon FSx API atau AWS CLI, Anda dapat mengaktifkan CopyTagsToBackups untuk secara otomatis menyalin tag apa pun dari volume Anda ke cadangan.

Note

Jika Anda menentukan tag saat membuat cadangan yang dimulai pengguna (termasuk tag nama saat Anda membuat cadangan menggunakan FSx konsol Amazon), tag tidak akan disalin dari volume meskipun Anda telah mengaktifkannya. CopyTagsToBackups

Untuk informasi selengkapnya tentang pencadangan, lihat [Melindungi data Anda dengan backup volume](#). Untuk informasi selengkapnya tentang mengaktifkan CopyTagsToBackups, lihat [Untuk membuat volume \(CLI\)](#) dan [Untuk memperbarui konfigurasi volume \(CLI\)](#) di Amazon FSx untuk Panduan Pengguna NetApp ONTAP atau [CreateVolume](#) dan [UpdateVolume](#) di Referensi API Amazon FSx untuk NetApp ONTAP.

Batasan tag

Batasan dasar berikut berlaku untuk tag:

- Jumlah maksimum tag per sumber daya adalah 50.
- Panjang kunci maksimum adalah 128 karakter Unicode di UTF-8.
- Panjang nilai maksimum adalah 256 karakter Unicode di UTF-8.
- Karakter yang diizinkan adalah huruf, angka, dan spasi yang dapat direpresentasikan dalam UTF-8, dan karakter berikut: + - (tanda hubung) (garis bawah). = . _ : / @
- Untuk setiap sumber daya, setiap kunci tag harus unik, dan setiap kunci tag hanya dapat memiliki satu nilai.
- Kunci dan nilai tanda peka huruf besar-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. 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 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 dan penandaan

Untuk informasi selengkapnya tentang izin yang diperlukan untuk menandai FSx sumber daya Amazon saat pembuatan, lihat [Memberikan 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](#)

Melindungi data Anda

Selain secara otomatis mereplikasi data sistem file Anda untuk memastikan [daya tahan tinggi](#), dengan Amazon FSx Anda juga memiliki opsi berikut yang dapat Anda gunakan untuk lebih melindungi data Anda:

- Pencadangan FSx volume Amazon asli yang mendukung retensi cadangan dan kebutuhan kepatuhan Anda di Amazon. FSx
- Menggunakan AWS Backup untuk menerapkan strategi pencadangan dan retensi otomatis yang dikelola secara terpusat di beberapa Layanan AWS.
- Snapshot yang memungkinkan pengguna Anda untuk dengan mudah membatalkan perubahan file yang tidak diinginkan, dengan memulihkan file ke versi sebelumnya.
- Gunakan SnapLock untuk membuat tulis sekali, baca banyak volume penyimpanan (WORM) untuk mencegah modifikasi atau penghapusan file setelah dilakukan, untuk periode retensi tertentu.
- FlexCachevolume menawarkan penyimpanan yang efisien, hemat biaya, replikasi data berkinerja tinggi untuk beban kerja baca-berat dengan data yang sebagian besar tetap tidak berubah.
- Gunakan SnapMirror untuk membuat replikasi sistem file otomatis terjadwal ke sistem file kedua untuk perlindungan data dan pemulihan bencana.

Topik

- [Melindungi data Anda dengan backup volume](#)
- [Melindungi data Anda dengan snapshot](#)
- [Melindungi data Anda dengan Autonomous Ransomware Protection](#)
- [Melindungi data Anda dengan SnapLock](#)
- [Mereplikasi data Anda dengan FlexCache](#)
- [Mereplikasi data Anda menggunakan NetApp SnapMirror](#)

Melindungi data Anda dengan backup volume

Dengan FSx untuk ONTAP, Anda dapat melindungi data Anda dengan mengambil cadangan harian otomatis dan pencadangan volume yang diprakarsai pengguna pada sistem file Anda. Membuat cadangan rutin untuk volume Anda adalah praktik terbaik yang membantu mendukung retensi data dan kebutuhan kepatuhan Anda. Anda dapat mengembalikan cadangan volume ke yang ada FSx

untuk sistem file ONTAP yang dapat Anda akses ke yang sama di Wilayah AWS mana cadangan disimpan. Bekerja dengan FSx cadangan Amazon membuatnya mudah untuk membuat, melihat, memulihkan, dan menghapus cadangan volume Anda.

Amazon FSx mendukung backup ONTAP volume dengan read-write (RW). `OntapVolumeType`

 Note

Amazon FSx tidak mendukung pencadangan volume perlindungan data (DP), volume load sharing mirror (LSM), atau volume tujuan untuk dan. FlexCache SnapMirror

Topik

- [Cara kerja backup](#)
- [Persyaratan penyimpanan](#)
- [Pencadangan harian otomatis](#)
- [Pencadangan yang diprakarsai pengguna](#)
- [Menyalin tag ke cadangan](#)
- [Menggunakan AWS Backup dengan Amazon FSx](#)
- [Memulihkan backup ke volume baru](#)
- [Backup dan pulihkan kinerja](#)
- [Mencadangkan volume SnapLock](#)
- [Membuat backup yang diinisiasi pengguna](#)
- [Memulihkan cadangan ke volume baru](#)
- [Memulihkan subset data](#)
- [Memantau kemajuan saat memulihkan cadangan](#)
- [Menghapus cadangan](#)

Cara kerja backup

Semua FSx cadangan Amazon (pencadangan harian otomatis dan pencadangan yang diprakarsai pengguna) bersifat inkremental, yang berarti bahwa mereka hanya menyimpan perubahan dalam data sejak pencadangan sebelumnya selesai. Ini meminimalkan waktu yang diperlukan untuk membuat cadangan dan jumlah penyimpanan yang digunakan oleh setiap cadangan. Pencadangan tambahan mengoptimalkan biaya penyimpanan dengan tidak menyimpan data duplikat. FSx untuk

cadangan ONTAP adalah per volume, dengan setiap cadangan hanya berisi data dari satu volume tertentu. FSx Cadangan Amazon disimpan secara berlebihan di beberapa Availability Zone untuk mencapai daya tahan tinggi.

FSx Pencadangan Amazon menggunakan snapshot — point-in-time, gambar hanya-baca volume Anda — untuk mempertahankan peningkatan antar cadangan. Setiap kali cadangan diambil, Amazon FSx pertama-tama mengambil snapshot volume Anda. Snapshot cadangan disimpan dalam volume Anda, dan menghabiskan ruang penyimpanan pada volume. Amazon FSx kemudian membandingkan snapshot ini dengan snapshot cadangan sebelumnya (jika ada) dan hanya menyalin data yang diubah ke cadangan Anda.

Jika tidak ada snapshot cadangan sebelumnya, maka seluruh konten snapshot cadangan terbaru disalin ke cadangan Anda. Setelah snapshot cadangan terbaru berhasil diambil, Amazon FSx menghapus snapshot cadangan sebelumnya. Snapshot yang digunakan untuk cadangan terbaru tetap ada di volume Anda hingga cadangan berikutnya diambil, saat proses berulang. Untuk mengoptimalkan biaya penyimpanan cadangan, ONTAP menjaga penghematan efisiensi penyimpanan volume dalam cadangannya.

Saat Anda [menghapus](#) cadangan, hanya data unik untuk cadangan itu yang dihapus. Setiap FSx cadangan Amazon berisi semua informasi yang diperlukan untuk membuat volume baru dari cadangan, secara efektif memulihkan point-in-time snapshot volume.

Ada batasan jumlah cadangan yang dapat Anda simpan per Akun AWS dan per volume. Untuk informasi selengkapnya, lihat [Kuota yang dapat Anda tingkatkan](#) dan [Kuota sumber daya untuk setiap sistem file](#).

Persyaratan penyimpanan

Volume dan sistem file Anda masing-masing harus memiliki kapasitas penyimpanan SSD yang cukup untuk menyimpan snapshot cadangan. Saat mengambil snapshot cadangan, kapasitas penyimpanan tambahan yang dikonsumsi oleh snapshot tidak dapat menyebabkan volume melebihi 98% pemanfaatan penyimpanan SSD. Jika ini terjadi, cadangan akan gagal. Anda dapat [meningkatkan penyimpanan SSD volume](#) atau [sistem file](#) kapan saja untuk memastikan bahwa cadangan Anda tidak akan terganggu.

Pencadangan harian otomatis

Saat Anda membuat sistem file, backup harian otomatis diaktifkan secara default untuk volume sistem file Anda. Anda dapat mengaktifkan atau menonaktifkan backup harian otomatis untuk sistem file yang ada kapan saja. Pencadangan harian otomatis untuk semua volume terjadi selama jendela

cadangan harian sistem file, yang secara otomatis diatur saat Anda membuat sistem file. Anda dapat memodifikasi jendela cadangan harian kapan saja. Untuk [kinerja pencadangan](#) yang optimal, kami sarankan Anda memilih jendela cadangan harian yang berada di luar jam operasi normal ketika klien dan aplikasi mengakses data pada volume Anda.

Dengan menggunakan konsol, Anda dapat mengatur periode retensi untuk pencadangan harian otomatis ke nilai dari 1 hingga 90 hari saat membuat sistem file atau kapan saja. Periode retensi cadangan harian otomatis default adalah 30 hari. Amazon FSx menghapus cadangan harian otomatis setelah periode retensi berakhir. Dengan menggunakan API AWS CLI dan, Anda dapat mengatur periode retensi ke nilai dari 0 hingga 90 hari; menyetelnya ke 0 mematikan pencadangan harian otomatis.

Pencadangan harian otomatis, jendela cadangan harian, dan periode retensi cadangan adalah pengaturan sistem file, dan berlaku untuk semua volume pada sistem file Anda. Anda dapat menggunakan FSx konsol Amazon, the AWS CLI, atau API untuk mengubah pengaturan ini. Untuk informasi selengkapnya, lihat [Memperbarui sistem file](#).

Anda tidak dapat membuat cadangan volume (pencadangan harian otomatis atau cadangan yang diprakarsai pengguna) jika volumenya offline. Untuk informasi selengkapnya, lihat [Melihat volume offline](#).

Note

Pencadangan harian otomatis memiliki periode retensi maksimum 90 hari, tetapi pencadangan yang [dimulai pengguna yang Anda buat, yang mencakup cadangan](#) yang dibuat menggunakan AWS Backup, dipertahankan selamanya kecuali Anda atau menghapusnya. AWS Backup

Anda dapat [menghapus](#) cadangan harian otomatis secara manual menggunakan FSx konsol Amazon, CLI, dan API. Saat Anda menghapus volume, Anda juga menghapus cadangan harian otomatis untuk volume itu. Amazon FSx menyediakan opsi untuk membuat cadangan akhir volume sebelum Anda menghapusnya. Cadangan terakhir disimpan selamanya, kecuali Anda menghapusnya.

Pencadangan yang diprakarsai pengguna

Dengan Amazon FSx, Anda dapat secara manual mengambil cadangan volume sistem file Anda kapan saja menggunakan Konsol Manajemen AWS, AWS CLI, dan API. Pencadangan yang

diprakarsai pengguna Anda bersifat inkremental relatif terhadap cadangan lain yang mungkin telah dibuat untuk volume dan dipertahankan selamanya, kecuali jika Anda menghapusnya. Pencadangan yang diprakarsai pengguna dipertahankan bahkan setelah Anda menghapus volume atau sistem file tempat cadangan dibuat. 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 petunjuk tentang cara membuat cadangan yang diprakarsai pengguna, lihat. [Membuat backup yang diinisiasi pengguna](#)

Menyalin tag ke cadangan

Saat Anda membuat atau memperbarui volume menggunakan CLI atau API, Anda dapat mengaktifkan CopyTagsToBackups untuk [secara otomatis menyalin tag apa pun](#) pada volume Anda ke cadangannya. Namun, jika Anda menambahkan tag apa pun saat membuat cadangan yang dimulai pengguna, termasuk penamaan cadangan saat Anda menggunakan konsol, Amazon FSx tidak menyalin tag dari volume, meskipun CopyTagsToBackups diaktifkan.

Menggunakan AWS Backup dengan Amazon FSx

AWS Backup adalah cara sederhana dan hemat biaya untuk melindungi data Anda dengan mencadangkan Amazon Anda FSx untuk NetApp volume ONTAP. AWS Backup adalah layanan cadangan terpadu yang dirancang untuk menyederhanakan pembuatan, pemulihan, dan penghapusan cadangan, sambil memberikan pelaporan dan audit yang lebih baik. Menggunakan AWS Backup membuatnya lebih mudah untuk mengembangkan strategi cadangan terpusat untuk kepatuhan hukum, peraturan, dan profesional. Ini juga membuat melindungi volume AWS penyimpanan, database, dan sistem file Anda lebih sederhana dengan menyediakan tempat sentral di mana Anda dapat melakukan hal berikut:

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

AWS Backup menggunakan fungsionalitas cadangan bawaan Amazon FSx. Pencadangan yang dibuat menggunakan AWS Backup konsol memiliki tingkat konsistensi dan kinerja sistem file yang sama, bersifat inkremental relatif terhadap pencadangan yang FSx diprakarsai pengguna

Amazon lainnya yang diambil dari volume Anda, dan menawarkan opsi pemulihan yang sama seperti cadangan yang diambil menggunakan konsol Amazon. FSx Menggunakan AWS Backup untuk mengelola cadangan ini menyediakan fungsionalitas tambahan, termasuk kemampuan untuk membuat cadangan terjadwal sesering setiap jam. [Anda dapat menambahkan lapisan pertahanan tambahan untuk melindungi cadangan dari penghapusan yang tidak disengaja atau berbahaya dengan menyimpannya di brankas cadangan.](#)

Cadangan yang dibuat oleh dianggap sebagai cadangan AWS Backup yang diprakarsai pengguna, dan mereka dihitung terhadap kuota cadangan yang diprakarsai pengguna untuk Amazon. FSx Untuk informasi selengkapnya, lihat [Kuota yang dapat Anda tingkatkan](#). Anda dapat melihat dan memulihkan cadangan yang dibuat AWS Backup menggunakan FSx konsol Amazon, CLI, dan API. Namun, Anda tidak dapat menghapus cadangan yang dibuat oleh AWS Backup di FSx konsol Amazon, CLI, atau API. Untuk informasi selengkapnya, lihat [Memulai AWS Backup](#) di Panduan AWS Backup Pengembang.

AWS Backup tidak dapat mencadangkan volume yang offline.

Anda dapat menggunakan tag untuk memilih sumber daya ONTAP mana yang dilindungi dalam paket cadangan. FSx Tag ini harus diterapkan pada tingkat volume daripada tingkat sistem file secara keseluruhan. Untuk informasi selengkapnya, lihat [Menetapkan sumber daya ke paket cadangan](#) di Panduan AWS Backup Pengembang.

Memulihkan backup ke volume baru

Anda dapat mengembalikan cadangan volume ke volume baru pada sistem file Wilayah AWS yang sama dengan cadangan yang disimpan. Anda tidak dapat mengembalikan cadangan ke sistem file yang terletak di berbeda Wilayah AWS dari cadangan.

Saat memulihkan cadangan FSx untuk sistem file generasi kedua ONTAP, klien dapat memasang dan membaca data dari volume saat sedang dipulihkan. Klien dapat memasang volume yang Anda pulihkan dan membaca data file setelah FSx Amazon memuat semua metadata ke volume baru dan volume melaporkan status siklus hidup. CREATED Anda dapat menemukan status siklus hidup volume pada halaman [detail Volume](#) di FSx konsol Amazon dan dalam respons [perintah](#) CLI deskripsi-volume.

Saat membaca data dari volume saat sedang dipulihkan dari cadangan, jika data belum diunduh ke volume, Anda akan dikenakan latensi baca hingga puluhan milidetik untuk akses pertama. Pembacaan ini di-cache di tingkat SSD, dan Anda dapat mengharapkan latensi baca sub-milidetik untuk pembacaan berikutnya.

Jumlah waktu yang dibutuhkan Amazon untuk membuat volume tersedia FSx untuk akses hanya-baca sebanding dengan jumlah metadata file yang disimpan dalam cadangan. Metadata file biasanya mengkonsumsi 1-7% dari keseluruhan data cadangan tergantung pada ukuran file rata-rata dalam kumpulan data Anda (kumpulan data file kecil mengkonsumsi lebih banyak metadata daripada kumpulan data file besar).

Saat Anda mengembalikan cadangan FlexGroup volume ke sistem file yang memiliki jumlah [pasangan ketersediaan tinggi \(HA\)](#) yang berbeda dari sistem file asli, Amazon FSx menambahkan volume konstituen tambahan untuk memastikan bahwa konstituen didistribusikan secara merata.

 Note

Amazon FSx tidak mendukung akses baca ke data saat volume dipulihkan dari cadangan untuk SnapLock volume atau volume apa pun pada sistem file generasi pertama. Saat memulihkan cadangan ini, volume menjadi tersedia untuk dipasang dan mengakses data setelah proses pemulihan selesai, dan semua metadata dan data dimuat ke volume baru.

Saat memulihkan cadangan, semua data awalnya ditulis ke tingkat penyimpanan SSD. Sementara pemulihan sedang berlangsung, data berjenjang ke penyimpanan kolam kapasitas sesuai dengan [kebijakan tingkatan volume](#) yang dipulihkan. Karena data pertama kali ditulis ke tingkat SSD, Amazon FSx akan menghentikan sementara proses restorasi jika sistem file kehabisan ruang penyimpanan SSD. Pemulihan secara otomatis dilanjutkan segera setelah ruang SSD yang cukup tersedia untuk melanjutkan proses. Jika kebijakan tingkatan volume yang dipulihkan adalah All, proses latar belakang berkala akan meningkatkan data ke kumpulan kapasitas. Jika kebijakan tiering volume yang dipulihkan adalah Snapshot Only atau Auto, data berjenjang ke kumpulan kapasitas jika pemanfaatan SSD untuk sistem file lebih besar dari 50%, dan laju pendinginan ditentukan oleh periode pendinginan kebijakan tiering.

Jika beban kerja Anda memerlukan latensi baca sub-milidetik yang konsisten saat memulihkan cadangan ke volume baru pada sistem file generasi kedua, sebaiknya Anda menyetel kebijakan tingkatan volume None saat memulai pemulihan, lalu tunggu hingga semua data diunduh sepenuhnya ke volume sebelum Anda mengaksesnya. Semua data akan dimuat ke penyimpanan SSD sebelum Anda mencoba mengaksesnya, memberi Anda akses latensi rendah yang konsisten ke data Anda.

Untuk step-by-step petunjuk tentang cara mengembalikan cadangan ke volume baru, lihat [Memulihkan cadangan ke volume baru](#).

Pada sistem file generasi kedua Anda juga dapat mengembalikan hanya sebagian data dari cadangan tanpa harus menunggu seluruh operasi pemulihan selesai. Memulihkan hanya sebagian dari data cadangan memungkinkan Anda untuk melanjutkan operasi lebih cepat jika terjadi penghapusan, modifikasi, atau korupsi data yang tidak disengaja. Untuk informasi selengkapnya, lihat [Memulihkan subset data](#).

Anda dapat memantau kemajuan saat memulihkan cadangan pada sistem file generasi kedua di Konsol Manajemen AWS, AWS CLI, dan API. Untuk informasi selengkapnya, lihat [Memantau kemajuan saat memulihkan cadangan](#).

 Note

- Anda tidak dapat membuat snapshot volume atau melakukan operasi berbasis snapshot seperti kloning, SnapMirror replikasi, dan membuat cadangan volume saat sedang dipulihkan dari cadangan.
- Volume yang dipulihkan selalu memiliki gaya volume yang sama dengan volume aslinya. Anda tidak dapat mengubah gaya volume saat memulihkan.

Backup dan pulihkan kinerja

Berbagai faktor dapat mempengaruhi kinerja operasi pencadangan dan pemulihan. Operasi Backup dan Restore adalah proses latar belakang, yang berarti mereka memiliki prioritas yang lebih rendah dibandingkan dengan operasi IO klien. Operasi IO klien termasuk data NFS, CIFS, dan iSCSI serta membaca dan menulis metadata. Semua proses latar belakang hanya menggunakan bagian yang tidak terpakai dari kapasitas throughput sistem file Anda, dan dapat memakan waktu dari beberapa menit hingga beberapa jam untuk menyelesaikannya tergantung pada ukuran cadangan Anda dan jumlah kapasitas throughput yang tidak digunakan pada sistem file Anda.

Faktor lain yang memengaruhi kinerja pencadangan dan pemulihan termasuk tingkat penyimpanan tempat data Anda disimpan dan profil kumpulan data. Kami menyarankan Anda membuat cadangan pertama volume Anda saat sebagian besar data ada di penyimpanan SSD. Dataset yang berisi sebagian besar file kecil biasanya akan memiliki kinerja yang lebih rendah dibandingkan dengan dataset berukuran sama yang sebagian besar berisi file besar. Ini karena memproses sejumlah besar file kecil menghabiskan lebih banyak siklus CPU dan overhead jaringan daripada memproses lebih sedikit file besar.

Umumnya, Anda dapat mengharapkan tingkat pencadangan berikut saat mencadangkan data yang disimpan di tingkat penyimpanan SSD:

- 750 MBps di beberapa backup bersamaan yang berisi sebagian besar file besar.
- 100 MBps di beberapa cadangan bersamaan yang sebagian besar berisi file kecil.

Umumnya, Anda dapat mengharapkan tingkat pemulihan berikut:

- 250 MBps di beberapa pemulihan bersamaan yang berisi sebagian besar file besar.
- 100 MBps di beberapa pemulihan bersamaan yang sebagian besar berisi file kecil.

Mencadangkan volume SnapLock

Anda dapat mencadangkan [SnapLock](#) volume untuk perlindungan data tambahan. Saat Anda memulihkan SnapLock volume, pengaturan asli volume — seperti retensi default, retensi minimum, dan retensi maksimum — dipertahankan. Tulis sekali, baca banyak pengaturan (WORM) dan Penahanan Hukum juga dipertahankan.

Note

Anda tidak dapat membuat cadangan SnapLock FlexGroup volume.

Anda dapat mengembalikan cadangan SnapLock volume sebagai SnapLock atau SnapLock non-volume. Namun, Anda tidak dapat mengembalikan cadangan SnapLock non-volume sebagai SnapLock volume.

Untuk informasi selengkapnya, lihat [Cara kerja SnapLock](#).

Membuat backup yang diinisiasi pengguna

Prosedur berikut menjelaskan cara membuat cadangan volume yang diprakarsai pengguna.

Anda tidak dapat membuat cadangan volume jika volumenya offline. Untuk informasi selengkapnya, lihat [Melihat volume offline](#).

Untuk membuat cadangan yang diprakarsai pengguna (konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.

2. Arahkan ke sistem File dan pilih sistem ONTAP file yang ingin Anda buat cadangan volumenya.
3. Pilih tab Volume.
4. Pilih volume yang ingin Anda cadangkan.
5. Dari Tindakan, pilih Buat backup.
6. 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 . + - = _ : /
7. Pilih Buat cadangan.

Anda sekarang telah membuat cadangan dari salah satu volume sistem file Anda. Anda dapat melihat semua cadangan Anda di FSx konsol Amazon dengan memilih Cadangan di navigasi sisi kiri. Anda dapat mencari nama yang Anda berikan pada backup Anda, dan filter tabel hanya akan menampilkan hasil yang cocok.

Ketika Anda membuat backup yang diinisiasi pengguna sebagaimana yang dijelaskan prosedur ini, backup tersebut berjenis USER_INITIATED, dan memiliki status CREATING sehingga backup menjadi sepenuhnya tersedia.

Memulihkan cadangan ke volume baru

Prosedur berikut menjelaskan cara mengembalikan cadangan FSx untuk ONTAP ke volume baru menggunakan Konsol Manajemen AWS dan AWS CLI. Saat memulihkan volume ke sistem file generasi kedua, Anda dapat [memantau](#) kemajuan menggunakan Konsol Manajemen AWS, AWS CLI, dan API.

Untuk mengembalikan cadangan volume ke volume baru (Konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi, pilih Cadangan, lalu pilih cadangan volume ONTAP FSx untuk yang ingin Anda pulihkan.
3. Di menu Tindakan kanan atas, pilih Pulihkan cadangan. Halaman Buat volume dari cadangan muncul.
4. Pilih sistem FSx File ONTAP dan mesin virtual Penyimpanan yang ingin Anda pulihkan cadangan dari menu tarik-turun.
5. Di menu Tindakan kanan atas, pilih Pulihkan cadangan. Halaman Buat volume dari cadangan muncul.

6. Pilih sistem FSx File ONTAP dan mesin virtual Penyimpanan yang ingin Anda pulihkan cadangan dari menu tarik-turun.
7. Di bawah Detail volume, ada beberapa pilihan. Pertama, masukkan nama Volume. Anda dapat menggunakan hingga 203 karakter alfanumerik atau garis bawah (_).
8. Untuk ukuran Volume, masukkan bilangan bulat apa pun dalam kisaran 20—314572800 untuk menentukan ukuran dalam mebibytes (MiB).
9. Untuk tipe Volume, pilih Read-Write (RW) untuk membuat volume yang dapat dibaca dan ditulis atau Data Protection (DP) untuk membuat volume yang hanya-baca dan dapat digunakan sebagai tujuan hubungan atau. NetApp SnapMirror SnapVault Untuk informasi selengkapnya, lihat [Tipe volume](#).
10. Untuk jalur Junction, masukkan lokasi di dalam sistem file untuk me-mount volume. Nama harus memiliki garis miring ke depan, misalnya /vol3.
11. Untuk efisiensi Penyimpanan, pilih Diaktifkan untuk mengaktifkan fitur ONTAP efisiensi penyimpanan (deduplikasi, kompresi, dan pemadatan). Untuk informasi selengkapnya, lihat [Efisiensi penyimpanan](#).
12. Untuk gaya keamanan Volume, pilih Unix (Linux), NTFS, atau Mixed. Gaya keamanan volume menentukan apakah preferensi diberikan kepada NTFS atau UNIX ACLs untuk akses multi-protokol. Mode MIXED tidak diperlukan untuk akses multi-protokol dan hanya direkomendasikan untuk pengguna tingkat lanjut.
13. Untuk kebijakan Snapshot, pilih kebijakan snapshot untuk volume. Untuk informasi selengkapnya tentang kebijakan snapshot, lihat [Kebijakan snapshot](#).

Jika memilih Kebijakan khusus, Anda harus menentukan nama kebijakan di bidang kebijakan khusus. Kebijakan kustom harus sudah ada di SVM atau di sistem file. Anda dapat membuat kebijakan snapshot khusus dengan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat [Membuat Kebijakan Snapshot](#) di Dokumentasi NetApp ONTAP Produk.

14. Untuk periode pendinginan kebijakan Tiering, nilai yang berlaku adalah 2-183 hari. Periode pendinginan kebijakan tingkat volume menentukan jumlah hari sebelum data yang belum diakses ditandai dingin dan dipindahkan ke penyimpanan kolam kapasitas. Pengaturan ini hanya memengaruhi Snapshot-only kebijakan Auto dan kebijakan.
15. Di bagian Lanjutan, untuk SnapLockKonfigurasi, Anda dapat meninggalkan pengaturan Nonaktif default atau memilih Diaktifkan untuk mengonfigurasi SnapLock volume. Untuk informasi selengkapnya tentang mengonfigurasi volume SnapLock Kepatuhan atau volume SnapLock Perusahaan, lihat [Memahami SnapLock Kepatuhan](#) dan [Memahami SnapLock Perusahaan](#). Untuk informasi selengkapnya tentang SnapLock, lihat [Melindungi data Anda dengan SnapLock](#).

16. Pilih Konfirmasi untuk membuat volume.
17. Jika Anda memulihkan cadangan ke sistem file generasi kedua, Anda dapat memantau kemajuan pemulihan cadangan pada tab Pembaruan di halaman Volume. Untuk informasi selengkapnya, lihat [Memantau kemajuan saat memulihkan cadangan](#).

Untuk mengembalikan cadangan ke volume baru (CLI)

Gunakan perintah [create-volume-from-backup](#) CLI, atau perintah [CreateVolumeFromBackup](#) API yang setara untuk mengembalikan cadangan volume ke volume baru.

```
$ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
  --name demo --ontap-configuration JunctionPath=/demo,SizeInMegabytes=100000,\
  StorageVirtualMachineId=svm-0f04a9c7c27e1908b,TieringPolicy={Name=ALL}
```

Respons sistem untuk permintaan pemulihan yang berhasil untuk mengembalikan cadangan ke sistem file generasi kedua terlihat sebagai berikut. Responsnya mencakup "AdministrativeActions" objek yang menyediakan informasi status dan kemajuan tentang permintaan..

```
{
  "Volume": {
    "CreationTime": 1692721488.428,
    "FileSystemId": "fs-07ab735385276ed60",
    "Lifecycle": "CREATING",
    "Name": "demo",
    "OntapConfiguration": {
      "FlexCacheEndpointType": "NONE",
      "JunctionPath": "/demo",
      "SizeInMegabytes": 100000,
      "StorageEfficiencyEnabled": true,
      "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
      "StorageVirtualMachineRoot": false,
      "TieringPolicy": {
        "Name": "ALL"
      },
    },
    "OntapVolumeType": "DP",
    "SnapshotPolicy": "default",
    "CopyTagsToBackups": false,
  },
}
```

```

    "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
    "VolumeId": "fsvol-0b6ec764c9c5f654a",
    "VolumeType": "ONTAP",
    ---> "AdministrativeActions": [
        {
            "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
            "RequestTime": 1685729972.069,
            "Status": "PENDING"
        }
    ]
}
<----
}

```

Respons sistem untuk permintaan yang berhasil mengembalikan cadangan ke sistem file generasi pertama terlihat sebagai berikut.

```

{
  "Volume": {
    "CreationTime": 1692721488.428,
    "FileSystemId": "fs-07ab735385276ed60",
    "Lifecycle": "CREATING",
    "Name": "demo",
    "OntapConfiguration": {
      "FlexCacheEndpointType": "NONE",
      "JunctionPath": "/demo",
      "SizeInMegabytes": 100000,
      "StorageEfficiencyEnabled": true,
      "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
      "StorageVirtualMachineRoot": false,
      "TieringPolicy": {
        "Name": "ALL"
      },
      "OntapVolumeType": "DP",
      "SnapshotPolicy": "default",
      "CopyTagsToBackups": false,
    },
    "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
    "VolumeId": "fsvol-0b6ec764c9c5f654a",
    "VolumeType": "ONTAP",
  }
}

```

```
}
```

Saat memulihkan volume ke sistem file generasi kedua, Anda dapat [memantau kemajuan](#) menggunakan Konsol Manajemen AWS, AWS CLI, dan API.

Memulihkan subset data

Anda dapat mengembalikan subset data dari cadangan saat sedang dikembalikan ke volume baru pada sistem file generasi kedua tanpa harus menunggu sampai seluruh kumpulan data cadangan telah dipulihkan sepenuhnya.

Prosedur berikut mencantumkan langkah-langkah yang harus diambil ketika Anda perlu memulihkan subset data saat memulihkan cadangan, dan tidak sabar menunggu seluruh pemulihan selesai:

Untuk mengembalikan subset data saat memulihkan cadangan

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di halaman Cadangan, cari cadangan yang berisi versi data yang ingin Anda pulihkan.
3. Di menu Tindakan kanan atas, pilih Pulihkan cadangan. Halaman Buat volume dari cadangan muncul.
4. Pilih sistem FSx File ONTAP dan mesin virtual Penyimpanan yang ingin Anda pulihkan cadangan dari menu tarik-turun.
5. Di bawah Detail volume, konfigurasi volume untuk memenuhi kebutuhan Anda.
6. Pilih Konfirmasi untuk membuat volume.
7. [Pantau kemajuan](#) pemulihan cadangan.
8. [Pasang volume](#) yang dipulihkan saat melaporkan status siklus hidup. CREATED
9. Temukan subset data pada volume yang perlu Anda salin.
10. Salin data ke volume yang ada yang digunakan aplikasi Anda.
11. Setelah data yang diperlukan dari cadangan telah disalin ke lokasi target, Anda dapat menghapus volume yang dipulihkan sebelum selesai untuk mengoptimalkan pemanfaatan sumber daya sistem file.

Memantau kemajuan saat memulihkan cadangan

Anda dapat memantau kemajuan saat memulihkan cadangan volume ke sistem file generasi kedua di Konsol Manajemen AWS, AWS CLI, dan API. Seperti semua tindakan FSx administratif Amazon, status pemulihan cadangan tersedia di konsol, CLI, dan API selama 30 hari setelah operasi selesai.

Untuk memantau kemajuan saat memulihkan cadangan (konsol)

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

1. Di menu navigasi kiri, pilih Volume.
2. Pilih volume tempat cadangan dikembalikan.
3. Pilih tab Pembaruan.
4. Jenis Backup restore Update memberikan informasi berikut:
 - PENDING menunjukkan bahwa metadata file sedang diunduh ke volume. Status Siklus Hidup volume adalah CREATING.
 - IN_PROGRESS menunjukkan bahwa volume tersedia dan klien dapat me-mount volume dengan akses read-only ke data. Progress% menunjukkan persentase data yang telah diunduh ke volume.
 - SELESAI menunjukkan bahwa semua data telah diunduh ke volume, dan pemulihan cadangan selesai. Klien sekarang memiliki akses baca-tulis. Untuk RW volume, jenis volume berubah dari DP ke RW pada saat ini.

Untuk memantau kemajuan saat memulihkan cadangan (CLI)

- Saat Anda mengembalikan cadangan ke volume baru pada generasi kedua FSx untuk sistem file ONTAP, Anda dapat memantau kemajuan pemulihan menggunakan perintah CLI [describe-volumes](#).

Saat memulihkan cadangan ke sistem file generasi kedua, respons menyertakan AdministrativeActions objek, yang memberikan informasi status tentang proses pengunduhan data. Bagian

```
$ aws fsx describe-volumes
{
  "Volumes": [
    {
```

```

    "CreationTime": 1691686114.674,
    "FileSystemId": fs-029ff92192bd4d375,
    "LifeCycle": "CREATING",
    "Name": vol1,
    "OntapConfiguration": {
      "FlexCacheEndpointType": "NONE",
      "JunctionPath": "/vol1",
      "SizeInMegabytes": 100000,
      "StorageEfficiencyEnabled": true,
      "StorageVirtualMachineId": "svm-0ed1d714019426ca9",
      "StorageVirtualMachineRoot": false,
      "TieringPolicy": {
        "Name": "ALL"
      },
      "OntapVolumeType": "DP",
      "SnapshotPolicy": "default",
      "CopyTagsToBackups": false,
    },
    "ResourceARN": "arn:aws:fsx:us-east-1:630831496844:volume/
fs-08ac75f715c6aec76/fsvol-094c015af930790fa",
    "VolumeId": "fsvol-094c015af930790fa",
    "VolumeType": "ONTAP",
    "AdministrativeActions": [
      {
        "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
        "RequestTime": 1685729972.069,
        "Status": "PENDING"
      }
    ]
  }
}

```

Setelah Amazon FSx memuat semua metadata file ke volume yang dipulihkan, bidang ini memiliki nilai berikut:

- "LifeCycle": "CREATED"— menunjukkan bahwa volume siap dipasang.
- "OntapVolumeType": "DP"— menunjukkan bahwa volume hanya-baca saat data file diunduh.
- "ProgressPercent"— menunjukkan persentase data file yang dimuat ke volume.
- "Status": "IN_PROGRESS"— Mengunduh data file ke volume sedang berlangsung.

Pada tahap ini dalam proses pemulihan Anda dapat memasang volume dengan akses hanya-baca ke semua data dalam cadangan yang Anda pulihkan.

Ketika Amazon FSx telah selesai mengunduh semua data file ke volume baru, klien memiliki akses baca-tulis penuh jika ini adalah RW volume. Indikator memiliki nilai-nilai berikut:

- "LifeCycle": "CREATED"— tidak berubah
- "OntapVolumeType": "RW"— menunjukkan bahwa klien memiliki akses baca-tulis penuh.
- "Status": "COMPLETED"— menunjukkan bahwa pemulihan selesai.

Jika proses pemulihan gagal, `AdministrativeAction > Status` akan memiliki nilai `FAILED`. Pesan kesalahan disediakan di `FailureDetails` objek. Untuk informasi selengkapnya, lihat [AdministrativeActionFailureDetails](#) di Referensi Amazon FSx API

Menghapus cadangan

Anda dapat menghapus pencadangan harian otomatis dan pencadangan volume yang diprakarsai pengguna menggunakan konsol Amazon, Amazon API FSx , atau (). FSx AWS Command Line Interface AWS CLI 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. Anda tidak dapat menghapus cadangan jika volume sumber [offline](#).

Anda dapat menghapus volume saat sedang dipulihkan dari cadangan pada semua FSx untuk sistem file ONTAP. Menghapus volume selama pemulihan secara efektif membatalkan operasi pemulihan yang sedang berlangsung.

Note

Amazon FSx tidak mendukung penghapusan `AVAILABLE` cadangan ONTAP volume terbaru kecuali semua cadangan volume lainnya telah dihapus.

Untuk menghapus cadangan yang dibuat menggunakan AWS Backup, lihat [Menghapus cadangan](#) di Panduan Pengembang. AWS Backup

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 yang ditampilkan adalah 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 disertakan sekarang dihapus secara permanen dan tidak dapat dipulihkan.

Untuk menghapus cadangan (CLI)

- Gunakan perintah CLI hapus-cadangan atau tindakan DeleteBackup API yang setara untuk menghapus cadangan volume ONTAP, seperti yang FSx ditunjukkan pada contoh berikut.

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

Respons sistem mencakup ID cadangan yang dihapus, dan status siklus hidupnya dengan nilai `DELETED`, yang menunjukkan bahwa permintaan berhasil.

```
{  
  "BackupId": "backup-a0123456789abcdef",  
  "Lifecycle": "DELETED"  
}
```

Melindungi data Anda dengan snapshot

Snapshot adalah gambar hanya-baca Amazon FSx untuk volume NetApp ONTAP pada suatu titik waktu. Snapshot menawarkan perlindungan terhadap penghapusan atau modifikasi file yang tidak disengaja dalam volume Anda. Dengan snapshot, pengguna Anda dapat dengan mudah melihat dan memulihkan file atau folder individual dari snapshot sebelumnya untuk membatalkan perubahan, memulihkan konten yang dihapus, dan membandingkan versi file.

Sebuah snapshot berisi data yang telah berubah sejak snapshot terakhir yang mengkonsumsi kapasitas penyimpanan SSD sistem file. Snapshot tidak termasuk dalam [cadangan](#) volume apa pun. Snapshot diaktifkan secara default pada volume Anda menggunakan kebijakan default snapshot. Snapshot disimpan di .snapshot direktori di root volume. Anda dapat menyimpan maksimal 1.023 snapshot per volume kapan saja. Setelah Anda mencapai batas ini, Anda harus [menghapus snapshot yang ada](#) sebelum snapshot baru volume Anda dapat dibuat.

Topik

- [Kebijakan snapshot](#)
- [Memulihkan file dari snapshot](#)
- [Melihat snapshot umum](#)
- [Memperbarui cadangan snapshot volume Anda](#)
- [Menonaktifkan snapshot otomatis](#)
- [Menghapus snapshot](#)
- [Menghapus snapshot](#)
- [Cadangan snapshot](#)

Kebijakan snapshot

Kebijakan snapshot mendefinisikan bagaimana sistem membuat snapshot untuk volume. Kebijakan menentukan kapan harus membuat snapshot, jumlah salinan yang akan disimpan, dan cara menamainya. Ada tiga kebijakan snapshot bawaan FSx untuk ONTAP:

- default
- default-1weekly
- none

Secara default, setiap volume dikaitkan dengan kebijakan default snapshot sistem file. Sebaiknya gunakan kebijakan ini untuk sebagian besar beban kerja.

defaultKebijakan secara otomatis membuat snapshot pada jadwal berikut, dengan salinan snapshot tertua dihapus untuk memberi ruang bagi salinan yang lebih baru:

- Maksimal enam snapshot per jam diambil lima menit melewati satu jam.
- Maksimal dua foto harian diambil dari Senin hingga Sabtu pukul 10 menit setelah tengah malam.

- Maksimal dua foto mingguan diambil setiap hari Minggu pada 15 menit setelah tengah malam.

Note

Waktu snapshot didasarkan pada zona waktu sistem file, yang default ke Coordinated Universal Time (UTC). Anda dapat mengatur zona waktu sistem file ONTAP dengan menggunakan perintah `timezone -timezone time_zone` ONTAP CLI. FSx Untuk informasi lebih lanjut tentang mengakses ONTAP CLI, lihat. [Menggunakan CLI NetApp ONTAP](#)

`default-1weekly` Kebijakan bekerja dengan cara yang sama seperti `default` kebijakan, kecuali hanya mempertahankan satu snapshot dari jadwal mingguan.

`none` Kebijakan tidak mengambil snapshot apa pun. Anda dapat menetapkan kebijakan ini ke volume untuk mencegah snapshot otomatis diambil.

Anda juga dapat membuat kebijakan snapshot khusus menggunakan ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat [Membuat Kebijakan Snapshot di Dokumentasi](#) Produk NetApp ONTAP. Anda dapat memilih kebijakan snapshot saat membuat atau memperbarui volume di FSx konsol Amazon, Amazon FSx API AWS CLI, atau Amazon. Untuk informasi selengkapnya, lihat [Membuat volume](#) dan [Memperbarui volume](#).

Memulihkan file dari snapshot

Menggunakan snapshot pada sistem FSx file Amazon Anda, Anda dapat dengan cepat memulihkan versi sebelumnya dari masing-masing file atau folder.

Jika Anda menggunakan klien Linux dan macOS, Anda dapat melihat snapshot di `.snapshot` direktori di root volume. Jika Anda menggunakan klien Windows, Anda dapat melihat snapshot di `Previous Versions` tab Windows Explorer (saat mengklik kanan pada file atau folder).

Untuk memulihkan file dari snapshot (klien Linux dan macOS)

1. Jika file asli masih ada dan Anda tidak ingin ditimpa oleh file dalam snapshot, maka gunakan klien Linux atau macOS Anda untuk mengganti nama file asli atau memindahkannya ke direktori yang berbeda.
2. Di `.snapshot` direktori, cari snapshot yang berisi versi file yang ingin Anda pulihkan.

3. Salin file dari .snapshot direktori ke direktori di mana file awalnya ada.

Untuk mengembalikan file dari snapshot (klien Windows)

Pengguna pada klien Windows dapat memulihkan file ke versi sebelumnya menggunakan antarmuka Windows File Explorer yang sudah dikenal.

1. Untuk memulihkan file, pengguna memilih file yang akan dipulihkan, lalu pilih Pulihkan versi sebelumnya dari menu konteks (klik kanan).
2. Pengguna kemudian dapat melihat dan memulihkan ke versi sebelumnya dari daftar Versi sebelumnya.

Data dalam snapshot adalah read-only. Jika Anda ingin membuat modifikasi pada file dan folder yang tercantum di tab Versi Sebelumnya, Anda harus menyimpan salinan file dan folder yang ingin Anda modifikasi ke lokasi yang dapat ditulis dan membuat modifikasi pada salinan.

Melihat snapshot umum

Snapshot umum digunakan untuk mempertahankan inkrementalitas di antara cadangan Anda. Prosedur ini menjelaskan cara mengidentifikasi snapshot umum pada volume Anda.

Untuk melihat snapshot umum volume

- Untuk menentukan snapshot mana yang merupakan snapshot umum volume, gunakan perintah CLI [volume snapshot show](#) ONTAP.

```
volume snapshot show -volume volume-name
```

Dalam output, nama snapshot umum memiliki format `backup-id`, di mana *id* adalah string alfanumerik 17 digit, seperti yang ditunjukkan pada contoh berikut:

```
FsxIdabc12345::> volume snapshot show -volume test_vol
                      ---Blocks---
Vserver Volume      Snapshot                Size      Total% Used%
-----
dest-svm test_vol
              snap1                144KB      0%      3%
              snap2                832KB      0%     16%
              ----> backup-abcdef0123456789a  4.87MB      0%     53% <---
```

weekly.2024-05-26_0015	5.02MB	0%	54%
weekly.2024-06-02_0015	2.22MB	0%	34%
daily.2024-06-04_0010	284KB	0%	6%
daily.2024-06-05_0010	4.29MB	0%	50%
hourly.2024-06-05_0705	168KB	0%	4%

8 entries were displayed.

Important

Jangan hapus snapshot umum pada volume karena digunakan untuk menjaga inkrementalitas di antara cadangan Anda. Menghapus snapshot umum volume akan menyebabkan cadangan berikutnya menjadi cadangan penuh volume alih-alih cadangan tambahan.

Memperbarui cadangan snapshot volume Anda

Anda dapat mengubah jumlah cadangan snapshot pada volume menggunakan NetApp ONTAP CLI atau API, yang dijelaskan dalam prosedur berikut.

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Gunakan perintah [volume modify](#) ONTAP CLI untuk mengubah persentase ruang disk yang digunakan untuk cadangan salinan Snapshot. Ganti nilai placeholder berikut dengan data Anda:
 - *svm_name*—gunakan nama SVM Anda.
 - *vol_name*—gunakan nama volume Anda.
 - *percent*—persentase ruang disk yang ingin Anda pesan untuk salinan Snapshot.

```
::> volume modify -vserver svm_name -volume vol_name -percent-snapshot-space percent
```

Contoh berikut mengubah cadangan snapshot untuk vol1 menjadi 25% dari kapasitas penyimpanan volume.

```
::> volume modify -vserver vs0 -volume vol1 -percent-snapshot-space 25
```

Menonaktifkan snapshot otomatis

Snapshot otomatis diaktifkan oleh kebijakan snapshot default untuk volume di sistem file ONTAP Anda FSx . Jika Anda tidak memerlukan snapshot data Anda (misalnya, jika Anda menggunakan data pengujian), Anda dapat menonaktifkan snapshot dengan menyetel [kebijakan snapshot](#) volume untuk none menggunakan Konsol Manajemen AWS, AWS CLI dan API, dan ONTAP CLI, seperti yang dijelaskan dalam prosedur berikut.

Untuk menonaktifkan snapshot otomatis (AWS konsol)

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Arahkan ke sistem File dan pilih sistem file ONTAP yang ingin Anda perbarui volumenya.
3. Pilih tab Volume.
4. Pilih volume yang ingin Anda perbarui.
5. Untuk Tindakan, pilih Perbarui volume.

Kotak dialog Perbarui volume ditampilkan dengan pengaturan volume saat ini.

6. Untuk kebijakan Snapshot, pilih Tidak ada.
7. Pilih Perbarui untuk memperbarui volume.

Untuk menonaktifkan snapshot otomatis (AWS CLI)

- Gunakan perintah AWS CLI [update-volume](#) (atau perintah API yang [UpdateVolumes](#) setara), untuk menyetel none ke, seperti SnapshotPolicy yang ditunjukkan pada contoh berikut.

```
aws fsx update-volume \  
  --volume-id fsvol-1234567890abcdefa \  
  --name new_vol \  
  --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \  
    SizeInMegabytes=2048,SnapshotPolicy=none, \  
    StorageEfficiencyEnabled=true, \  
    
```

TieringPolicy=all

Untuk menonaktifkan snapshot otomatis (ONTAPCLI)

Setel kebijakan snapshot volume untuk menggunakan kebijakan none default untuk menonaktifkan snapshot otomatis.

1. Gunakan perintah [volume snapshot policy show](#) ONTAPCLI untuk menampilkan kebijakan. none

```
::> snapshot policy show -policy none
```

```
Vserver: FsxIdabcdef01234567892
```

Policy Name	Number of Is	Schedules Enabled	Comment
none	0	false	Policy for no automatic snapshots.
Schedule	Count	Prefix	SnapMirror Label
-----	----	-----	-----
-	-	-	-

2. Gunakan perintah [volume modify](#) ONTAPCLI untuk mengatur kebijakan snapshot volume none untuk menonaktifkan snapshot otomatis. Ganti nilai placeholder berikut dengan data Anda:

- **svm_name**— gunakan nama SVM Anda.
- **vol_name**— gunakan nama volume Anda.

Saat diminta untuk melanjutkan, masukkan y.

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none
```

```
Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
Snapshot copies on this volume
```

```
that do not match any of the prefixes of the new Snapshot policy will not
be deleted. However, when
```

```
the new Snapshot policy takes effect, depending on the new retention
count, any existing Snapshot copies
```

```
that continue to use the same prefixes might be deleted. See the 'volume
modify' man page for more information.
```

```
Do you want to continue? {y|n}: y
```

Volume modify successful on volume *vol_name* of Vserver *svm_name*.

Menghapus snapshot

Snapshot mengkonsumsi kapasitas penyimpanan hanya untuk data pada volume yang telah berubah sejak snapshot terakhir. Untuk alasan ini, jika beban kerja Anda menulis data dengan cepat, snapshot dari data lama dapat mengambil sejumlah besar kapasitas penyimpanan volume.

Misalnya, output perintah [volume show-space](#) ONTAP CLI menunjukkan 140 KB dari User Data. Namun, volumenya memiliki 9,8 GB User Data sebelum data pengguna dihapus. Bahkan jika Anda telah menghapus file dari volume Anda, snapshot mungkin masih mereferensikan data pengguna lama. Karena itu, Snapshot Reserve dan Snapshot Spill dalam contoh sebelumnya mengambil total 9,8 GB ruang, meskipun hampir tidak ada data pengguna pada volume.

Untuk mengosongkan ruang pada volume, Anda dapat menghapus snapshot lama yang tidak lagi Anda perlukan. Karena snapshot bersifat inkremental, Anda tidak merebut kembali jumlah penyimpanan yang sama dengan ukuran snapshot saat Anda menghapusnya. Anda dapat melihat jumlah penyimpanan yang dapat Anda reklamasi saat menghapus snapshot dengan menggunakan perintah [volume snapshot compute-reclaimable](#) ONTAP CLI, menggunakan data Anda untuk mengganti, dan. *svm_name vol_name snapshot_name*

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
                  -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

Anda dapat menghapus snapshot baik dengan membuat [kebijakan penghapusan otomatis snapshot](#) atau dengan menghapus snapshot secara [manual](#). Menghapus snapshot menghapus data yang diubah yang disimpan pada snapshot.

Menghapus snapshot

Gunakan perintah [volume snapshot delete](#) ONTAP CLI untuk menghapus snapshot secara manual, mengganti nilai placeholder berikut dengan data Anda:

- Ganti *svm_name* dengan nama SVM tempat volume dibuat.
- Ganti *vol_name* dengan nama volume.

- Ganti *snapshot_name* dengan nama snapshot. Perintah ini mendukung karakter wildcard (*) untuk *snapshot_name*. Oleh karena itu, Anda dapat menghapus semua snapshot per jam, misalnya, dengan menggunakan `hourly*`

Important

Jika Anda mengaktifkan FSx cadangan Amazon, Amazon FSx menyimpan snapshot untuk FSx cadangan Amazon terbaru dari setiap volume. Snapshot tersebut digunakan untuk menjaga inkrementalitas di antara cadangan, dan tidak boleh dihapus dengan menggunakan metode ini. Untuk informasi selengkapnya, lihat [Melihat snapshot umum](#).

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -  
snapshot snapshot_name
```

Membuat kebijakan penghapusan otomatis Snapshot

Anda dapat membuat kebijakan untuk menghapus snapshot secara otomatis ketika jumlah ruang yang tersedia dalam volume Anda hampir habis. Gunakan perintah [ONTAPCLI modifikasi otomatis snapshot volume](#) untuk membuat kebijakan penghapusan otomatis untuk volume.

Saat menggunakan perintah ini, gunakan data Anda untuk mengganti nilai placeholder berikut:

- Ganti *svm_name* dengan nama SVM tempat volume dibuat.
- Ganti *vol_name* dengan nama volume.

Untuk-trigger, tetapkan salah satu nilai berikut:

- `volume`— Gunakan `volume` jika Anda ingin ambang batas di mana snapshot dihapus sesuai dengan total ambang kapasitas volume yang digunakan. Ambang batas kapasitas volume yang digunakan yang memicu penghapusan snapshot ditentukan oleh ukuran volume Anda, dengan penskalaan ambang batas dari 85-98 persen kapasitas yang digunakan. Volume yang lebih kecil memiliki ambang yang lebih kecil, dan volume yang lebih besar memiliki ambang yang lebih besar.
- `snap_reserve`— Gunakan `snap_reserve` jika Anda ingin snapshot dihapus berdasarkan apa yang dapat disimpan di cadangan snapshot Anda.

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true  
-trigger [volume|snap_reserve]
```

Untuk informasi selengkapnya, lihat perintah [modifikasi hapus otomatis snapshot volume](#) di Pusat Dokumentasi NetApp ONTAP.

Cadangan snapshot

Cadangan salinan snapshot menetapkan persentase tertentu dari kapasitas penyimpanan volume untuk menyimpan salinan Snapshot, dengan nilai default 5 persen. [Cadangan salinan Snapshot harus memiliki ruang yang cukup dialokasikan untuk salinan Snapshot, termasuk cadangan volume.](#)

Jika salinan Snapshot melebihi ruang cadangan Snapshot, Anda harus menghapus salinan Snapshot yang ada dari sistem file aktif untuk memulihkan kapasitas penyimpanan untuk penggunaan sistem file. Anda juga dapat memodifikasi persentase ruang disk yang dialokasikan ke salinan Snapshot.

Setiap kali Snapshots mengkonsumsi lebih dari 100% cadangan Snapshot, mereka mulai menempati ruang penyimpanan SSD utama. Proses ini disebut Snapshot spill. Ketika Snapshots terus menempati ruang sistem file aktif, sistem file berisiko menjadi penuh. Jika sistem file menjadi penuh karena tumpahan Snapshot, Anda dapat membuat file hanya setelah Anda menghapus cukup Snapshot.

Ketika ruang disk yang cukup tersedia untuk snapshot dalam cadangan snapshot, menghapus file dari tingkat SSD utama membebaskan ruang disk untuk file baru, sedangkan salinan Snapshot yang mereferensikan file-file tersebut hanya menghabiskan ruang dalam cadangan salinan Snapshot.

Karena tidak ada cara untuk mencegah Snapshot mengkonsumsi ruang disk lebih besar dari jumlah yang disediakan untuk mereka (cadangan Snapshot), penting untuk memesan ruang disk yang cukup untuk Snapshots sehingga tingkat SSD utama selalu memiliki ruang yang tersedia untuk membuat file baru atau memodifikasi yang sudah ada.

Jika snapshot dibuat saat disk penuh, menghapus file dari tingkat SSD utama tidak menciptakan ruang kosong karena semua data itu juga direferensikan oleh Snapshot yang baru dibuat. Anda harus [menghapus Snapshot](#) untuk mengosongkan penyimpanan untuk membuat atau memperbarui file apa pun.

Anda dapat mengubah jumlah cadangan Snapshot pada volume menggunakan NetApp ONTAP CLI. Lihat informasi yang lebih lengkap di [Memperbarui cadangan snapshot volume Anda](#).

Melindungi data Anda dengan Autonomous Ransomware Protection

Autonomous Ransomware Protection (ARP) adalah fitur NetApp ONTAP berbasis AI yang memantau dan melindungi data Anda dari serangan ransomware dan malware jika klien Windows atau Linux Anda terganggu. Menggunakan pembelajaran mesin, ARP menjadi akrab dengan sistem file ONTAP Anda FSx untuk secara proaktif mendeteksi aktivitas abnormal. ARP tersedia untuk semua yang baru dan yang sudah ada FSx untuk sistem file ONTAP di semua tempat Wilayah AWS Amazon FSx untuk NetApp ONTAP tersedia.

Bagaimana ARP bekerja

Anda dapat mengaktifkan ARP berdasarkan per volume atau secara default pada semua volume baru dalam SVM menggunakan CLI ONTAP atau REST API. Untuk informasi selengkapnya tentang mengaktifkan ARP, lihat [Mengaktifkan Perlindungan Ransomware Otonom](#)

Karena AI ARP dilatih pada kumpulan data yang komprehensif, ARP tidak memerlukan periode pembelajaran agar ARP berjalan pada FlexVol volume, dan karenanya segera dimulai dalam mode aktif. ARP AI juga dilengkapi dengan kemampuan pembaruan otomatis untuk memastikan perlindungan dan ketahanan konstan terhadap ancaman terbaru. Dalam mode aktif, ARP memantau data dan aktivitas yang masuk pada volume untuk mengidentifikasi potensi serangan ransomware dan malware. Untuk informasi selengkapnya, lihat [Apa yang dicari ARP](#). Jika ARP mendeteksi aktivitas abnormal, ONTAP snapshot dibuat secara otomatis untuk membantu Anda memulihkan data sedekat mungkin dengan waktu serangan potensial. Snapshot akan memiliki awalan `Anti_ransomware_backup`, sehingga mudah untuk mengidentifikasi. Jika ditentukan bahwa probabilitas serangan moderat, ONTAP akan menghasilkan pesan Sistem Manajemen Acara (EMS) untuk Anda tinjau. Untuk informasi selengkapnya, lihat [Bagaimana menanggapi dugaan serangan dengan ARP](#) dan [Memahami peringatan EMS untuk Perlindungan Ransomware Otonom](#).

Overhead kinerja untuk ARP minimal untuk sebagian besar beban kerja. Jika volume Anda memiliki beban kerja intensif baca, NetApp merekomendasikan untuk melindungi tidak lebih dari 150 volume tersebut per sistem file. Jika Anda melebihi angka ini, IOPS untuk beban kerja itu mungkin turun hingga 4%. Jika volume Anda memiliki beban kerja intensif tulis, NetApp merekomendasikan untuk melindungi tidak lebih dari 60 volume tersebut per sistem file. Jika tidak, IOPS untuk beban kerja itu mungkin turun hingga 10%. Untuk informasi selengkapnya tentang kinerja, lihat [Amazon FSx untuk kinerja NetApp ONTAP](#).

Tidak ada biaya tambahan untuk mengaktifkan ARP pada sistem file ONTAP Anda FSx .

Apa yang dicari ARP

ARP mencari tanda-tanda bahwa klien Windows atau Linux Anda dikompromikan. Secara khusus, ARP mencari jenis aktivitas berikut pada volume:

- Perubahan entropi, yang berarti perbedaan keacakan data dalam file.
- Perubahan jenis ekstensi file, yang berarti ekstensi baru tidak konsisten dengan jenis ekstensi yang biasa digunakan. Defaultnya adalah 20 file dengan ekstensi file yang sebelumnya tidak diamati dalam volume.
- Perubahan file IOPS, yang berarti lonjakan aktivitas volume abnormal dengan data terenkripsi.

Anda dapat memodifikasi parameter deteksi ransomware untuk volume Anda jika perlu. Misalnya, jika volume Anda menampung banyak jenis ekstensi file. Untuk informasi selengkapnya, lihat [Mengelola parameter deteksi serangan Perlindungan Ransomware Otonomi ONTAP di Pusat Dokumentasi](#).

NetApp

Note

ARP tidak mencegah administrator nakal dengan kredensial mengakses sistem file ONTAP Anda. FSx AWS merekomendasikan pendekatan keamanan berlapis termasuk AWS Backup, ONTAP snapshot, dan. SnapLock

Bagaimana menanggapi dugaan serangan dengan ARP

Jika ARP mendeteksi serangan, itu akan menghasilkan snapshot yang dapat digunakan sebagai titik pemulihan. Snapshot terkunci dan tidak dapat dihapus dengan cara normal. Tergantung pada tingkat keparahan serangan, itu juga akan menghasilkan peringatan EMS yang menunjukkan volume yang terpengaruh, probabilitas serangan, dan garis waktu serangan. Jika Anda ingin menerima peringatan untuk pembuatan snapshot baru atau pengamatan ekstensi file baru pada volume Anda, Anda dapat mengonfigurasi ARP untuk mengirim peringatan ini. Untuk informasi selengkapnya, lihat [Mengkonfigurasi peringatan ARP di Pusat](#) NetApp Dokumentasi.

Anda dapat membuat laporan untuk melihat informasi rinci tentang serangan yang dicurigai. Setelah Anda meninjau laporan, Anda dapat mengetahui ONTAP apakah peringatan itu dihasilkan oleh positif palsu atau serangan yang dicurigai. Jika Anda memberi label peringatan sebagai serangan yang dicurigai, Anda harus menentukan ruang lingkup serangan dan kemudian memulihkan data

dari snapshot yang dibuat ARP. Jika Anda memberi label serangan sebagai positif palsu, snapshot yang dibuat ARP akan dihapus secara otomatis. Untuk informasi selengkapnya, lihat [Menanggapi peringatan Autonomous Ransomware Protection](#).

Kami merekomendasikan untuk memantau pesan EMS sistem file Anda dan status volume Anda di ONTAP CLI dan REST API. Untuk informasi selengkapnya tentang pesan EMS untuk ARP, lihat [Memahami peringatan EMS untuk Perlindungan Ransomware Otonom](#).

Topik

- [Mengaktifkan Perlindungan Ransomware Otonom](#)
- [Menanggapi peringatan Autonomous Ransomware Protection](#)
- [Memahami peringatan EMS untuk Perlindungan Ransomware Otonom](#)

Mengaktifkan Perlindungan Ransomware Otonom

Prosedur berikut menjelaskan cara menggunakan ONTAP CLI untuk mengaktifkan mode aktif Autonomous Ransomware Protection (ARP) serta cara memverifikasi bahwa ARP diaktifkan. Untuk informasi lebih lanjut tentang ARP, lihat [Bagaimana ARP bekerja](#).

Mengaktifkan ARP dalam mode aktif

Untuk mengaktifkan ARP dalam mode aktif pada volume yang ada menggunakan CLI ONTAP

- Jalankan perintah berikut. Ganti *vol_name* dan *svm_name* dengan informasi Anda sendiri.

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

Untuk informasi selengkapnya tentang perintah ini, lihat [security anti-ransomware volume enable](#) di pusat NetApp dokumentasi.

Mengaktifkan ARP secara default di tingkat SVM

Untuk mengaktifkan ARP secara default pada SVM yang ada menggunakan CLI ONTAP

- Jalankan perintah berikut. Ganti *svm_name* dengan informasi Anda sendiri.

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

Untuk informasi selengkapnya tentang perintah ini, lihat [vserver modify](#) di pusat NetApp dokumentasi.

Memverifikasi status ARP

Untuk memverifikasi status ARP menggunakan CLI ONTAP

- Jalankan perintah berikut.

```
security anti-ransomware volume show
```

Untuk informasi selengkapnya tentang perintah ini, lihat [security anti-ransomware volume show](#) di pusat NetApp dokumentasi.

Anda dapat menangguhkan sementara (dan kemudian melanjutkan) ARP jika Anda mengantisipasi peristiwa beban kerja yang berat. Untuk informasi selengkapnya, lihat [Menjeda ONTAP Autonomous Ransomware Protection untuk mengecualikan peristiwa beban kerja dari analisis](#) di Pusat Dokumentasi. NetApp

Menanggapi peringatan Autonomous Ransomware Protection

Prosedur berikut menjelaskan cara menggunakan ONTAP CLI untuk melihat peringatan Autonomous Ransomware Protection (ARP), menghasilkan laporan serangan, dan mengambil tindakan atas laporan. Untuk informasi lebih lanjut tentang bagaimana ARP mendeteksi dan merespons serangan, lihat dan. [Apa yang dicari ARP](#) [Bagaimana menanggapi dugaan serangan dengan ARP](#)

Melihat peringatan ARP

Untuk melihat peringatan ARP pada volume menggunakan CLI ONTAP

- Jalankan perintah berikut. Ganti *svm_name* dan *vol_name* dengan informasi Anda sendiri.

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

Setelah menjalankan perintah, Anda akan melihat output yang mirip dengan contoh berikut:

```
Vserver Name: fsx  
Volume Name: vol1
```

```
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

Untuk informasi selengkapnya tentang perintah ini, lihat [security anti-ransomware volume show](#) di pusat NetApp dokumentasi.

Menghasilkan laporan ARP

Untuk menghasilkan laporan ARP menggunakan CLI ONTAP

- Jalankan perintah berikut. Ganti *vol_name* dan */file_location/* dengan informasi Anda sendiri. Setelah Anda membuat laporan, Anda dapat melihatnya di sistem klien.

```
security anti-ransomware volume attack generate-report -volume vol_name -dest-path /file_location/
```

Untuk informasi selengkapnya tentang perintah ini, lihat [security anti-ransomware volume attack generate-report](#) di pusat NetApp dokumentasi.

Mengambil tindakan atas laporan ARP

Untuk mengambil tindakan atas serangan positif palsu dari laporan ARP menggunakan CLI ONTAP

- Jalankan perintah berikut. Ganti *svm_name*, *vol_name*, dan *[extension identifiers]* dengan informasi Anda sendiri.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -volume vol_name [extension identifiers] -false-positive true
```

Untuk informasi selengkapnya tentang perintah ini, lihat [security anti-ransomware volume attack clear-suspect](#) di pusat NetApp dokumentasi.

Note

Ketika Anda menandai peringatan sebagai positif palsu, itu memperbarui profil ransomware. Setelah melakukannya, Anda tidak akan menerima peringatan tentang skenario tertentu lagi.

Untuk mengambil tindakan terhadap serangan potensial dari laporan ARP menggunakan CLI ONTAP

- Jalankan perintah berikut. Ganti *svm_name*, *vol_name*, dan *[extension identifiers]* dengan informasi Anda sendiri.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive false
```

Untuk informasi selengkapnya tentang perintah ini, lihat [security anti-ransomware volume attack clear-suspect](#) di pusat NetApp dokumentasi.

Memahami peringatan EMS untuk Perlindungan Ransomware Otonom

Anda dapat menggunakan NetApp ONTAP's Events Management System (EMS) untuk memantau peristiwa yang terkait dengan ARP termasuk potensi serangan. Untuk informasi lebih lanjut tentang ARP dan cara mendeteksi serangan, lihat [Bagaimana ARP bekerja](#) dan [Apa yang dicari ARP](#).

Tabel berikut berisi semua peringatan yang terkait dengan ARP. Untuk informasi lebih lanjut tentang EMS, lihat [Pemantauan FSx untuk acara ONTAP EMS](#).

Nama pesan EMS	Deskripsi pesan EMS
<code>arw.analytics.ext.report</code>	Pesan ini terjadi ketika analitik anti-ransomware menghasilkan atau memperbarui laporan ekstensi file yang mencurigakan untuk volume.
<code>arw.analytics.high.entropy</code>	Pesan ini terjadi ketika jumlah pesan log data entropi tinggi (berkaitan dengan deteksi dan analisis ransomware) melewati ambang batas yang telah ditentukan untuk volume.

Nama pesan EMS	Deskripsi pesan EMS
<code>arw.analytics.probability</code>	Pesan ini terjadi ketika probabilitas serangan anti-ransomware telah berubah dari high pada low volume.
<code>arw.analytics.report</code>	Pesan ini terjadi ketika laporan analitik anti-ransomware dibuat atau diperbarui untuk volume.
<code>arw.analytics.suspects</code>	Pesan ini terjadi ketika daftar tersangka yang dihasilkan oleh analitik anti-ransomware tumbuh ke titik di mana penyelidikan lebih lanjut diperlukan.
<code>arw.new.file.extn.seen</code>	Pesan ini terjadi ketika ekstensi file baru diamati dalam volume yang diaktifkan anti-ransomware. Tujuannya adalah untuk segera memberi tahu pengguna tentang ekstensi yang diamati, yang memungkinkan penyelidikan tepat waktu.
<code>arw.snapshot.created</code>	Pesan ini terjadi ketika snapshot ARP baru dibuat dalam volume yang diaktifkan anti-ransomware. Selain itu, ini memberikan informasi tentang alasan mengapa snapshot dibuat.
<code>arw.volume.state</code>	Pesan ini terjadi ketika status anti-ransomware dari volume diubah.
<code>arw.vserver.state</code>	Pesan ini terjadi ketika keadaan anti-ransomware SVM diubah.

Melindungi data Anda dengan SnapLock

SnapLock adalah fitur yang memungkinkan Anda untuk melindungi file Anda dengan mentransisikannya ke status tulis sekali, baca banyak (WORM), yang mencegah modifikasi atau penghapusan untuk periode retensi tertentu. Anda dapat menggunakannya SnapLock untuk memenuhi kepatuhan terhadap peraturan, untuk melindungi data penting bisnis dari serangan ransomware, dan

untuk memberikan lapisan perlindungan tambahan untuk data Anda terhadap perubahan atau penghapusan.

Amazon FSx untuk NetApp ONTAP mendukung mode retensi Kepatuhan dan Perusahaan.

SnapLock Untuk informasi selengkapnya, lihat [Memahami SnapLock Kepatuhan](#) dan [Memahami SnapLock Perusahaan](#).

Anda dapat membuat SnapLock volume FSx untuk sistem file ONTAP yang dibuat pada atau setelah 13 Juli 2023. Sistem file yang ada akan mendapatkan SnapLock dukungan selama jendela pemeliharaan mingguan mendatang.

Topik

- [Cara kerja SnapLock](#)
- [Memahami SnapLock Kepatuhan](#)
- [Memahami SnapLock Perusahaan](#)
- [Memahami periode SnapLock retensi](#)
- [Mengkomit file ke status WORM](#)

Cara kerja SnapLock

SnapLock dapat membantu Anda memenuhi tujuan peraturan dan tata kelola dengan mencegah file Anda dihapus, diubah, atau diganti namanya. Ketika Anda membuat SnapLock volume, Anda mengkomit file Anda untuk menulis sekali, membaca banyak penyimpanan (WORM) dan mengatur periode retensi untuk data. File Anda dapat disimpan dalam keadaan yang tidak dapat dihapus, tidak dapat ditulis untuk jangka waktu yang ditentukan, atau tanpa batas waktu.

Important

Anda harus menentukan apakah volume akan menggunakan SnapLock pengaturan pada saat pembuatan. SnapLockNon-volume tidak dapat dikonversi ke SnapLock volume setelah pembuatan.

Mode retensi

SnapLock memiliki dua mode retensi: Kepatuhan dan Perusahaan. Amazon FSx untuk NetApp ONTAP mendukung keduanya. Mereka memiliki kasus penggunaan yang berbeda dan beberapa fitur

berbeda, tetapi keduanya melindungi data Anda dari modifikasi atau penghapusan menggunakan model WORM. Tabel berikut menjelaskan beberapa persamaan dan perbedaan antara mode retensi ini.

SnapLockfitur	Memahami SnapLock Kepatuhan	Memahami SnapLock Perusahaan
Deskripsi	File yang dialihkan ke WORM pada volume Kepatuhan tidak dapat dihapus hingga periode retensi berakhir.	File yang dialihkan ke WORM pada volume Perusahaan dapat dihapus oleh pengguna yang berwenang sebelum periode retensi mereka kedaluwarsa menggunakan penghapusan hak istimewa.
Kasus penggunaan	• Untuk mengatasi mandat khusus pemerintah atau industri seperti Aturan SEC 17a-4 (f), Aturan FINRA 4511, dan Peraturan CFTC 1.31. • Untuk melindungi dari serangan ransomware.	• Untuk memajukan integritas data organisasi dan kepatuhan internal. • Untuk menguji setelan retensi sebelum menggunakan SnapLock Kepatuhan.
Komit otomatis	Ya	Ya
Retensi berbasis peristiwa (EBR)¹	Ya	Ya
Penahanan Hukum¹	Ya	Tidak
Menggunakan penghapusan hak istimewa	Tidak	Ya
Mode Volume-append	Ya	Ya
SnapLockvolume log audit	Ya	Ya

 Note

¹ Operasi EBR dan Legal Hold didukung di ONTAP CLI dan REST API.

 Note

FSx untuk ONTAP mendukung tiering data ke kumpulan kapasitas pada semua SnapLock volume, apa pun jenisnya. SnapLock Untuk informasi selengkapnya, lihat [Tingkat data volume](#).

SnapLockadministrator

Anda harus memiliki hak SnapLock administrator untuk melakukan tindakan tertentu pada SnapLock volume. SnapLockhak administrator didefinisikan dalam `vsadmin-snaplock` peran dalam ONTAP CLI. Anda harus menjadi administrator cluster untuk membuat akun administrator mesin virtual penyimpanan (SVM) dengan peran SnapLock administrator.

Anda dapat melakukan tindakan berikut dengan `vsadmin-snaplock` peran dalam ONTAP CLI:

- Kelola akun pengguna, kata sandi lokal, dan informasi kunci Anda sendiri
- Kelola volume, kecuali volume bergerak
- Mengelola kuota, qtrees, salinan snapshot, dan file
- Melakukan SnapLock tindakan, termasuk penghapusan hak istimewa dan Penahanan Hukum
- Konfigurasi protokol Network File System (NFS) dan Server Message Block (SMB)
- Konfigurasi layanan Sistem Nama Domain (DNS), Protokol Akses Direktori Ringan (LDAP), dan Layanan Informasi Jaringan (NIS)
- Pantau pekerjaan

Prosedur berikut merinci cara membuat SnapLock administrator di ONTAP CLI. Anda harus masuk sebagai administrator kluster pada koneksi aman, seperti Secure Shell Protocol (SSH) untuk melakukan tugas ini.

Untuk membuat akun administrator SVM dengan peran vsadmin-snaplock di CLI ONTAP

- Jalankan perintah berikut. Ganti *SVM_name* dan *SnapLockAdmin* dengan informasi Anda sendiri.

```
cluster1::> security login create -vserver SVM_name -user-or-group-  
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-  
snaplock
```

Untuk informasi selengkapnya, lihat [ONTAPperan dan pengguna](#).

SnapLockvolume log audit

Volume log SnapLock audit berisi log SnapLock audit, yang berisi cap waktu peristiwa seperti ketika SnapLock administrator dibuat, ketika operasi penghapusan hak istimewa dijalankan, atau ketika Penahanan Hukum ditempatkan pada file. Volume log SnapLock audit adalah catatan peristiwa yang tidak dapat dihapus.

Anda harus membuat volume log SnapLock audit dalam SVM yang sama dengan SnapLock volume untuk tindakan berikut:

- Untuk mengaktifkan atau menonaktifkan penghapusan hak istimewa pada volume SnapLock Perusahaan.
- Untuk menerapkan Penahanan Hukum pada file dalam volume SnapLock Kepatuhan.

Warning

- Periode retensi minimum untuk volume log SnapLock audit adalah enam bulan. Sampai periode retensi ini berakhir, volume log SnapLock audit dan SVM serta sistem file yang terkait dengannya tidak dapat dihapus meskipun volume dibuat dalam mode SnapLock Enterprise.
- Jika file dihapus menggunakan penghapusan hak istimewa dan periode retensi lebih lama dari periode penyimpanan volume, maka volume log audit mewarisi periode penyimpanan file. Misalnya, jika file yang memiliki periode retensi 10 bulan dihapus menggunakan penghapusan hak istimewa dan periode retensi volume log audit adalah enam bulan, periode retensi volume log audit diperpanjang hingga 10 bulan.

Anda hanya dapat memiliki satu volume log SnapLock audit aktif di SVM, tetapi dapat dibagikan oleh beberapa SnapLock volume di SVM. Untuk berhasil memasang volume log SnapLock audit, atur jalur persimpangan ke `/snaplock_audit_log`. Tidak ada volume lain yang dapat menggunakan jalur persimpangan ini, termasuk volume yang bukan volume log audit.

Anda dapat menemukan log SnapLock audit di `/snaplock_log` direktori di bawah akar volume log audit. Operasi penghapusan hak istimewa dicatat di `privdel_log` subdirektori. Penahanan Hukum mulai dan operasi akhir masuk `/snaplock_log/legal_hold_logs/`. Semua log lainnya disimpan di `system_log` subdirektori.

Anda dapat membuat volume log SnapLock audit dengan FSx konsol Amazon, Amazon FSx API, AWS CLI, dan ONTAP CLI dan REST API.

Note

Volume perlindungan data (DP) tidak dapat digunakan sebagai volume log SnapLock audit.

Untuk mengaktifkan volume log SnapLock audit dengan Amazon FSx API, gunakan `AuditLogVolume` di file [CreateSnaplockConfiguration](#). Di FSx konsol Amazon, untuk volume log Audit, pilih Diaktifkan. Pastikan bahwa jalur Junction diatur ke `/snaplock_audit_log`.

Mengakses data Anda dalam volume SnapLock

Anda dapat menggunakan protokol file terbuka seperti NFS dan SMB untuk mengakses data Anda dalam volume. SnapLock Tidak ada dampak kinerja dari menulis data ke SnapLock volume atau dari membaca data yang dilindungi oleh WORM.

Anda dapat menyalin file di seluruh SnapLock volume dengan NFS dan SMB, tetapi mereka tidak akan mempertahankan properti WORM mereka pada volume tujuan SnapLock. Anda harus mengkomit ulang file yang disalin ke WORM untuk mencegahnya dimodifikasi atau dihapus. Untuk informasi selengkapnya, lihat [Mengkomit file ke status WORM](#).

Anda juga dapat mereplikasi SnapLock data dengan SnapMirror, tetapi volume sumber dan tujuan harus SnapLock volume dengan mode retensi yang sama (misalnya, keduanya harus Kepatuhan atau Perusahaan).

SnapLock dan kapasitas SSD mengurangi operasi

Pertimbangkan poin-poin ini tentang penurunan SSD sebelum membuat SnapLock volume:

- Amazon FSx akan menolak permintaan penurunan kapasitas SSD pada sistem file yang berisi SnapLock volume.
- Anda tidak dapat membuat SnapLock volume selama operasi penurunan kapasitas SSD.

Keterbatasan ini ada karena ONTAP memberlakukan periode retensi minimum 6 bulan untuk volume log SnapLock audit, yang akan mencegah penghapusan sistem file selama periode itu jika SnapLock volume dipindahkan sebagai bagian dari operasi penurunan SSD.

Jika Anda perlu mengurangi kapasitas SSD pada sistem file dengan SnapLock volume, Anda perlu memigrasikan data Anda ke sistem file baru dengan kapasitas SSD yang lebih kecil. Untuk informasi selengkapnya tentang penurunan kapasitas SSD operasi, termasuk batasan dan pertimbangan, lihat [Memperbarui penyimpanan SSD sistem file dan IOPS](#).

Memahami SnapLock Kepatuhan

Bagian ini menjelaskan kasus penggunaan dan pertimbangan untuk mode retensi SnapLock Kepatuhan.

Anda dapat memilih mode retensi Kepatuhan untuk kasus penggunaan berikut.

- Anda dapat menggunakan SnapLock Kepatuhan untuk menangani mandat khusus pemerintah atau industri seperti Aturan SEC 17a-4 (f), Aturan FINRA 4511, dan Peraturan CFTC 1.31. SnapLock Kepatuhan di Amazon FSx untuk NetApp ONTAP dinilai untuk mandat dan peraturan ini oleh Cohasset Associates Untuk informasi selengkapnya, lihat [Laporan Penilaian Kepatuhan untuk Amazon FSx untuk NetApp ONTAP](#).
- Anda dapat menggunakan SnapLock Kepatuhan untuk melengkapi atau meningkatkan strategi perlindungan data yang komprehensif untuk memerangi serangan ransomware.

Berikut adalah beberapa hal penting yang perlu dipertimbangkan tentang mode retensi SnapLock Kepatuhan.

- Setelah file dialihkan ke status tulis sekali, baca many (WORM) pada volume SnapLock Kepatuhan, file tersebut tidak dapat dihapus sebelum periode retensi berakhir oleh pengguna mana pun.
- Volume SnapLock Kepatuhan hanya dapat dihapus ketika periode retensi semua file WORM pada volume telah kedaluwarsa, dan file WORM telah dihapus dari volume.
- Anda tidak dapat mengganti nama volume SnapLock Kepatuhan setelah pembuatan.

- Anda dapat menggunakan SnapMirror untuk mereplikasi file WORM, tetapi volume sumber dan volume tujuan harus memiliki mode retensi yang sama (misalnya, keduanya harus Kepatuhan).
- Volume SnapLock Kepatuhan tidak dapat dikonversi ke volume SnapLock Perusahaan, dan sebaliknya.

Memahami SnapLock Perusahaan

Bagian ini menjelaskan kasus penggunaan dan pertimbangan untuk mode retensi SnapLock Perusahaan.

Anda dapat memilih mode retensi SnapLock Enterprise untuk kasus penggunaan berikut.

- Anda dapat menggunakan SnapLock Enterprise untuk mengotorisasi hanya pengguna tertentu untuk menghapus file.
- Anda dapat menggunakan SnapLock Enterprise untuk memajukan integritas data dan kepatuhan internal organisasi Anda.
- Anda dapat menggunakan SnapLock Enterprise untuk menguji setelan retensi sebelum menggunakan SnapLock Kepatuhan.

Berikut adalah beberapa hal penting yang perlu dipertimbangkan tentang mode retensi SnapLock Perusahaan.

- Anda dapat menggunakan SnapMirror untuk mereplikasi file WORM, tetapi volume sumber dan volume tujuan harus memiliki mode retensi yang sama (misalnya, keduanya harus Enterprise).
- SnapLockVolume tidak dapat dikonversi dari Perusahaan ke Kepatuhan, atau dari Kepatuhan ke Perusahaan.
- SnapLockEnterprise tidak mendukung Legal Hold.

Menggunakan penghapusan hak istimewa

Salah satu perbedaan utama antara SnapLock Perusahaan dan SnapLock Kepatuhan adalah SnapLock administrator dapat mengaktifkan penghapusan hak istimewa pada volume SnapLock Perusahaan untuk memungkinkan file dihapus sebelum periode penyimpanan file berakhir.

SnapLockAdministrator adalah satu-satunya pengguna yang dapat menghapus file dari volume SnapLock Perusahaan yang memiliki kebijakan retensi aktif yang ditempatkan di dalamnya. Untuk informasi selengkapnya, lihat [SnapLockadministrator](#).

Anda dapat mengaktifkan atau menonaktifkan penghapusan istimewa dengan FSx konsol Amazon, Amazon FSx API AWS CLI, dan ONTAP CLI dan REST API. Untuk mengaktifkan penghapusan hak istimewa, Anda harus terlebih dahulu membuat volume log SnapLock audit dalam SVM yang sama dengan SnapLock volume. Untuk informasi selengkapnya, lihat [SnapLockvolume log audit](#).

Untuk mengaktifkan penghapusan hak istimewa dengan Amazon FSx API, gunakan PrivilegedDelete di file. [CreateSnaplockConfiguration](#) Di FSx konsol Amazon, untuk Privileged Delete, pilih Diaktifkan.

Note

Anda tidak dapat mengeluarkan perintah hapus dengan hak istimewa untuk menghapus file tulis sekali, baca banyak (WORM) yang memiliki periode retensi kedaluwarsa. Anda dapat mengeluarkan operasi penghapusan normal setelah periode retensi berakhir.

Anda dapat memilih untuk menonaktifkan penghapusan hak istimewa secara permanen, tetapi tindakan ini tidak dapat diubah. Jika penghapusan hak istimewa dimatikan secara permanen, Anda tidak perlu memiliki volume log SnapLock audit yang terkait dengan volume SnapLock Perusahaan.

Untuk mematikan penghapusan hak istimewa secara permanen dengan Amazon FSx API, gunakan PrivilegedDelete di file. [CreateSnaplockConfiguration](#) Di FSx konsol Amazon, untuk Hapus Hak Istimewa, pilih Dinonaktifkan secara permanen.

Melewati mode SnapLock Enterprise

Jika Anda menggunakan FSx konsol Amazon atau Amazon FSx API, Anda harus memiliki `fsx:BypassSnapLockEnterpriseRetention` izin IAM untuk menghapus volume SnapLock Perusahaan yang berisi file WORM dengan kebijakan retensi aktif.

Untuk informasi selengkapnya, lihat [Menghapus volume SnapLock](#).

Memahami periode SnapLock retensi

Saat membuat SnapLock volume, Anda dapat mengatur periode retensi default untuk volume, atau Anda dapat mengatur periode retensi untuk menulis sekali, membaca banyak file (WORM) secara eksplisit. Selama periode penyimpanan, Anda tidak dapat menghapus atau memodifikasi file yang dilindungi Worm. Periode retensi digunakan untuk menghitung waktu retensi. Misalnya, jika Anda

mentransisikan file ke WORM pada 14 Juli 2023 pada tengah malam dan mengatur periode retensi menjadi lima tahun, maka waktu retensi akan sampai 14 Juli 2028 pada tengah malam.

Untuk informasi lebih lanjut tentang WORM, lihat [Mengkomit file ke status WORM](#).

Kebijakan periode retensi

Periode retensi ditentukan oleh nilai yang Anda tetapkan ke parameter berikut:

- Retensi default — Periode retensi default yang ditetapkan ke file WORM jika Anda tidak memberikan periode retensi eksplisit untuk file tersebut.
- Retensi minimum — Periode retensi terpendek yang dapat ditetapkan ke file WORM.
- Retensi maksimum - Periode retensi terpanjang yang dapat ditetapkan ke file WORM.

Note

Bahkan setelah periode retensi berakhir, Anda tidak dapat memodifikasi file WORM. Anda hanya dapat menghapusnya atau mengatur periode retensi baru untuk mengaktifkan perlindungan WORM lagi.

Anda dapat menentukan periode retensi menggunakan beberapa unit waktu yang berbeda. Tabel berikut mencantumkan rentang spesifik yang didukung.

Tipe	Nilai	Catatan
Detik	0 - 65,535	
Menit	0 - 65,535	
Jam	0 - 24	
Hari	0 - 365	
Bulan	0 -12	
Tahun	0 - 100	

Tipe	Nilai	Catatan
Tak terbatas	-	Mempertahankan file selamanya. Tersedia untuk Retensi default, Retensi maksimum, dan Retensi minimum.
Tidak ditentukan 1	-	Mempertahankan file sampai Anda menetapkan periode retensi. Hanya tersedia untuk retensi default.

Note

¹ Saat Anda mentransisikan file ke WORM dengan periode retensi yang tidak ditentukan, file tersebut diberikan periode retensi minimum yang dikonfigurasi untuk SnapLock volume. Saat Anda mentransisikan file yang dilindungi Worm ke waktu retensi absolut, periode retensi baru harus lebih besar dari periode minimum yang Anda tetapkan pada file sebelumnya.

Periode retensi kedaluwarsa

Setelah periode penyimpanan file WORM berakhir, Anda dapat menghapus file atau menetapkan periode retensi baru untuk mengaktifkan kembali perlindungan WORM. File WORM tidak dihapus secara otomatis setelah periode retensi berakhir. Anda masih tidak dapat memodifikasi konten file WORM, bahkan setelah periode retensi telah kedaluwarsa.

Mengatur periode retensi SnapLock volume

Anda dapat mengatur periode retensi SnapLock volume dengan FSx konsol Amazon, Amazon FSx API AWS CLI, dan ONTAP CLI dan REST API.

Untuk mengatur periode retensi dengan Amazon FSx API, gunakan

[SnaplockRetentionPeriod](#) konfigurasi. Di FSx konsol Amazon, untuk periode Retensi, masukkan

nilai untuk Retensi default, Retensi minimum, dan Retensi maksimum. Kemudian pilih Unit yang sesuai untuk masing-masing.

Mengkomit file ke status WORM

Bagian ini membahas bagaimana Anda dapat mentransisikan file Anda ke status tulis sekali, baca banyak (WORM). Ini juga membahas mode volume-append, yang merupakan cara untuk menulis data secara bertahap ke file yang dilindungi Worm.

Komit otomatis

Anda dapat menggunakan autocommit untuk mentransisikan file ke WORM jika file tersebut belum dimodifikasi untuk jangka waktu yang Anda tentukan. Anda dapat mengaktifkan komit otomatis dengan FSx konsol Amazon, FSx API Amazon AWS CLI, dan ONTAP CLI dan REST API.

Anda dapat menentukan periode komit otomatis antara lima menit dan 10 tahun. Tabel berikut mencantumkan rentang spesifik yang didukung.

Unit	Nilai
Menit	5 - 65,535
Jam	1 - 65,535
Hari	1 - 3,650
Bulan	1 - 120
Tahun	1 - 10

Untuk mengaktifkan komit otomatis dengan Amazon FSx API, gunakan `AutocommitPeriod` di file. [CreateSnaplockConfiguration](#) Di FSx konsol Amazon, untuk Komit Otomatis, pilih Diaktifkan. Kemudian, untuk periode Autocommit, masukkan nilai dan pilih unit Autocommit yang sesuai.

Anda dapat menentukan nilai antara 5 menit dan 10 tahun.

Mode Volume-append

Anda tidak dapat mengubah data yang ada dalam file yang dilindungi Worm. Namun, SnapLock memungkinkan Anda untuk mempertahankan perlindungan untuk data yang ada menggunakan file

Worm-appendable. Misalnya, Anda dapat membuat file log atau menyimpan data streaming audio atau video sambil menulis data secara bertahap. Anda dapat mengaktifkan atau menonaktifkan mode volume-append dengan FSx konsol Amazon, Amazon FSx API, dan ONTAP CLI dan REST API.

AWS CLI

Persyaratan untuk memperbarui mode volume-append

- SnapLockVolume harus dilepas.
- SnapLockVolume harus kosong dari salinan snapshot dan data pengguna.

Untuk mengaktifkan mode volume-append dengan Amazon FSx API, gunakan `VolumeAppendModeEnabled` di file. [CreateSnaplockConfiguration](#) Di FSx konsol Amazon, untuk mode Volume append, pilih Diaktifkan.

Retensi berbasis peristiwa (EBR)

Anda dapat menggunakan retensi berbasis peristiwa (EBR) untuk membuat kebijakan khusus dengan periode retensi terkait. Misalnya, Anda dapat mentransisikan semua file di jalur tertentu ke WORM dan mengatur periode retensi selama satu tahun dengan `snaplock event-retention apply` perintah `snaplock event-retention policy create` dan. Bila Anda menggunakan EBR, Anda harus menentukan volume, direktori, atau file. Periode penyimpanan yang Anda pilih saat membuat kebijakan EBR diterapkan ke semua file di jalur yang ditentukan.

EBR didukung oleh ONTAP CLI dan REST API.

Note

ONTAP tidak mendukung EBR dengan FlexGroup volume.

Prosedur berikut menjelaskan cara membuat, menerapkan, memodifikasi, dan menghapus kebijakan EBR. Anda harus menjadi SnapLock administrator (memiliki `vsadmin-snaplock` peran) untuk menyelesaikan tugas-tugas ini di ONTAP CLI. Untuk informasi selengkapnya, lihat [SnapLock administrator](#).

Membuat kebijakan EBR di CLI ONTAP

Untuk membuat kebijakan EBR di CLI ONTAP

- Jalankan perintah berikut. Ganti *p1* dan *"10 years"* dengan informasi Anda sendiri.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

Menerapkan kebijakan EBR di CLI ONTAP

Untuk menerapkan kebijakan EBR di CLI ONTAP

- Jalankan perintah berikut. Ganti *p1* dan *slc* dengan informasi Anda sendiri. Anda dapat menambahkan jalur setelah garis miring maju (/) jika Anda ingin menentukan jalur tertentu untuk kebijakan EBR. Jika tidak, perintah ini menerapkan kebijakan EBR ke semua file pada volume.

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

Memodifikasi kebijakan EBR di CLI ONTAP

Untuk memodifikasi kebijakan EBR di CLI ONTAP

- Jalankan perintah berikut. Ganti *p1* dan *"5 years"* dengan informasi Anda sendiri.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

Menghapus kebijakan EBR di CLI ONTAP

Untuk menghapus kebijakan EBR di CLI ONTAP

- Jalankan perintah berikut. Ganti *p1* dengan informasi Anda sendiri.

```
vs1::> snaplock event-retention policy delete -name p1
```

Perintah terkait di Pusat NetApp Dokumentasi:

- [pembatalan retensi acara snaplock](#)

- [snaplock acara-retensi acara show-vservers](#)
- [pertunjukan retensi acara snaplock](#)
- [tampilan kebijakan retensi acara snaplock](#)

Penahanan Hukum

Anda dapat menyimpan file WORM untuk jangka waktu yang tidak terbatas menggunakan Legal Hold. Legal Hold umumnya digunakan untuk tujuan litigasi. File WORM yang tunduk pada Penahanan Hukum tidak dapat dihapus sampai Penahanan Hukum dicabut.

Legal Hold didukung oleh ONTAP CLI dan REST API.

Note

ONTAP tidak mendukung Legal Hold dengan FlexGroup volume.

Prosedur berikut menjelaskan cara memulai dan mengakhiri Penahanan Hukum. Anda harus menjadi SnapLock administrator (memiliki `vsadmin-snaplock` peran) untuk menyelesaikan tugas-tugas ini di ONTAP CLI. Untuk informasi selengkapnya, lihat [SnapLock administrator](#).

Memulai Penahanan Hukum pada file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

Untuk memulai Penahanan Hukum pada file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

- Jalankan perintah berikut. Ganti *litigation1slc_vol1*, dan *file1* dengan informasi Anda sendiri.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -  
path /file1
```

Memulai Penahanan Hukum pada semua file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

Untuk memulai Penahanan Hukum pada semua file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

- Jalankan perintah berikut. Ganti *litigation1* dan *slc_vol1* dengan informasi Anda sendiri.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -  
path /
```

Mengakhiri Penahanan Hukum pada file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

Untuk mengakhiri Penahanan Hukum pada file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

- Jalankan perintah berikut. Ganti *litigation1slc_vol1*, dan *file1* dengan informasi Anda sendiri.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -  
path /file1
```

Note

Kami menyarankan Anda memantau `-operation-status` dengan `snaplock legal-hold show` perintah saat mengeluarkan Penahanan Hukum untuk memastikan bahwa itu tidak gagal.

Mengakhiri Penahanan Hukum pada semua file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

Untuk mengakhiri Penahanan Hukum pada semua file dalam volume SnapLock Kepatuhan dengan ONTAP CLI

- Jalankan perintah berikut. Ganti *litigation1* dan *slc_vol1* dengan informasi Anda sendiri.


```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -  
path /
```

Note

Kami menyarankan Anda memantau `-operation-status` dengan `snaplock legal-hold show` perintah saat mengeluarkan Penahanan Hukum untuk memastikan bahwa itu tidak gagal.

Perintah terkait di Pusat NetApp Dokumentasi:

- [pembatalan penahanan hukum snaplock](#)
- [snaplock dump-file penahanan hukum](#)
- [snaplock dump-litigasi penahanan hukum](#)
- [pertunjukan penahanan hukum snaplock](#)

Mereplikasi data Anda dengan FlexCache

FlexCache adalah kemampuan caching NetApp ONTAP's jarak jauh yang membawa dataset lebih dekat ke klien, meningkatkan kinerja akses dan mengurangi biaya. Ini menyederhanakan distribusi file dan mengurangi biaya WAN. Saat Anda membuat FlexCache volume, awalnya hanya menyalin metadata dari sistem file asal. Pendekatan ini lebih cepat dan lebih hemat ruang daripada salinan data lengkap, hanya menghabiskan sebagian kecil dari kapasitas penyimpanan.

Cara kerja FlexCache

FlexCacheVolume adalah cache yang jarang penduduknya yang menyediakan akses ke data yang disimpan dalam volume asal. Cache dapat ditemukan di sistem file yang berbeda, secara opsional jarak jauh. Alih-alih menyalin semua data dari volume asal, FlexCache menyalin data hanya sesuai kebutuhan. FlexCache volume paling cocok untuk alur kerja intensif baca dengan perubahan data yang jarang terjadi karena setiap perubahan pada data asal memerlukan cache untuk di-refresh.

Anda dapat menggunakan FlexCache dengan FSx untuk ONTAP dalam konfigurasi berikut:

Volume asal	FlexCache volume
Di premis NetApp ONTAP	FSx untuk ONTAP
FSx untuk ONTAP	Di premis NetApp ONTAP
FSx untuk ONTAP	FSx untuk ONTAP

FlexCachemenulis mode

FlexCachevolume mendukung dua mode operasi untuk operasi tulis: mode write-around dan mode write-back.

Dalam mode write-around, yang merupakan mode default, penulisan diteruskan dari cache ke volume asal. Operasi tulis tidak diakui ke klien sampai setelah data berkomitmen ke penyimpanan pada volume asal dan asal mengakui penulisan kembali ke cache. Karena setiap penulisan harus melintasi jaringan antara cache dan asal, mode ini memiliki latensi yang lebih tinggi daripada mode tulis kembali.

Dalam mode write-back, diperkenalkan pada ONTAP 9.15.1, penulisan berkomitmen untuk penyimpanan di lokasi cache dan segera diakui ke klien. Data tersebut kemudian ditulis secara asinkron ke volume asal. Mode ini memungkinkan penulisan untuk bekerja pada kecepatan mendekati lokal, yang secara signifikan dapat meningkatkan kinerja untuk beban kerja terdistribusi.

Gunakan mode tulis kembali untuk beban kerja berat tulis yang memerlukan penulisan cache latensi rendah. Gunakan mode write-around untuk beban kerja baca-berat yang tidak sensitif terhadap latensi, atau ketika sistem file asal Anda memiliki lebih dari 10 volume asal. FlexCache

FlexCacheikhtisar pembuatan volume

Membuat FlexCache volume terdiri dari langkah-langkah berikut:

1. Kumpulkan antarmuka logis sumber dan tujuan () LIFs
2. Membangun cluster peering antara sistem file asal dan cache
3. Buat hubungan peering mesin virtual penyimpanan (SVM)
4. Buat FlexCache volume dan pilih mode tulis
5. Pasang FlexCache volume pada klien Anda

Untuk petunjuk mendetail, lihat [MembuatFlexCache](#).

MembuatFlexCache

Dengan menggunakan prosedur berikut, Anda akan membuat FlexCache volume di Amazon FSx untuk sistem file NetApp ONTAP, yang didukung oleh volume asal yang terletak di kluster lokalNetApp ONTAP.

Menggunakan CLI ONTAP

Anda akan menggunakan ONTAP CLI untuk membuat dan mengelola FlexCache konfigurasi pada sistem file ONTAP Anda FSx .

Perintah dalam prosedur ini menggunakan alias berikut untuk cluster, SVM, dan volume:

- `Cache_ID`— ID cache cluster (dalam format FSx idabcdef1234567890a)
- `Origin_ID`— ID cluster asal
- `CacheSVM`— nama cache SVM
- `OriginSVM`— nama SVM asal
- `OriginVol`— nama volume asal
- `CacheVol`— nama FlexCache volume

Prosedur di bagian ini menggunakan perintah NetApp ONTAP CLI berikut.

- [network interfaces show](#)
- [cluster peer](#)perintah
- [volume flexcache create](#)

Prasyarat

Sebelum Anda mulai menggunakan prosedur di bagian berikut, pastikan Anda telah memenuhi prasyarat berikut:

- Sistem file sumber dan tujuan terhubung dalam VPC yang sama, atau berada di jaringan yang diintegrasikan menggunakan Amazon VPC,,, atau. AWS Transit Gateway Direct Connect Site-to-Site VPN Untuk informasi lebih lanjut, lihat [Mengakses data dari dalam AWS Cloud](#) dan [Apa itu VPC peering?](#) di Panduan Peering VPC Amazon.

- Grup keamanan VPC untuk sistem file ONTAP memiliki aturan masuk dan keluar yang memungkinkan ICMP serta TCP pada port 11104 dan 11105 untuk titik akhir antar-cluster () Anda. FSx LIFs
- Anda telah membuat tujuan FSx untuk sistem file ONTAP dengan SVM, tetapi Anda belum membuat volume yang akan digunakan sebagai file. FlexCache Untuk informasi selengkapnya, lihat [Membuat sistem file](#).

Rekam sumber dan tujuan antar cluster LIFs

1. Untuk sistem file FSx for ONTAP yang merupakan cluster tujuan:
 - a. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
 - b. Pilih sistem File, lalu pilih sistem file FSx untuk ONTAP yang merupakan cluster tujuan untuk membuka halaman detail sistem file.
 - c. Di Administrasi, temukan titik akhir Inter-cluster - alamat IP, dan catat nilainya.

Note

Untuk sistem file scale-out, ada dua alamat IP titik akhir antar-cluster untuk setiap pasangan ketersediaan tinggi (HA).

2. Untuk kluster sumber lokal, ambil alamat IP LIF antar-cluster menggunakan perintah CLI berikut: ONTAP

```
Origin::> network interface show -role intercluster
```

Logical Vserver	Interface	Status	Network Address/Mask
OriginSVM	inter_1	up/up	10.0.0.36/24
	inter_2	up/up	10.0.1.69/24

3. Simpan inter_1 dan inter_2 IP alamatnya. Mereka direferensikan dalam OriginSVM alias as origin_inter_1 dan origin_inter_2 dan CacheSVM alias as dan. cache_inter_1 cache_inter_2

Membangun cluster peering antara asal dan cache

Membangun hubungan rekan cluster pada Cache dan Source cluster menggunakan perintah [cluster peer create](#) ONTAP CLI. Anda akan memberikan alamat IP antar-cluster yang Anda simpan sebelumnya dalam prosedur. [Rekam sumber dan tujuan antar cluster LIFs](#) Saat diminta, Anda akan diminta untuk membuat *cluster-peer-passphrase* yang harus Anda masukkan saat Anda membuat cluster peering di Origin cluster.

1. Siapkan cluster peering pada Cache cluster (FSx untuk sistem file ONTAP Anda).
 - a. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

- b. Gunakan perintah berikut, dan catat kata sandi yang Anda buat. Untuk sistem file scale-out, berikan alamat inter_2 IP inter_1 dan IP untuk setiap pasangan HA.

```
FSx-Cache::> cluster peer create -address-family ipv4 -peer-  
addrs origin_inter_1,origin_inter_2
```

Enter the passphrase: *cluster-peer-passphrase*

Confirm the passphrase: *cluster-peer-passphrase*

Notice: Now use the same passphrase in the "cluster peer create" command in the other cluster.

2. Gunakan perintah berikut untuk menyiapkan pengintip klaster di klaster source (lokal). Anda harus memasukkan frasa sandi yang Anda buat pada langkah sebelumnya untuk mengautentikasi. Untuk sistem file scale-out, Anda harus memberikan alamat IP antar-cluster untuk setiap pasangan HA.

```
Origin::> cluster peer create -address-family ipv4 -peer-  
addrs cache_inter_1,cache_inter_2
```

Enter the passphrase: *cluster-peer-passphrase*

Confirm the passphrase: *cluster-peer-passphrase*

3. Di source cluster, verifikasi bahwa pengintip cluster berhasil diatur menggunakan perintah berikut. Dalam output, Availability harus diatur ke Available.

```
Origin::> cluster peer show
```

Peer Cluster Name	Availability	Authentication
-----	-----	-----
Cache_ID	Available	ok

Jika output tidak muncul Available, ulangi langkah sebelumnya pada source dan cache cluster.

Konfigurasi pengintip mesin virtual penyimpanan (SVM)

Setelah Anda berhasil membuat cluster peering, langkah selanjutnya adalah membuat hubungan peering SVM pada cluster cache (Cache) menggunakan perintah. `vserver peer` Alias tambahan yang digunakan dalam prosedur berikut adalah sebagai berikut:

- **CacheLocalName**— nama yang digunakan untuk mengidentifikasi cache SVM saat mengonfigurasi SVM mengintip SVM. `origin`
- **OriginLocalName**— nama yang digunakan untuk mengidentifikasi origin SVM saat mengonfigurasi SVM mengintip SVM. `cache`

1. Pada cache SVM, gunakan perintah berikut untuk membuat hubungan peering SVM.

```
FSx-Cache::> vserver peer create -vserver CacheSVM -peer-vserver OriginSVM -peer-cluster Origin_ID -local-name OriginLocalName -application flexcache
```

2. Pada cluster sumber, gunakan perintah berikut untuk menerima hubungan peering SVM.

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-name CacheLocalName
```

3. Pada cluster sumber, terima hubungan peering.

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-name CacheLocalName
```

4. Verifikasi bahwa peering SVM berhasil menggunakan perintah berikut; Peer State harus disetel ke `peered` dalam respons.

```
Origin::> vservers peer show
```

Vserver	Peer Vserver	Peer State	Peering Cluster	Remote Applications
-----	-----	-----	-----	
OriginSVM	CacheSVM	peered	FSx-Cache	flexcache

Buat FlexCache volume

Setelah berhasil membuat hubungan peering SVM, langkah selanjutnya adalah membuat FlexCache volume pada cache SVM. FlexCacheVolume harus aFlexGroup. Anda juga akan memilih mode operasi untuk FlexCache volume Anda. Untuk informasi selengkapnya, lihat [FlexCachemenulis mode](#).

1. Pada cluster cache, gunakan perintah ONTAP CLI berikut untuk membuat FlexCache volume Anda. Contoh ini membuat FlexCache volume 2 TB bernama *CacheVol*.
 - Untuk membuat FlexCache volume write-around, gunakan perintah berikut.

```
FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
               -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
               aggr-list aggr1
```

- Untuk membuat FlexCache volume write-back, gunakan perintah berikut.

```
FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
               -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
               aggr-list aggr1 -is-writeback-enabled true
```

Note

Anda dapat menggunakan `volume flexcache config modify -is-writeback-enabled {true|false}` perintah untuk memodifikasi mode tulis. Sebelum

menggunakan perintah ini, pastikan Anda masuk ke mode lanjutan ONTAP CLI dengan menggunakan `set -privilege advanced` perintah.

2. Verifikasi FlexCache hubungan antara FlexCache volume dan volume asal.

- Untuk volume FlexCache penulisan, output Anda akan terlihat mirip dengan contoh berikut.

```
FSx-Cache::> volume flexcache show
```

Vserver	Volume	Size	Origin-Vserver	Origin-Volume	Origin-Cluster
-----	-----	-----	-----	-----	-----
CacheSVM	CacheVol	2TB	OriginSVM	OriginVol	Origin

- Untuk volume FlexCache write-back, output Anda akan terlihat mirip dengan contoh berikut.

```
FSx-Cache::> volume flexcache show
```

Vserver	Volume	Size	Origin-Vserver	Origin-Volume	Origin-Cluster
Writeback					
-----	-----	-----	-----	-----	-----

CacheSVM	CacheVol	2TB	OriginSVM	OriginVol	Origin
true					

Pasang FlexCache volumenya

Setelah FlexCache volume menjadi TERSEDIA,, NFSv3 NFSv4, dan klien SMB dapat memasangnya. Setelah FlexCache dipasang, klien memiliki akses ke seluruh kumpulan data pada volume asal di lokasi.

- Untuk membuat titik pemasangan dan memasang FlexCache, jalankan perintah berikut pada klien:

```
$ sudo mkdir -p /fsx/CacheVol
$ sudo mount -t nfs management.fs-01d2f606463087f6d.fsx.us-east-1.amazonaws.com:/
CacheVol /fsx/CacheVol
```


Mereplikasi data Anda menggunakan NetApp SnapMirror

Anda dapat menggunakan NetApp SnapMirror untuk menjadwalkan replikasi berkala FSx untuk sistem file ONTAP Anda ke atau dari sistem file kedua. Kemampuan ini tersedia untuk penyebaran dalam wilayah dan lintas wilayah.

NetApp SnapMirror mereplikasi data dengan kecepatan tinggi, sehingga Anda mendapatkan ketersediaan data yang tinggi dan replikasi data yang cepat di seluruh ONTAP sistem, baik Anda mereplikasi antara dua sistem FSx file Amazon di AWS, atau dari lokal ke. AWS Replikasi dapat dijadwalkan sesering setiap 5 menit, meskipun interval harus dipilih dengan cermat berdasarkan RPOs (Tujuan Titik Pemulihan), RTOs (Tujuan Waktu Pemulihan), dan pertimbangan kinerja.

Ketika Anda mereplikasi data ke sistem NetApp penyimpanan dan terus memperbarui data sekunder, data Anda tetap terkini dan tetap tersedia kapan pun Anda membutuhkannya. Tidak diperlukan server replikasi eksternal. Untuk informasi selengkapnya tentang penggunaan NetApp SnapMirror untuk mereplikasi data Anda, lihat [Pelajari tentang NetApp Replikasi](#) dalam dokumentasi. NetApp Console

Anda dapat membuat volume tujuan perlindungan data (DP) untuk NetApp SnapMirror menggunakan FSx konsol Amazon, FSx API Amazon AWS CLI, dan Amazon, selain NetApp ONTAP CLI dan REST API. Untuk informasi tentang membuat volume tujuan menggunakan FSx konsol Amazon dan AWS CLI, lihat [Membuat volume](#).

Anda dapat menggunakan NetApp Console atau ONTAP CLI untuk menjadwalkan replikasi untuk sistem file Anda.

Note

Ada dua jenis SnapMirror replikasi: Volume-level SnapMirror dan SVM Disaster Recovery (SVMDR). Hanya SnapMirror replikasi tingkat volume yang didukung oleh FSx untuk ONTAP. Synchronous SnapMirror, termasuk StrictSync, tidak didukung.

Menggunakan NetApp Console untuk menjadwalkan replikasi

Anda dapat menggunakan NetApp Console untuk mengatur replikasi dengan SnapMirror pada sistem file FSx ONTAP Anda. Untuk informasi selengkapnya, lihat [Mengatur replikasi data di NetApp Replikasi](#) di dokumentasi NetApp Konsol.

Menggunakan ONTAP CLI untuk menjadwalkan replikasi

Anda dapat menggunakan ONTAP CLI untuk mengonfigurasi replikasi volume terjadwal. Untuk selengkapnya, lihat [Mengelola replikasi SnapMirror volume](#) di Pusat NetApp ONTAP Dokumentasi.

AWS laporan penagihan dan penggunaan FSx untuk ONTAP

AWS menyediakan dua laporan penggunaan FSx untuk ONTAP:

- Laporan AWS penagihan adalah tampilan tingkat tinggi dari semua aktivitas Layanan AWS yang Anda gunakan, termasuk FSx untuk ONTAP.
- Laporan AWS penggunaan adalah ringkasan aktivitas untuk layanan tertentu, digabungkan berdasarkan jam, hari, atau bulan. Ini juga mencakup grafik penggunaan yang memberikan representasi grafis Anda FSx untuk penggunaan ONTAP.

Note

Seperti lainnya Layanan AWS, FSx untuk ONTAP menagih Anda hanya untuk apa yang Anda gunakan. Untuk informasi selengkapnya, lihat [Amazon FSx untuk Harga NetApp ONTAP](#).

Lihat laporan AWS penagihan FSx untuk ONTAP

Anda dapat melihat ringkasan AWS penggunaan dan biaya Anda, yang tercantum berdasarkan layanan, di halaman Tagihan di AWS Manajemen Penagihan dan Biaya konsol.

Untuk melihat laporan AWS penagihan

1. Masuk ke Konsol Manajemen AWS dan buka AWS Manajemen Penagihan dan Biaya konsol di <https://console.aws.amazon.com/costmanagement/>.
2. Di panel navigasi, pilih Tagihan.
3. Pilih periode Penagihan (misalnya, Agustus 2024).
4. Untuk melihat FSx tagihan Amazon, pada tab Biaya berdasarkan layanan, masukkan FSx bidang teks filter menurut layanan, lalu perluas FSx untuk melihat biaya menurut Wilayah AWS.

Biaya FSx untuk sistem file ONTAP muncul di bawah entri Amazon: onTAP FSx CreateFileSystem dalam laporan.

5. Untuk mengunduh laporan penagihan terperinci dalam format CSV, pilih Unduh semua ke CSV di bagian atas halaman Tagihan.

Untuk informasi selengkapnya tentang AWS tagihan [Anda, lihat Melihat tagihan Anda](#) di Panduan AWS Billing Pengguna.

Laporan penagihan mencakup jenis penggunaan berikut yang berlaku FSx untuk sistem file ONTAP:

First generation FSx for ONTAP file systems

Jenis biaya	Unit	Deskripsi	
Penyimpanan SSD ONTAP Single-AZ	GB-Bulan	Jumlah penyimpanan SSD yang disediakan pada sistem file ONTAP Single-AZ generasi pertama	
Penyimpanan SSD Multi-AZ ONTAP	GB-Bulan	Jumlah penyimpanan SSD yang disediakan pada Multi-AZ FSx generasi pertama untuk sistem file ONTAP	
Kapasitas throughput ONTAP Single-AZ	MBps-Bulan	Jumlah kapasitas throughput yang disediakan pada FSx single-AZ generasi pertama untuk sistem file ONTAP	
Kapasitas throughput Multi-AZ ONTAP	MBps-Bulan	Jumlah kapasitas throughput yang disediakan pada FSx Multi-AZ generasi pertama untuk sistem file ONTAP	
IOPS SSD ONTAP Single-AZ yang disediakan	IOPS - Bulan	Jumlah IOPS SSD yang disediakan pada FSx single-AZ generasi pertama untuk sistem file ONTAP	
IOPS SSD Multi-AZ ONTAP yang disediakan	IOPS - Bulan	Jumlah IOPS SSD yang disediakan pada FSx Multi-AZ generasi pertama untuk sistem file ONTAP	

Second generation FSx for ONTAP file systems

Jenis biaya	Unit	Deskripsi	
Penyimpanan SSD ONTAP Single-AZ-2	GB-Bulan	Jumlah penyimpanan SSD yang disediakan pada FSx single-AZ generasi kedua untuk sistem file ONTAP	
Penyimpanan SSD Multi-AZ-2 ONTAP	GB-Bulan	Jumlah penyimpanan SSD yang disediakan pada FSx Multi-AZ generasi kedua untuk sistem file ONTAP	
Kapasitas throughput ONTAP Single-AZ-2	MBps-Bulan	Jumlah kapasitas throughput yang disediakan pada single-AZ generasi kedua untuk sistem file ONTAP FSx	
Kapasitas throughput Multi-AZ-2 ONTAP	MBps-Bulan	Jumlah kapasitas throughput yang disediakan pada Multi-AZ generasi kedua untuk sistem file ONTAP FSx	
IOPS SSD ONTAP Single-AZ-2 yang disediakan	IOPS - Bulan	Jumlah IOPS SSD yang disediakan pada AZ tunggal generasi kedua untuk sistem file ONTAP FSx	
IOPS SSD Multi-AZ-2 ONTAP yang disediakan	IOPS - Bulan	Jumlah IOPS SSD yang disediakan pada Multi-AZ generasi kedua untuk sistem file ONTAP FSx	

All FSx for ONTAP filesystems

Jenis biaya	Unit	Deskripsi	
Penyimpanan kolam kapasitas standar ONTAP	GB-Bulan	Jumlah penyimpanan kolam kapasitas yang digunakan oleh sistem file FSx for ONTAP.	
Penyimpanan cadangan ONTAP	GB-Bulan	Jumlah kapasitas penyimpanan yang digunakan untuk backup	
SnapLock penggunaan	GB-Bulan	Jumlah kapasitas penyimpanan yang digunakan oleh SnapLock volume	
Baca permintaan ke penyimpanan kolam kapasitas standar ONTAP	Operasi	Jumlah permintaan baca yang dibuat untuk penyimpanan kolam kapasitas standar pada sistem file FSx untuk ONTAP	
Tulis permintaan ke penyimpanan kolam kapasitas standar ONTAP	Operasi	Jumlah permintaan tulis yang dibuat untuk penyimpanan kolam kapasitas standar pada sistem file FSx untuk ONTAP	

Lihat laporan AWS penggunaan FSx untuk ONTAP

AWS menyediakan laporan FSx penggunaan yang lebih rinci daripada laporan penagihan. Laporan penggunaan menyediakan data penggunaan agregat berdasarkan jam, hari, atau bulan, dan mencantumkan operasi berdasarkan wilayah dan jenis penggunaan.

Untuk melihat laporan AWS penggunaan

1. Masuk ke Konsol Manajemen AWS dan buka AWS Manajemen Penagihan dan Biaya konsol di <https://console.aws.amazon.com/costmanagement/>.
2. Di panel navigasi, pilih Cost Explorer.
3. Di bagian Parameter laporan, pilih Rentang tanggal dan perincian laporan Anda.
4. Biarkan Grup dengan > dimensi diatur ke Layanan.
5. Di bawah Filter > Layanan, pilih FSx
6. Pilih jenis Penggunaan. Lihat tabel mengikuti prosedur ini untuk daftar untuk jenis penggunaan ONTAP. FSx
7. Buat pilihan filter tambahan untuk laporan Anda.
8. Untuk mengunduh detail laporan ke file, pilih Unduh sebagai CSV.

Tabel berikut mencantumkan jenis penggunaan ONTAP yang dapat Anda gunakan untuk memfilter laporan guna melihat data penggunaan untuk sistem file ONTAP. FSx Untuk informasi selengkapnya tentang penggunaan Cost Explorer, lihat [Menganalisis biaya dan penggunaan Anda AWS Cost Explorer](#) di Panduan AWS Cost Management Pengguna.

First generation FSx for ONTAP file systems

Jenis Penggunaan	Unit	Deskripsi
<i>region</i> -PenyimpananSAZ_2N: SSD	GB-Bulan	Jumlah penyimpanan SSD yang disediakan pada single-AZ generasi pertama FSx untuk sistem file ONTAP.
<i>region</i> -Penyimpanan.MAZ: SSD	GB-Bulan	Jumlah penyimpanan SSD yang disediakan pada Multi-AZ generasi pertama FSx untuk sistem file ONTAP.
<i>region</i> - Throughput Capacity .SAZ_2N	MiBps-Mo	Jumlah kapasitas throughput yang disediakan pada single-AZ FSx generasi pertama untuk sistem file ONTAP.

Jenis Penggunaan	Unit	Deskripsi
<i>region</i> -ThroughputCapacity .MAZ	MiBps-Mo	Jumlah kapasitas throughput yang disediakan pada Multi-AZ FSx generasi pertama untuk sistem file ONTAP.
<i>region</i> -Provisionedssdiops.saz_2n	IOP-mo	Jumlah IOPS SSD yang disediakan di atas 3 IOPS per GiB penyimpanan SSD pada single-AZ generasi pertama FSx untuk sistem file ONTAP.
<i>region</i> -DiberikanSSdiops.maz	IOP-mo	Jumlah IOPS SSD yang disediakan di atas 3 IOPS per GiB penyimpanan SSD pada multi-AZ generasi pertama FSx untuk sistem file ONTAP.

Second generation FSx for ONTAP file systems

Jenis Penggunaan	Unit	Deskripsi
<i>region</i> -PenyimpananSAZ_2N2: SSD	GB-Bulan	Jumlah penyimpanan SSD yang disediakan pada single-AZ FSx generasi kedua untuk sistem file ONTAP.
<i>region</i> -Penyimpanan. MAZ2:SSD	GB-Bulan	Jumlah penyimpanan SSD yang disediakan pada Multi-AZ FSx generasi kedua untuk sistem file ONTAP.
<i>region</i> -ThroughputCapacity .SAZ_2N2	MiBps-Mo	Jumlah kapasitas throughput yang disediakan pada FSx single-AZ generasi kedua untuk sistem file ONTAP.

Jenis Penggunaan	Unit	Deskripsi
<i>region</i> -ThroughputCapacity.MAZ2	MiBps-Mo	Jumlah kapasitas throughput yang disediakan pada FSx Multi-AZ generasi kedua untuk sistem file ONTAP.
<i>region</i> -Provisionedssdiops.saz_2n2	IOP-mo	Jumlah IOPS SSD yang disediakan di atas 3 IOPS per GiB penyimpanan SSD pada single-AZ generasi kedua FSx untuk sistem file ONTAP.
<i>region</i> -ProvisionedssDiops. MAZ2	IOP-mo	Jumlah IOPS SSD yang disediakan di atas 3 IOPS per GiB penyimpanan SSD pada multi-AZ generasi kedua FSx untuk sistem file ONTAP.

All FSx for ONTAP file systems

Jenis Penggunaan	Unit	Deskripsi
<i>region</i> -penyimpanan.saz_2n: Std CPool	GB-Mo	Jumlah penyimpanan kolom kapasitas standar yang digunakan pada single-AZ generasi pertama atau kedua FSx untuk sistem file ONTAP.
<i>region</i> -Storage.maz: Std CPool	GB-Mo	Jumlah penyimpanan kolom kapasitas standar yang digunakan pada Multi-AZ generasi pertama atau kedua FSx untuk sistem file ONTAP.
<i>region</i> -BackupUsage	GB-Bulan	Jumlah kapasitas penyimpanan yang digunakan untuk backup.

Jenis Penggunaan	Unit	Deskripsi
<i>region</i> -SnaplockUsage	GB-Bulan	Jumlah kapasitas penyimpanan yang digunakan oleh SnapLock volume.
<i>region</i> -Permintaan.SAZ_2N: CPool StdRd	Operasi	Jumlah permintaan baca yang dibuat untuk penyimpanan kolom kapasitas standar pada sistem file AZ tunggal FSx untuk ONTAP.
<i>region</i> -Permintaan.SAZ_2N: CPool StdWr	Operasi	Jumlah permintaan tulis yang dibuat untuk penyimpanan kolom kapasitas standar pada sistem file AZ tunggal FSx untuk ONTAP.
<i>region</i> -Permintaan.maz: CPool StdRd	Operasi	Jumlah permintaan baca yang dibuat untuk penyimpanan kolom kapasitas standar pada Multi-AZ FSx untuk sistem file ONTAP.
<i>region</i> -Permintaan.maz: CPool StdWr	Operasi	Jumlah permintaan tulis yang dibuat untuk penyimpanan kolom kapasitas standar pada Multi-AZ FSx untuk sistem file ONTAP.

Memantau Amazon FSx untuk NetApp ONTAP

Anda dapat menggunakan layanan dan alat berikut untuk memantau Amazon FSx untuk penggunaan dan aktivitas NetApp ONTAP:

- **Amazon CloudWatch** — Anda dapat memantau sistem file menggunakan Amazon CloudWatch, yang secara otomatis mengumpulkan dan memproses data mentah dari ONTAP menjadi FSx metrik yang dapat dibaca. Statistik ini disimpan untuk jangka waktu 15 bulan sehingga Anda dapat mengakses informasi historis dan melihat kinerja sistem file Anda. Anda juga dapat menyetel alarm berdasarkan metrik selama periode waktu tertentu dan melakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas yang Anda tentukan.
- **Acara ONTAP EMS** - Anda dapat memantau sistem file ONTAP Anda FSx dengan menggunakan peristiwa yang dihasilkan oleh Sistem Manajemen Acara (EMS) ONTAP. Peristiwa EMS adalah pemberitahuan kejadian di sistem file Anda, seperti pembuatan iSCSI LUN atau ukuran volume otomatis.
- **NetApp Wawasan Infrastruktur Data** — Anda dapat memantau metrik konfigurasi, kapasitas, dan kinerja untuk sistem file ONTAP Anda FSx menggunakan layanan NetApp Data Infrastructure Insights. Anda juga dapat membuat peringatan berdasarkan kondisi metrik.
- **NetApp Harvest dan NetApp Grafana** — Anda dapat memantau sistem file ONTAP Anda FSx dengan menggunakan Harvest NetApp dan Grafana. NetApp Harvest memantau sistem file ONTAP dengan mengumpulkan metrik kinerja, kapasitas, dan perangkat keras dari FSx untuk sistem file ONTAP. Grafana menyediakan dasbor tempat metrik Harvest yang dikumpulkan dapat ditampilkan.
- **AWS CloudTrail**— Anda dapat menggunakan AWS CloudTrail untuk menangkap semua panggilan API untuk Amazon FSx sebagai acara. Peristiwa ini memberikan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon FSx.

Topik

- [Pemantauan CloudWatch dengan Amazon](#)
- [Pemantauan FSx untuk acara ONTAP EMS](#)
- [Pemantauan dengan Wawasan Infrastruktur Data](#)
- [Pemantauan FSx untuk sistem file ONTAP menggunakan Harvest dan Grafana](#)
- [Pemantauan FSx Panggilan API ONTAP dengan AWS CloudTrail](#)

Pemantauan CloudWatch dengan Amazon

Anda dapat memantau sistem file menggunakan Amazon CloudWatch, yang mengumpulkan dan memproses data mentah dari Amazon FSx untuk NetApp ONTAP menjadi metrik yang dapat dibaca, mendekati waktu nyata. Statistik ini disimpan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis untuk menentukan kinerja sistem file Anda. FSx untuk data metrik ONTAP secara otomatis dikirim ke CloudWatch periode 1 menit secara default. Untuk informasi selengkapnya CloudWatch, lihat [Apa itu Amazon CloudWatch?](#) di Panduan CloudWatch Pengguna Amazon.

Note

Secara default, FSx untuk ONTAP mengirimkan data CloudWatch metrik ke periode 1 menit kecuali untuk metrik berikut yang dikirim dalam interval 5 menit:

- FileServerDiskThroughputBalance
- FileServerDiskIopsBalance

CloudWatch metrik FSx untuk ONTAP disusun menjadi empat kategori, yang ditentukan oleh dimensi yang digunakan untuk menanyakan setiap metrik. Untuk informasi selengkapnya tentang dimensi, lihat [Dimensi](#) di Panduan CloudWatch Pengguna Amazon.

- Metrik sistem file: metrik File-system-level kinerja dan kapasitas penyimpanan.
- Metrik server file: File-server-level metrik.
- Metrik agregat sistem file terperinci: Metrik sistem file terperinci per agregat.
- Metrik sistem file terperinci: metrik File-system-level penyimpanan per tingkat penyimpanan (SSD dan kumpulan kapasitas).
- Metrik volume: Kinerja per volume dan metrik kapasitas penyimpanan.
- Metrik volume terperinci: Metrik kapasitas penyimpanan per volume berdasarkan tingkat penyimpanan atau menurut jenis data (pengguna, snapshot, atau lainnya).

Semua CloudWatch metrik FSx untuk ONTAP dipublikasikan ke AWS/FSx namespace di CloudWatch

Topik

- [Mengakses metrik CloudWatch](#)
- [Pemantauan di FSx konsol Amazon](#)
- [Metrik sistem file](#)
- [Metrik sistem file generasi kedua](#)
- [Metrik volume](#)

Mengakses metrik CloudWatch

Anda dapat melihat CloudWatch metrik Amazon untuk Amazon dengan FSx cara berikut:

- FSx Konsol Amazon
- CloudWatch Konsol Amazon
- AWS Command Line Interface (AWS CLI) untuk CloudWatch
- CloudWatch API

Prosedur berikut menjelaskan cara melihat CloudWatch metrik sistem file Anda dengan FSx konsol Amazon.

Untuk melihat CloudWatch metrik untuk sistem file Anda menggunakan konsol Amazon FSx

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file yang metriknya ingin Anda lihat.
3. Pada halaman Ringkasan, pilih Pemantauan & kinerja dari panel kedua untuk melihat grafik metrik sistem file Anda.

Ada empat tab pada panel Monitoring & Performance.

- Pilih Ringkasan (tab default) untuk menampilkan peringatan aktif, CloudWatch alarm, dan grafik untuk 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 Anda.

Prosedur berikut menjelaskan cara melihat CloudWatch metrik volume Anda dengan konsol Amazon FSx

Untuk melihat CloudWatch metrik volume Anda menggunakan konsol Amazon FSx

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Volume, lalu pilih volume yang metriknya ingin Anda lihat.
3. Pada halaman Ringkasan, pilih Monitoring (tab default) dari panel kedua untuk melihat grafik untuk metrik volume Anda.

Prosedur berikut menjelaskan cara melihat CloudWatch metrik sistem file Anda dengan CloudWatch konsol Amazon.

Untuk melihat metrik menggunakan konsol Amazon CloudWatch

1. Pada halaman Ringkasan sistem file Anda, pilih Pemantauan & kinerja dari panel kedua untuk melihat grafik untuk metrik sistem file Anda.
2. Pilih Lihat dalam metrik dari menu tindakan di kanan atas grafik yang ingin Anda lihat di CloudWatch konsol Amazon. Ini membuka halaman Metrik di CloudWatch konsol Amazon.

Prosedur berikut menjelaskan cara menambahkan FSx metrik sistem file ONTAP ke dasbor di konsol Amazon CloudWatch .

Untuk menambahkan metrik ke konsol Amazon CloudWatch

1. Pilih kumpulan metrik (Ringkasan, Penyimpanan, atau Kinerja) di panel Pemantauan & kinerja FSx konsol Amazon.
2. Pilih Tambahkan ke dasbor di kanan atas panel. Ini membuka CloudWatch konsol Amazon.
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.

Prosedur berikut menjelaskan cara mengakses metrik sistem file Anda dengan. AWS CLI

Untuk mengakses metrik dari AWS CLI

- Gunakan perintah CLI CloudWatch [daftar-metrik](#) dengan parameter. --namespace "AWS/FSx"
Untuk informasi selengkapnya, lihat [Referensi Perintah AWS CLI](#).

Prosedur berikut menjelaskan cara mengakses metrik sistem file Anda dengan CloudWatch API.

Untuk mengakses metrik dari API CloudWatch

- Panggil operasi [GetMetricStatistics](#) API. Untuk informasi selengkapnya, lihat [Referensi Amazon CloudWatch API](#).

Pemantauan di FSx konsol Amazon

CloudWatch Metrik yang dilaporkan oleh Amazon FSx memberikan informasi berharga tentang sistem dan FSx volume file ONTAP Anda.

Topik

- [Memantau metrik sistem file di konsol Amazon FSx](#)
- [Memantau metrik volume di konsol Amazon FSx](#)
- [Peringatan dan rekomendasi kinerja](#)
- [Membuat CloudWatch alarm Amazon untuk memantau Amazon FSx](#)

Memantau metrik sistem file di konsol Amazon FSx

Anda dapat menggunakan panel Pemantauan & kinerja di dasbor sistem file Anda di FSx konsol Amazon untuk melihat metrik yang dijelaskan dalam tabel berikut. Untuk informasi selengkapnya, lihat [Mengakses metrik CloudWatch](#).

Pemantauan & kinerja	Bagaimana saya...	Bagan	Metrik terkait
Ringkasan	... menentukan jumlah kapasitas penyimpanan yang tersedia pada sistem file saya?	Kapasitas penyimpanan primer	StorageCapacity {SSD} - StorageUsed {SSD}

Pemantauan & kinerja	Bagaimana saya...	Bagan	Metrik terkait
		yang tersedia (byte)	
	... menentukan total throughput klien sistem file saya?	Total throughput klien (byte/detik)	$\text{SUM (DataReadBytes + DataWriteBytes) / PERIODE (dalam detik)}$
	... menentukan IOPS klien total sistem file saya?	Total IOPS klien (operasi/detik)	$\text{SUM (DataReadOperations + DataWriteOperations + MetadataOperations) / PERIODE (dalam detik)}$
	... menentukan latensi rata-rata untuk operasi baca, tulis, dan metadata sistem file saya?	Latensi rata-rata (ms/operasi)	Latensi baca rata-rata: $\text{DataReadOperationTime} * 1000 / \text{DataReadOperations}$ Latensi tulis rata-rata: $\text{DataWriteOperationTime} * 1000 / \text{DataWriteOperations}$ Latensi metadata rata-rata: $* 1000 / \text{MetadataOperationTime}$ $\text{MetadataOperations}$

Pemantauan & kinerja	Bagaimana saya...	Bagan	Metrik terkait
	... menentukan distribusi kapasitas penyimpanan bekas dan gratis pada sistem file saya?	Distribusi penyimpanan	Tingkat utama tersedia: <code>StorageCapacity {SSD} - StorageUsed {SSD}</code> Tingkat primer yang digunakan: <code>StorageUsed {SSD}</code> Kolam kapasitas yang digunakan: <code>StorageUsed {StandardCapacityPool }</code>
	... menentukan penghematan dari efisiensi penyimpanan (kompresi, deduplikasi, dan pemadatan)?	Penghematan efisiensi penyimpanan	<code>StorageEfficiencySavings</code>
	... menentukan berapa banyak penyimpanan primer yang tersedia?	Kapasitas penyimpanan primer yang tersedia (byte)	<code>StorageCapacity {SSD} - StorageUsed {SSD}</code>
Penyimpanan	... menentukan persen penyimpanan primer yang digunakan untuk sistem file saya?	Pemanfaatan kapasitas penyimpanan primer (persen)	$\frac{\text{StorageUsed \{SSD\}}}{\text{StorageCapacity \{SSD\}}} * 100$

Pemantauan & kinerja	Bagaimana saya...	Bagan	Metrik terkait
	... menentukan apakah sistem file saya mendekati batas throughput jaringannya?	Throughput jaringan — pemanfaatan (persen)	NetworkThroughputUtilization
	... tentukan apakah sistem file saya mendekati batas throughput disknya?	Disk throughput — pemanfaatan (persen)	FileServerDiskThroughputUtilization
Kinerja server file	... tentukan apakah sistem file saya telah kehabisan kredit burst yang diizinkan untuk throughput disk?	Throughput disk — keseimbangan burst (persen)	FileServerDiskThroughputBalance
	... tentukan apakah sistem file saya mendekati batas IOPS SSD server file-nya?	Disk IOPS - pemanfaatan (persen)	FileServerDiskIopsUtilization
	... tentukan apakah sistem file saya telah kehabisan kredit burst yang diizinkan server file-nya untuk disk SSD IOPS?	Disk IOPS — keseimbangan burst (persen)	FileServerDiskIopsBalance

Pemantauan & kinerja	Bagaimana saya...	Bagan	Metrik terkait
	... menentukan rata-rata pemanfaatan CPU sistem file?	Pemanfaatan CPU (persen)	CPUUtilization
	... menentukan apakah beban kerja saya memanfaatkan RAM sistem file saya secara efisien dan NVMe membaca cache?	Rasio hit cache (persen)	FileServerCacheHitRatio
Performa disk	... tentukan apakah sistem file saya mendekati kapasitas IOPS SSD yang saat ini disediakan?	Disk IOPS - pemanfaatan (SSD) (persen)	DiskIopsUtilization

Note

Kami menyarankan Anda mempertahankan pemanfaatan kapasitas throughput rata-rata dari setiap dimensi terkait kinerja seperti pemanfaatan jaringan, pemanfaatan CPU, dan pemanfaatan SSD IOPS hingga di bawah 50%. Ini memastikan bahwa Anda memiliki kapasitas throughput cadangan yang cukup untuk lonjakan tak terduga dalam beban kerja Anda, serta untuk setiap operasi penyimpanan latar belakang (seperti sinkronisasi penyimpanan, tiering data, atau cadangan).

Memantau metrik volume di konsol Amazon FSx

Anda dapat melihat panel Monitoring di dasbor volume Anda di FSx konsol Amazon untuk melihat metrik kinerja tambahan. Untuk informasi selengkapnya, lihat [Mengakses metrik CloudWatch](#).

Memantau	Bagaimana saya...	Bagan	Metrik terkait
	... menentukan kapasitas penyimpanan volume saya yang tersedia?	Kapasitas penyimpanan	StorageCapacity

Memantau	Bagaimana saya...	Bagan	Metrik terkait
		an yang tersedia	
	... menentukan total throughput klien volume saya?	Total throughput klien (byte/detik)	$\text{SUM (DataReadBytes + DataWriteBytes) / PERIODE (dalam detik)}$
	... menentukan total IOPS klien volume saya?	Total IOPS klien (operasi/detik)	$\text{SUM (DataReadOperations + DataWriteOperations + MetadataOperations) / PERIODE (dalam detik)}$
	... menentukan berapa banyak operasi baca dan tulis yang berasal dari atau pergi ke tingkat kumpulan kapasitas?	Kapasitas Kolam IOPS (operasi/detik)	Baca operasi: CapacityPoolReadOperations Tulis operasi: CapacityPoolWriteOperations
	... menentukan latensi rata-rata untuk operasi baca, tulis, dan metadata volume saya?	Latensi rata-rata (ms/operasi)	Latensi baca rata-rata: $\text{DataReadOperationTime} * 1000 / \text{DataReadOperations}$ Latensi tulis rata-rata: $\text{DataWriteOperationTime} * 1000 / \text{DataWriteOperations}$ Latensi metadata rata-rata: $* 1000 / \text{MetadataOperationTime}$ $\text{MetadataOperations}$

Memantau	Bagaimana saya...	Bagan	Metrik terkait
	... menentukan jumlah file atau inode yang tersedia pada volume saya?	File yang tersedia (inode)	FilesCapacity - FilesUsed
	... menentukan distribusi kapasitas penyimpanan bekas dan gratis pada volume saya?	Distribusi penyimpanan	StorageCapacity - StorageUsed

Peringatan dan rekomendasi kinerja

FSx untuk ONTAP menampilkan peringatan untuk 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 tempat grafik metrik ditampilkan.

Anda dapat membuat CloudWatch alarm untuk salah satu FSx metrik Amazon. Untuk informasi selengkapnya, lihat [Membuat CloudWatch alarm Amazon untuk memantau Amazon FSx](#).

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.

Bagian dasbor	Jika ada peringatan untuk metrik ini	Lakukan hal berikut
Penyimpanan	Pemanfaatan kapasitas penyimpanan primer	Tingkatkan kapasitas penyimpanan utama sistem file Anda jika sistem file Anda belum mencapai kapasitas penyimpanan SSD maksimum. Untuk informasi selengkapnya, lihat Memperbarui kapasitas penyimpanan dan IOPS yang disediakan. Jika sistem file Anda memiliki beberapa pasangan HA dan pemanfaatan kapasitas penyimpanan utama Anda hanya lebih tinggi untuk subset agregat sistem file Anda (kumpulan penyimpanan yang membentuk tingkat penyimpanan utama Anda), maka Anda juga dapat menyeimbangkan kembali beban kerja Anda sehingga pemanfaatan kapasitas penyimpanan utama Anda lebih merata di seluruh sistem file Anda. Untuk informasi selengkapnya tentang menyeimbangkan kembali beban kerja Anda, lihat Menyeimbangkan beban kerja di seluruh pasangan HA. Jika saat ini Anda melakukan operasi penurunan SSD dan pemanfaatan melebihi 80% pada set disk baru, Anda dapat meningkatkan data ke kumpulan kapasitas, menghapus data dari volume yang telah dialihkan ke disk baru, atau mengajukan permintaan untuk meningkatkan kapasitas SSD selama operasi penurunan. Amazon FSx akan memprioritaskan permintaan kenaikan sebelum melanjutkan operasi penurunan. Untuk informasi selengkapnya, lihat Untuk mengurangi kapasitas penyimpanan SSD untuk sistem file (konsol).
	Throughput jaringan	Tingkatkan kapasitas throughput sistem file Anda jika sistem file Anda belum mencapai kapasitas throughput maksimum. Untuk informasi selengkapnya tentang
	Throughput disk	
Kinerja server file		

Bagian dasbor	Jika ada peringatan untuk metrik ini	Lakukan hal berikut
	IOPS Disk	memperbarui kapasitas throughput, lihat Memperbarui kapasitas throughput .
	Penggunaan CPU	Jika sistem file Anda memiliki beberapa pasangan HA dan pemanfaatannya tinggi hanya untuk sebagian dari server file, maka Anda juga dapat menyeimbangkan kembali beban kerja Anda sehingga beban kerja Anda lebih merata memanfaatkan kemampuan kinerja masing-masing pasangan HA sistem file Anda. Untuk informasi selengkapnya tentang menyeimbangkan kembali beban kerja Anda, lihat. Menyeimbangkan beban kerja di seluruh pasangan HA
Performa disk	IOPS Disk	Tingkatkan IOPS SSD jika sistem file Anda belum mencapai IOPS SSD maksimum untuk kapasitas throughput sistem file Anda saat ini. Untuk informasi selengkapnya tentang memperbarui IOPS yang disediakan sistem file Anda, lihat. Memperbarui kapasitas penyimpanan dan IOPS yang disediakan Jika sistem file Anda memiliki beberapa pasangan HA dan pemanfaatan IOPS disk Anda hanya lebih tinggi untuk subset agregat sistem file Anda (kumpulan penyimpanan yang membentuk tingkat penyimpanan utama Anda), maka Anda juga dapat menyeimbangkan kembali beban kerja Anda sehingga IOPS disk Anda digunakan lebih merata di seluruh sistem file Anda. Untuk informasi selengkapnya tentang menyeimbangkan kembali beban kerja Anda, lihat. Menyeimbangkan beban kerja di seluruh pasangan HA

Note

Selama operasi penurunan SSD, beban kerja berat tulis dapat mengalami penurunan kinerja sementara karena operasi mengkonsumsi disk dan sumber daya jaringan. Untuk meminimalkan dampak kinerja, pertahankan headroom yang memadai dengan memastikan beban kerja yang sedang berlangsung tidak secara konsisten mengkonsumsi lebih dari 50% CPU, 50% disk throughput, atau 50% SSD IOPS sebelum memulai operasi penurunan SSD. I/O Jeda singkat hingga 60 detik mungkin terjadi untuk setiap volume karena akses klien dialihkan ke set disk baru. Jeda ini diharapkan dan normal selama fase cutover operasi.

Untuk informasi selengkapnya tentang kinerja sistem file, lihat [Amazon FSx untuk kinerja NetApp ONTAP](#).

Membuat CloudWatch alarm Amazon untuk memantau Amazon FSx

Anda dapat membuat CloudWatch alarm yang mengirimkan pesan Amazon Simple Notification Service (Amazon SNS) saat alarm berubah status. Alarm mengawasi metrik tunggal selama periode waktu yang Anda tentukan. Jika diperlukan, alarm kemudian melakukan satu atau lebih tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama beberapa periode waktu. 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 Amazon.

Prosedur berikut menjelaskan cara membuat alarm menggunakan FSx konsol Amazon, AWS Command Line Interface (AWS CLI), dan API.

Untuk mengatur alarm menggunakan konsol Amazon FSx

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file yang ingin Anda buat alarm.
3. Pada halaman Ringkasan, pilih Pemantauan & kinerja dari panel kedua.
4. Pilih tab CloudWatch alarm.
5. Pilih Buat CloudWatch alarm. Anda dialihkan ke konsol CloudWatch.

6. Pilih Pilih Metrik.
7. Di bagian Metrik, pilih FSx.
8. Pilih kategori metrik:
 - Metrik Sistem File
 - Metrik Sistem File Terperinci
 - Metrik Volume
 - Metrik Volume Terperinci
9. Pilih metrik yang ingin Anda atur alarmnya, lalu pilih Pilih metrik.
10. Di bagian Kondisi, pilih kondisi yang Anda inginkan untuk alarm, lalu pilih Berikutnya.

 Note

Metrik mungkin tidak dipublikasikan selama pemeliharaan sistem file. 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 mengirim Anda email atau pemberitahuan Amazon SNS saat status alarm memulai tindakan, pilih status alarm untuk Pemicu status alarm.

Untuk Kirim pemberitahuan ke topik SNS berikut, pilih opsi. 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 dikirim saat alarm memasuki status alarm. Jika perubahan keadaan alarm ini terjadi sebelum alamat email diverifikasi, alamat tidak akan menerima pemberitahuan.

12. Isi kolom Nama alarm dan deskripsi Alarm, lalu pilih Berikutnya.
13. Pada halaman Pratinjau dan buat, tinjau alarm yang akan Anda buat, lalu pilih Buat alarm.

Untuk mengatur alarm menggunakan konsol CloudWatch

1. Buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih Buat Alarm Untuk memulai Wizard Buat Alarm.
3. Ikuti prosedur di Untuk mengatur alarm menggunakan FSx konsol Amazon, dimulai dengan langkah 6.

Untuk mengatur alarm menggunakan AWS CLI

- Panggil perintah [put-metric-alarm](#) CLI. Untuk informasi selengkapnya, lihat [Referensi Perintah AWS CLI](#).

Untuk menyetel alarm menggunakan CloudWatch API

- Panggil operasi [PutMetricAlarm](#) API. Untuk informasi selengkapnya, lihat [Referensi Amazon CloudWatch API](#).

Metrik sistem file

Metrik sistem file Amazon FSx untuk NetApp ONTAP Anda diklasifikasikan sebagai metrik sistem file atau metrik sistem file terperinci.

- Metrik sistem file adalah metrik kinerja dan penyimpanan agregat untuk satu sistem file yang mengambil satu dimensi. `FileSystemId` Metrik ini mengukur kinerja jaringan dan penggunaan kapasitas penyimpanan untuk sistem file Anda.
- Metrik sistem file terperinci mengukur kapasitas penyimpanan sistem file Anda dan penyimpanan yang digunakan di setiap tingkat penyimpanan (misalnya, penyimpanan SSD dan penyimpanan kolam kapasitas). Setiap metrik mencakup `FileSystemId`, `StorageTier`, dan `DataType` dimensi.

Perhatikan hal berikut tentang kapan Amazon FSx menerbitkan titik data untuk metrik ini ke: CloudWatch

- Untuk metrik pemanfaatan (metrik apa pun yang namanya diakhiri dengan Pemanfaatan, seperti `NetworkThroughputUtilization`), ada titik data yang dipancarkan setiap periode untuk setiap server file aktif atau agregat. Misalnya, Amazon FSx memancarkan satu metrik kecil per

server file aktif untuk `FileServerDiskIopsUtilization`, dan satu metrik kecil per agregat untuk `DiskIopsUtilization`

- Untuk semua metrik lainnya, ada satu titik data yang dipancarkan setiap periode, sesuai dengan nilai total metrik di semua server file aktif Anda (seperti `DataReadBytes` untuk metrik server file) atau semua agregat Anda (seperti `DiskReadBytes` untuk metrik penyimpanan).

Topik

- [I/O Metrik jaringan](#)
- [Metrik server file](#)
- [I/O Metrik disk](#)
- [Metrik kapasitas penyimpanan](#)
- [Metrik sistem file terperinci](#)

I/O Metrik jaringan

Semua metrik ini mengambil satu dimensi, `FileSystemId`.

Metrik	Deskripsi
<code>NetworkThroughputUtilization</code>	Persentase pemanfaatan throughput jaringan untuk sistem file. Perhatikan bahwa metrik ini mencerminkan arah - yaitu inbound atau outbound - yang memiliki arus lalu lintas yang lebih tinggi. Untuk melihat metrik individual untuk setiap arah, silakan lihat <code>NetworkReceivedBytes</code> dan <code>NetworkSentBytes</code> metrik. <code>AverageStatistik</code> adalah pemanfaatan throughput jaringan rata-rata dari sistem file selama periode tertentu. <code>MinimumStatistik</code> adalah pemanfaatan throughput jaringan terendah dari sistem file selama periode tertentu.

Metrik	Deskripsi
	MaximumStatistik adalah pemanfaatan throughput jaringan tertinggi dari sistem file selama periode tertentu. Unit: Persen Statistik yang valid: Average, Minimum, dan Maximum
NetworkSentBytes	Jumlah byte (jaringan I/O) yang dikirim oleh sistem file. SumStatistik adalah jumlah total byte yang dikirim oleh sistem file selama periode tertentu. Untuk menghitung throughput terkirim (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode yang ditentukan. Unit: Byte Statistik valid: Sum
NetworkReceivedBytes	Jumlah byte (jaringan I/O) yang diterima oleh sistem file. SumStatistik adalah jumlah total byte yang diterima oleh sistem file selama periode tertentu. Untuk menghitung throughput yang diterima (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode yang ditentukan. Unit: Byte Statistik valid: Sum

Metrik	Deskripsi
DataReadBytes	Jumlah byte (jaringan I/O) dari dibaca oleh klien ke sistem file. SumStatistik adalah jumlah total byte yang terkait dengan operasi baca selama periode yang ditentukan. Untuk menghitung throughput rata-rata (byte per detik) untuk suatu periode, bagilah Sum statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Byte Statistik valid: Sum
DataWriteBytes	Jumlah byte (jaringan I/O) dari penulisan oleh klien ke sistem file. SumStatistik adalah jumlah total byte yang terkait dengan operasi tulis selama periode yang ditentukan. Untuk menghitung throughput rata-rata (byte per detik) untuk suatu periode, bagilah Sum statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Byte Statistik valid: Sum

Metrik	Deskripsi
DataReadOperations	Hitungan operasi baca (jaringan I/O) dari pembacaan oleh klien ke sistem file. SumStatistik adalah jumlah total I/O operasi yang terjadi selama periode tertentu. Untuk menghitung operasi baca rata-rata per detik untuk suatu periode, bagilah Sum statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: Sum
DataWriteOperations	Hitungan operasi tulis (jaringan I/O) dari penulisan oleh klien ke sistem file. SumStatistik adalah jumlah total I/O operasi yang terjadi selama periode tertentu. Untuk menghitung operasi tulis rata-rata per detik untuk suatu periode, bagilah Sum statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: Sum

Metrik	Deskripsi
MetadataOperations	Hitungan operasi metadata (jaringan I/O) oleh klien ke sistem file. SumStatistik adalah jumlah total I/O operasi yang terjadi selama periode tertentu. Untuk menghitung rata-rata operasi metadata per detik untuk suatu periode, bagilah Sum statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: Sum
DataReadOperationTime	Jumlah total waktu yang dihabiskan dalam sistem file untuk operasi baca (jaringan I/O) dari klien yang mengakses data dalam sistem file. SumStatistik adalah jumlah detik yang dihabiskan oleh operasi baca selama periode yang ditentukan. Untuk menghitung latensi baca rata-rata untuk suatu periode, bagilah Sum statistik dengan DataReadOperations metrik selama periode yang sama. Sum Unit: detik Statistik valid: Sum

Metrik	Deskripsi
DataWriteOperationTime	Jumlah total waktu yang dihabiskan dalam sistem file untuk memenuhi operasi tulis (jaringan I/O) dari klien yang mengakses data dalam sistem file. SumStatistik adalah jumlah detik yang dihabiskan oleh operasi tulis selama periode yang ditentukan. Untuk menghitung latensi tulis rata-rata untuk suatu periode, bagilah Sum statistik dengan DataWriteOperations metrik selama periode yang sama. Sum Unit: detik Statistik valid: Sum
CapacityPoolReadBytes	Jumlah byte yang dibaca (jaringan I/O) dari tingkat kumpulan kapasitas sistem file. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. SumStatistik adalah jumlah total byte yang dibaca dari tingkat kumpulan kapasitas sistem file selama periode tertentu. Untuk menghitung byte kumpulan kapasitas per detik, bagi Sum statistik dengan detik dalam periode tertentu. Unit: Byte Statistik valid: Sum

Metrik	Deskripsi
CapacityPoolReadOperations	Jumlah operasi baca (jaringan I/O) dari tingkat kumpulan kapasitas sistem file. Ini berarti permintaan baca kumpulan kapasitas. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. SumStatistik adalah jumlah total operasi baca dari tingkat kumpulan kapasitas sistem file selama periode tertentu. Untuk menghitung permintaan kumpulan kapasitas per detik, bagi Sum statistik dengan detik dalam periode tertentu. Unit: Hitungan Statistik valid: Sum
CapacityPoolWriteBytes	Jumlah byte yang ditulis (jaringan I/O) ke tingkat kumpulan kapasitas sistem file. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. SumStatistik adalah jumlah total byte yang ditulis ke tingkat kumpulan kapasitas sistem file selama periode tertentu. Untuk menghitung byte kumpulan kapasitas per detik, bagi Sum statistik dengan detik dalam periode tertentu. Unit: Byte Statistik valid: Sum

Metrik	Deskripsi
CapacityPoolWriteOperations	Jumlah operasi tulis (jaringan I/O) ke sistem file dari tier pool kapasitas. Ini diterjemahkan menjadi permintaan tulis. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. SumStatistik adalah jumlah total operasi penulisan ke tingkat kumpulan kapasitas sistem file selama periode tertentu. Untuk menghitung permintaan kumpulan kapasitas per detik, bagi Sum statistik dengan detik dalam periode tertentu. Unit: Hitungan Statistik valid: Sum

Metrik server file

Semua metrik ini mengambil satu dimensi, `FileSystemId`.

Metrik	Deskripsi
CPUUtilization	Persentase pemanfaatan sumber daya CPU sistem file. AverageStatistik adalah pemanfaatan CPU rata-rata dari sistem file selama periode tertentu. MinimumStatistik adalah pemanfaatan CPU terendah dari sistem file selama periode tertentu.

Metrik	Deskripsi
	MaximumStatistik adalah pemanfaatan CPU tertinggi dari sistem file selama periode tertentu. Unit: Persen Statistik yang valid:Average,Minimum, dan Maximum
FileServerDiskThroughputUtilization	Throughput disk antara server file Anda dan tingkat utama, sebagai persentase dari batas yang disediakan ditentukan oleh kapasitas throughput. AverageStatistik adalah persentase rata-rata pemanfaatan throughput disk server file selama periode tertentu. MinimumStatistik adalah persentase pemanfaatan terendah dari throughput disk server file selama periode tertentu. MaximumStatistik adalah pemanfaatan tertinggi dari throughput disk server file selama periode tertentu. Unit: Persen Statistik yang valid:Average,Minimum, dan Maximum

Metrik	Deskripsi
FileServerDiskThroughputBalance	Persentase kredit burst yang tersedia untuk throughput disk antara server file Anda dan tingkat utama. Ini berlaku untuk sistem file yang disediakan dengan kapasitas throughput kurang dari 512. MBps AverageStatistik adalah saldo burst rata-rata yang tersedia selama periode tertentu. MinimumStatistik adalah saldo burst minimum yang tersedia selama periode tertentu. MaximumStatistik adalah saldo burst maksimum yang tersedia selama periode tertentu. Unit: Persen Statistik yang valid: Average, Minimum, dan Maximum

Metrik	Deskripsi
FileServerDiskIopsBalance	Persentase kredit burst yang tersedia untuk IOPS disk antara server file Anda dan tingkat utama. Ini berlaku untuk sistem file yang disediakan dengan kapasitas throughput kurang dari 512. MBps AverageStatistik adalah saldo burst rata-rata yang tersedia selama periode tertentu. MinimumStatistik adalah saldo burst minimum yang tersedia selama periode tertentu. MaximumStatistik adalah saldo burst maksimum yang tersedia selama periode tertentu. Unit: Persen Statistik yang valid: Average, Minimum, dan Maximum

Metrik	Deskripsi
FileServerDiskIopsUtilization	Persentase pemanfaatan IOPS kapasitas IOPS disk yang tersedia untuk server file Anda. AverageStatistik adalah pemanfaatan IOPS disk rata-rata dari sistem file selama periode tertentu. MinimumStatistik adalah pemanfaatan IOPS disk minimum dari sistem file selama periode tertentu. MaximumStatistik adalah pemanfaatan IOPS disk maksimum dari sistem file selama periode tertentu. Unit: Persen Statistik yang valid:Average,Minimum, dan Maximum

Metrik	Deskripsi
<code>FileServerCacheHitRatio</code>	Persentase semua permintaan baca yang dilayani oleh data dalam RAM dan NVMe cache sistem file. Persentase yang lebih tinggi berarti bahwa lebih banyak pembacaan disajikan oleh cache baca sistem file. Unit: Persen <code>AverageStatistik</code> adalah persentase hit cache rata-rata untuk sistem file selama periode tertentu. <code>MinimumStatistik</code> adalah persentase hit cache terendah untuk sistem file selama periode tertentu. <code>MaximumStatistik</code> adalah persentase hit cache tertinggi untuk sistem file selama periode tertentu. Statistik yang valid: <code>Average</code>, <code>Minimum</code>, dan <code>Maximum</code>

I/O Metrik disk

Semua metrik ini mengambil satu dimensi, `FileSystemId`.

Metrik	Deskripsi
<code>DiskReadBytes</code>	Jumlah byte (disk I/O) dari disk apa pun dibaca ke tingkat utama sistem file. <code>SumStatistik</code> adalah jumlah total byte yang dibaca dari sistem file selama periode tertentu.

Metrik	Deskripsi
	Untuk menghitung throughput disk baca (byte per detik) untuk statistik apa pun, bagilah Sum statistik dengan detik dalam periode yang ditentukan. Unit: Byte Statistik valid: Sum
DiskWriteBytes	Jumlah byte (disk I/O) dari disk apa pun menulis ke tingkat utama sistem file. SumStatistik adalah jumlah total byte yang ditulis dari sistem file selama periode tertentu. Untuk menghitung throughput disk tulis (byte per detik) untuk statistik apa pun, bagilah Sum statistik dengan detik dalam periode yang ditentukan. Unit: Byte Statistik valid: Sum

Metrik	Deskripsi
DiskIopsUtilization	Disk IOPS antara server file Anda dan volume penyimpanan, sebagai persentase dari batas IOPS disk yang disediakan tingkat primer. AverageStatistik adalah pemanfaatan IOPS disk rata-rata dari sistem file selama periode tertentu. MinimumStatistik adalah pemanfaatan IOPS disk minimum dari sistem file selama periode tertentu. MaximumStatistik adalah pemanfaatan IOPS disk maksimum dari sistem file selama periode tertentu. Unit: Persen Statistik yang valid: Average, Minimum, dan Maximum
DiskReadOperations	Jumlah operasi baca (disk I/O) dari tingkat utama sistem file. SumStatistik adalah jumlah total operasi baca dari tingkat primer selama periode tertentu. Unit: Hitungan Statistik valid: Sum

Metrik	Deskripsi
DiskWriteOperations	Jumlah operasi tulis (disk I/O) ke tingkat utama sistem file. SumStatistik adalah jumlah total operasi penulisan ke tingkat primer selama periode tertentu. Unit: Hitungan Statistik valid: Sum

Metrik kapasitas penyimpanan

Semua metrik ini mengambil satu dimensi, `FileSystemId`.

Metrik	Deskripsi
StorageEfficiencySavings	Byte disimpan dari fitur efisiensi penyimpanan (kompresi, deduplikasi, dan pemadatan). AverageStatistik adalah penghematan efisiensi penyimpanan rata-rata selama periode tertentu. Untuk menghitung penghematan efisiensi penyimpanan sebagai persentase dari semua data yang disimpan, selama periode satu menit, bagi <code>StorageEfficiencySavings</code> dengan jumlah <code>StorageEfficiencySavings</code> dan metrik sistem <code>StorageUsed</code> file, menggunakan Sum statistik untuk <code>StorageUsed</code>. MinimumStatistik adalah penghematan efisiensi penyimpanan minimum selama periode tertentu.

Metrik	Deskripsi
	MaximumStatistik adalah penghematan efisiensi penyimpanan maksimum selama periode tertentu. Unit: Byte Statistik yang valid:Average,Minimum, dan Maximum
StorageUsed	Jumlah total data fisik yang tersimpan pada sistem file, pada tingkat primer (SSD) dan tingkat kolam kapasitas. Metrik ini mencakup penghematan dari fitur efisiensi penyimpanan, seperti kompresi data dan deduplikasi. Unit: Byte Statistik yang valid:Average,Minimum, dan Maximum

Metrik	Deskripsi
LogicalDataStored	Jumlah total data logis yang disimpan pada sistem file, mengingat tingkat SSD dan tingkat kolam kapasitas. Metrik ini mencakup ukuran logis total snapshot dan FlexClones, tetapi tidak termasuk penghematan efisiensi penyimpanan yang dicapai melalui kompresi, pemadatan, dan deduplikasi. Untuk menghitung penghematan efisiensi penyimpanan dalam byte, ambil Average dari StorageUsed selama periode tertentu dan kurangi dari periode yang samaAverage. LogicalDataStored Untuk menghitung penghematan efisiensi penyimpanan sebagai persentase dari total ukuran data logis, ambil Average dari StorageUsed selama periode tertentu dan kurangi dari LogicalDataStored periode yang samaAverage. Kemudian bagi perbedaannya Average dengan LogicalDataStored periode yang sama. Unit: Byte Statistik yang valid:Average,Minimum, dan Maximum

Metrik sistem file terperinci

Metrik sistem file terperinci adalah metrik pemanfaatan penyimpanan terperinci untuk setiap tingkatan penyimpanan Anda. Metrik sistem file terperinci semuanya memiliki dimensiFileSystemId,StorageTier, danDataType.

- StorageTierDimensi menunjukkan tingkat penyimpanan yang diukur metrik, dengan kemungkinan nilai SSD danStandardCapacityPool.

- `DataTypeDimensi` menunjukkan jenis data yang diukur metrik, dengan nilai yang mungkin `All`.

Ada baris untuk setiap kombinasi unik dari pasangan nilai kunci metrik dan dimensi tertentu, dengan deskripsi tentang apa yang diukur kombinasi itu.

Metrik	Deskripsi
<code>StorageCapacityUtilization</code>	Pemanfaatan kapasitas penyimpanan untuk setiap agregat sistem file Anda. Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. <code>AverageStatistik</code> adalah jumlah rata-rata pemanfaatan kapasitas penyimpanan untuk tingkat kinerja sistem file Anda selama periode yang ditentukan. <code>MinimumStatistik</code> adalah jumlah pemanfaatan kapasitas penyimpanan terendah untuk tingkat kinerja sistem file Anda selama periode yang ditentukan. <code>MaximumStatistik</code> adalah jumlah pemanfaatan kapasitas penyimpanan tertinggi untuk tingkat kinerja sistem file Anda selama periode yang ditentukan. Unit: Persen Statistik yang valid: <code>Average</code>, <code>Minimum</code>, dan <code>Maximum</code>
<code>StorageCapacity</code>	Total kapasitas penyimpanan tingkat primer (SSD). Unit: Byte Statistik valid: <code>Maximum</code>

Metrik	Deskripsi
StorageUsed	Kapasitas penyimpanan fisik yang digunakan dalam byte, khusus untuk tingkat penyimpanan. Nilai ini mencakup penghematan dari fitur efisiensi penyimpanan, seperti kompresi data dan deduplikasi. Nilai dimensi yang valid untuk <code>StorageTier</code> are <code>SSD</code> dan <code>StandardCapacityPool</code>, sesuai dengan tingkat penyimpanan yang diukur metrik ini. Metrik ini juga membutuhkan <code>DataType</code> dimensi dengan nilai <code>All</code>. The <code>Average</code>, <code>Minimum</code>, dan <code>Maximum</code> statistik adalah konsumsi penyimpanan per tingkat dalam byte untuk periode tertentu. Untuk menghitung pemanfaatan kapasitas penyimpanan tingkat penyimpanan utama (SSD) Anda, bagilah salah satu statistik ini dengan <code>Maximum StorageCapacity</code> periode yang sama, dengan <code>StorageTier</code> dimensi yang sama dengan. <code>SSD</code> Untuk menghitung kapasitas penyimpanan gratis tingkat penyimpanan utama (SSD) Anda dalam byte, kurangi salah satu statistik ini dari periode yang sama, dengan dimensi yang <code>StorageTier</code> sama dengan. <code>Maximum StorageCapacity SSD</code> Unit: Byte Statistik yang valid: <code>Average</code>, <code>Minimum</code>, dan <code>Maximum</code>

Metrik sistem file generasi kedua

Metrik berikut disediakan FSx untuk sistem file generasi kedua ONTAP. Untuk metrik, titik data dipancarkan untuk setiap pasangan HA dan untuk setiap agregat (untuk metrik pemanfaatan penyimpanan).

Note

Jika Anda memiliki sistem file dengan beberapa pasangan HA, Anda juga dapat menggunakan metrik [sistem file pasangan HA tunggal dan metrik volume](#).

Topik

- [I/O Metrik jaringan](#)
- [Metrik server file](#)
- [I/O Metrik disk](#)
- [Metrik sistem file terperinci](#)

I/O Metrik jaringan

Semua metrik ini mengambil dua dimensi, `FileSystemId` dan `FileServer`.

- `FileSystemId`— ID AWS sumber daya sistem file Anda.
- `FileServer`— Nama server file (atau node) di ONTAP (misalnya, `FsId01234567890abcdef-01`). Server file bernomor ganjil adalah server file yang disukai (yaitu, mereka melayani lalu lintas kecuali sistem file gagal ke server file sekunder), sedangkan server file bernomor genap adalah server file sekunder (yaitu, mereka melayani lalu lintas hanya ketika mitra mereka tidak tersedia). Karena itu, server file sekunder biasanya menunjukkan pemanfaatan yang lebih sedikit daripada server file pilihan.

Metrik	Deskripsi
<code>NetworkThroughputUtilization</code>	Pemanfaatan throughput jaringan sebagai persentase dari throughput jaringan yang tersedia untuk sistem file Anda. Metrik ini setara dengan maksimum <code>NetworkSe</code>

Metrik	Deskripsi
	<code>ntBytes</code> dan <code>NetworkReceivedBytes</code> sebagai persentase kapasitas throughput jaringan dari satu pasangan HA untuk sistem file Anda. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti <code>SnapMirror</code>, <code>tiering</code>, dan <code>backup</code>). Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. <code>AverageStatistik</code> adalah pemanfaatan throughput jaringan rata-rata untuk server file yang diberikan selama periode yang ditentukan. <code>MinimumStatistik</code> adalah pemanfaatan throughput jaringan terendah untuk server file yang diberikan selama satu menit, untuk periode yang ditentukan. <code>MaximumStatistik</code> adalah pemanfaatan throughput jaringan tertinggi untuk server file yang diberikan selama satu menit, untuk periode yang ditentukan. Unit: Persen Statistik yang valid: <code>Average</code>, <code>Minimum</code>, dan <code>Maximum</code>

Metrik	Deskripsi
NetworkSentBytes	Jumlah byte (jaringan IO) yang dikirim oleh sistem file Anda. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. SumStatistik adalah jumlah total byte yang dikirim melalui jaringan oleh server file yang diberikan selama periode yang ditentukan. AverageStatistik adalah jumlah rata-rata byte yang dikirim melalui jaringan oleh server file yang diberikan selama periode yang ditentukan. MinimumStatistik adalah jumlah byte terendah yang dikirim melalui jaringan oleh server file yang diberikan selama periode yang ditentukan. MaximumStatistik adalah jumlah byte tertinggi yang dikirim melalui jaringan oleh server file yang diberikan selama periode yang ditentukan. Untuk menghitung throughput terkirim (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode yang ditentukan. Unit: Byte Statistik yang valid: Sum, Average, Minimum, dan Maximum

Metrik	Deskripsi
NetworkReceivedBytes	Jumlah byte (jaringan IO) yang diterima oleh sistem file Anda. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. SumStatistik adalah jumlah total byte yang diterima melalui jaringan oleh server file yang diberikan selama periode yang ditentukan. AverageStatistik adalah jumlah rata-rata byte yang diterima melalui jaringan oleh server file yang diberikan setiap menit selama periode yang ditentukan. MinimumStatistik adalah jumlah byte terendah yang diterima melalui jaringan oleh server file yang diberikan setiap menit selama periode yang ditentukan. MaximumStatistik adalah jumlah byte tertinggi yang diterima melalui jaringan oleh server file yang diberikan setiap menit selama periode yang ditentukan. Untuk menghitung throughput yang diterima (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode tersebut. Unit: Byte Statistik yang valid: Sum, Average, Minimum, dan Maximum

Metrik server file

Semua metrik ini mengambil dua dimensi, `FileSystemId` dan `FileServer`.

Metrik	Deskripsi
<code>CPUUtilization</code>	Persentase pemanfaatan sumber daya CPU sistem file. Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. <code>AverageStatistik</code> adalah pemanfaatan CPU rata-rata dari sistem file selama periode tertentu. <code>MinimumStatistik</code> adalah pemanfaatan CPU terendah untuk server file yang diberikan selama periode yang ditentukan. <code>MaximumStatistik</code> adalah pemanfaatan CPU tertinggi untuk server file yang diberikan selama periode yang ditentukan. Unit: Persen Statistik yang valid: <code>Average</code>, <code>Minimum</code>, dan <code>Maximum</code>
<code>FileServerDiskThroughputUtilization</code>	Throughput disk antara server file Anda dan agregat, sebagai persentase dari batas yang disediakan ditentukan oleh kapasitas throughput. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti <code>SnapMirror</code>, <code>tiering</code>, dan <code>backup</code>). Metrik ini setara dengan jumlah <code>DiskReadBytes</code> dan <code>DiskWriteBytes</code> sebagai persentase kapasitas throughput disk server file dari satu pasangan HA untuk sistem file Anda. Ada satu

Metrik	Deskripsi
	metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. AverageStatistik adalah rata-rata pemanfaatan throughput disk server file untuk server file yang diberikan selama periode yang ditentukan. MinimumStatistik adalah pemanfaatan throughput disk server file terendah untuk server file yang diberikan selama periode yang ditentukan. MaximumStatistik adalah pemanfaatan throughput disk server file tertinggi untuk server file yang diberikan selama periode yang ditentukan. Unit: Persen Statistik yang valid: Average, Minimum, dan Maximum

Metrik	Deskripsi
FileServerDiskIopsUtilization	Penggunaan IOPS kapasitas IOPS disk yang tersedia untuk server file Anda, sebagai persentase dari batas IOPS disk. Ini berbeda dari DiskIopsUtilization penggunaan IOPS disk dari maksimum yang dapat ditangani oleh server file Anda, dibandingkan dengan IOPS disk yang disediakan. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. AverageStatistik adalah pemanfaatan IOPS disk rata-rata untuk server file yang diberikan selama periode yang ditentukan. MinimumStatistik adalah pemanfaatan IOPS disk terendah untuk server file yang diberikan selama periode yang ditentukan. MaximumStatistik adalah pemanfaatan IOPS disk tertinggi untuk server file yang diberikan selama periode yang ditentukan. Unit: Persen Statistik yang valid: Average, Minimum, dan Maximum

Metrik	Deskripsi
<code>FileServerCacheHitRatio</code>	Persentase semua permintaan baca yang disajikan oleh data yang berada di RAM atau NVMe cache sistem file Anda untuk setiap pasangan HA Anda (misalnya, server file aktif dalam pasangan HA). Persentase yang lebih tinggi menunjukkan rasio pembacaan cache yang lebih tinggi terhadap total pembacaan. Semua I/O dipertimbangkan, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap server file sistem file Anda. Unit: Persen <code>AverageStatistik</code> adalah rasio hit cache rata-rata untuk salah satu pasangan HA sistem file Anda selama periode yang ditentukan. <code>MinimumStatistik</code> adalah rasio hit cache terendah untuk salah satu pasangan HA sistem file Anda selama periode yang ditentukan. <code>MaximumStatistik</code> adalah rasio hit cache tertinggi untuk salah satu pasangan HA sistem file Anda selama periode yang ditentukan. Statistik yang valid: <code>Average</code>, <code>Minimum</code>, dan <code>Maximum</code>

I/O Metrik disk

Semua metrik ini mengambil dua dimensi, `FileSystemId` dan `Aggregate`.

- `FileSystemId`— ID AWS sumber daya sistem file Anda.

- **Aggregate**— Tingkat kinerja sistem file Anda terdiri dari beberapa kumpulan penyimpanan yang disebut agregat. Ada satu agregat untuk setiap pasangan HA. Misalnya, agregat `aggr1` peta ke server file `FsxD01234567890abcdef-01` (server file aktif) dan server file `FsxD01234567890abcdef-02` (server file sekunder) dalam pasangan HA.

Metrik	Deskripsi
DiskReadBytes	Jumlah byte (disk IO) dari disk ay dibaca dari agregat ini. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. Selama operasi penurunan kapasitas SSD, metrik ini dilaporkan untuk agregat asli (<code>aggr1_old</code>) dan agregat baru yang lebih kecil (<code>aggr1</code>). SumStatistik adalah jumlah total byte yang dibaca setiap menit dari agregat yang diberikan selama periode yang ditentukan. AverageStatistik adalah jumlah rata-rata byte yang dibaca setiap menit dari agregat yang diberikan selama periode yang ditentukan. MinimumStatistik adalah jumlah byte terendah yang dibaca setiap menit dari agregat yang diberikan selama periode yang ditentukan. MaximumStatistik adalah jumlah byte tertinggi yang dibaca setiap menit dari agregat yang diberikan selama periode yang ditentukan. Untuk menghitung throughput disk baca (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode tersebut.

Metrik	Deskripsi
	Unit: Byte
	Statistik yang valid:Sum,Average,Minimum, dan Maximum

Metrik	Deskripsi
DiskWriteBytes	Jumlah byte (disk IO) dari disk apa pun menulis ke agregat ini. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. Selama operasi penurunan kapasitas SSD, metrik ini dilaporkan untuk agregat asli (aggr1_old) dan agregat baru yang lebih kecil (aggr1). SumStatistik adalah jumlah total byte yang ditulis ke agregat yang diberikan selama periode yang ditentukan. AverageStatistik adalah jumlah rata-rata byte yang ditulis ke agregat yang diberikan setiap menit selama periode yang ditentukan. MinimumStatistik adalah jumlah byte terendah yang ditulis ke agregat yang diberikan setiap menit selama periode yang ditentukan. MaximumStatistik adalah jumlah byte tertinggi yang ditulis ke agregat yang diberikan setiap menit selama periode yang ditentukan. Untuk menghitung throughput disk tulis (byte per detik) untuk statistik apa pun, bagilah statistik dengan detik dalam periode yang ditentukan. Unit: Byte

Metrik	Deskripsi
	Statistik yang valid: Sum, Average, Minimum, dan Maximum

Metrik	Deskripsi
DiskIopsUtilization	Pemanfaatan IOPS disk dari satu agregat, sebagai persentase dari batas IOPS disk agregat (yaitu, total IOPS sistem file dibagi dengan jumlah pasangan HA untuk sistem file Anda). Ini berbeda dari FileServerDiskIopsUtilization itu adalah pemanfaatan IOPS disk yang disediakan terhadap batas IOPS yang Anda berikan, sebagai lawan dari IOPS disk maksimum yang didukung oleh server file (yaitu, ditentukan oleh kapasitas throughput Anda yang dikonfigurasi per pasangan HA). Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. Selama operasi penurunan kapasitas SSD, metrik ini dilaporkan untuk agregat asli (aggr1_old) dan agregat baru yang lebih kecil (aggr1). AverageStatistik adalah pemanfaatan IOPS disk rata-rata untuk agregat yang diberikan selama periode yang ditentukan. MinimumStatistik adalah pemanfaatan IOPS disk terendah untuk agregat yang diberikan selama periode yang ditentukan. MaximumStatistik ii pemanfaatan IOPS disk tertinggi untuk agregat yang diberikan selama periode yang ditentukan. Unit: Persen

Metrik	Deskripsi
	Statistik yang valid: Average, Minimum, dan Maximum

Metrik	Deskripsi
DiskReadOperations	Jumlah operasi baca (disk IO) ke agregat ini. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. Selama operasi penurunan kapasitas SSD, metrik ini dilaporkan untuk agregat asli (aggr1_old) dan agregat baru yang lebih kecil (aggr1). SumStatistik adalah jumlah total operasi baca yang dilakukan oleh agregat yang diberikan selama periode yang ditentukan. AverageStatistik adalah jumlah rata-rata operasi baca yang dilakukan setiap menit oleh agregat yang diberikan selama periode yang ditentukan. MinimumStatistik adalah jumlah operasi baca terendah yang dilakukan setiap menit oleh agregat yang diberikan selama periode yang ditentukan. MaximumStatistik adalah jumlah operasi baca tertinggi yang dilakukan setiap menit oleh agregat yang diberikan selama periode yang ditentukan. Untuk menghitung IOPS disk rata-rata selama periode tersebut, gunakan Average statistik dan bagi hasilnya dengan 60 (detik). Unit: Hitungan

Metrik	Deskripsi
	Statistik yang valid: Sum, Average, Minimum, dan Maximum
DiskWriteOperations	Jumlah operasi tulis (disk IO) ke agregat ini. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang (seperti SnapMirror, tiering, dan backup). Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. Selama operasi penurunan kapasitas SSD, metrik ini dilaporkan untuk agregat asli (aggr1_old) dan agregat baru yang lebih kecil (aggr1). SumStatistik adalah jumlah total operasi penulisan yang dilakukan oleh agregat yang diberikan selama periode yang ditentukan. AverageStatistik adalah jumlah rata-rata operasi tulis yang dilakukan setiap menit oleh agregat yang diberikan selama periode yang ditentukan. Untuk menghitung IOPS disk rata-rata selama periode tersebut, gunakan Average statistik dan bagi hasilnya dengan 60 (detik). Unit: Hitungan Statistik yang valid: Sum dan Average

Metrik sistem file terperinci

Metrik sistem file terperinci adalah metrik pemanfaatan penyimpanan terperinci untuk setiap tingkatan penyimpanan Anda. Metrik sistem file terperinci memiliki `FileSystemId`, `StorageTier`, dan `DataType` dimensi, atau, `FileSystemId`, `StorageTierDataType`, dan `Aggregate` dimensi.

- Ketika Aggregate dimensi tidak disediakan, metrik adalah untuk seluruh sistem file Anda. `StorageCapacityMetric` `StorageUsed` dan memiliki titik data tunggal setiap menit yang sesuai dengan total penyimpanan yang dikonsumsi sistem file (per tingkat penyimpanan) dan kapasitas penyimpanan total (untuk tingkat SSD). Sementara itu, `StorageCapacityUtilization` metrik memancarkan satu metrik setiap menit untuk setiap agregat.
- Ketika Aggregate dimensi disediakan, metrik untuk setiap agregat.

Arti dimensi adalah sebagai berikut:

- `FileSystemId`— ID AWS sumber daya sistem file Anda.
- `Aggregate`— Tingkat kinerja sistem file Anda terdiri dari beberapa kumpulan penyimpanan yang disebut agregat. Ada satu agregat untuk setiap pasangan HA. Misalnya, agregat `aggr1` peta ke server file `FsxD01234567890abcdef-01` (server file aktif) dan server file `FsxD01234567890abcdef-02` (server file sekunder) dalam pasangan HA.
- `StorageTier`— Menunjukkan tingkat penyimpanan yang diukur metrik, dengan kemungkinan nilai `SSD` dan `StandardCapacityPool`.
- `DataType`— Menunjukkan jenis data yang diukur metrik, dengan nilai yang mungkin `All`.

Ada baris untuk setiap kombinasi unik dari pasangan nilai kunci metrik dan dimensi tertentu, dengan deskripsi tentang apa yang diukur kombinasi itu.

Metrik	Deskripsi
<code>StorageCapacityUtilization</code>	Pemanfaatan kapasitas penyimpanan untuk agregat sistem file tertentu. Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. <code>AverageStatistic</code> adalah jumlah rata-rata pemanfaatan kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentukan. <code>MinimumStatistic</code> adalah jumlah minimum pemanfaatan kapasitas penyimpanan untuk

Metrik	Deskripsi
	agregat tertentu selama periode yang ditentukan. MaximumStatistik adalah jumlah maksimum pemanfaatan kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentukan. Selama operasi penurunan kapasitas SSD, metrik ini dilaporkan untuk agregat asli (aggr1_old) dan agregat baru yang lebih kecil (aggr1). Unit: Persen Statistik yang valid: Average, Minimum, dan Maximum

Metrik	Deskripsi
StorageCapacity	Kapasitas penyimpanan untuk agregat sistem file tertentu. Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. AverageStatistik adalah jumlah rata-rata kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentukan. MinimumStatistik adalah jumlah minimum kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentukan. MaximumStatistik adalah jumlah maksimum kapasitas penyimpanan untuk agregat tertentu selama periode yang ditentukan. Selama operasi penurunan kapasitas SSD, metrik ini dilaporkan untuk agregat asli (aggr1_old) dan agregat baru yang lebih kecil (aggr1). Unit: Byte Statistik yang valid: Average, Minimum, dan Maximum

Metrik	Deskripsi
StorageUsed	Kapasitas penyimpanan fisik yang digunakan dalam byte, khusus untuk tingkat penyimpanan. Nilai ini mencakup penghematan dari fitur efisiensi penyimpanan, seperti kompresi data dan deduplikasi. Nilai dimensi yang valid untuk <code>StorageTier</code> are <code>SSD</code> dan <code>StandardCapacityPool</code>, sesuai dengan tingkat penyimpanan yang diukur metrik ini. Ada satu metrik yang dipancarkan setiap menit untuk setiap agregat sistem file Anda. <code>AverageStatistic</code> adalah jumlah rata-rata kapasitas penyimpanan fisik yang dikonsumsi pada tingkat penyimpanan yang diberikan oleh agregat yang diberikan selama periode yang ditentukan. <code>MinimumStatistic</code> adalah jumlah minimum kapasitas penyimpanan fisik yang dikonsumsi pada tingkat penyimpanan yang diberikan oleh agregat yang diberikan selama periode yang ditentukan. <code>MaximumStatistic</code> adalah jumlah maksimum kapasitas penyimpanan fisik yang dikonsumsi pada tingkat penyimpanan yang diberikan oleh agregat yang diberikan selama periode yang ditentukan. Selama operasi penurunan kapasitas SSD, metrik ini dilaporkan untuk agregat asli (<code>aggr1_old</code>) dan agregat baru yang lebih kecil (<code>aggr1</code>). Unit: Byte

Metrik	Deskripsi
	Statistik yang valid: Average, Minimum, dan Maximum

Metrik volume

Sistem file Amazon FSx untuk NetApp ONTAP Anda dapat memiliki satu atau lebih volume yang menyimpan data Anda. Masing-masing volume ini memiliki satu set CloudWatch metrik, diklasifikasikan sebagai Metrik volume atau metrik volume terperinci.

- Metrik volume adalah metrik kinerja per volume dan penyimpanan yang mengambil dua dimensi, dan. `FileSystemId` `VolumeId` `FileSystemId` memetakan ke sistem file yang menjadi milik volume.
- Metrik volume terperinci adalah per-storage-tier metrik yang mengukur konsumsi penyimpanan per tingkat dengan `StorageTier` dimensi (dengan kemungkinan nilai `SSD` dan `StandardCapacityPool`) dan per tipe data dengan `DataType` dimensi (dengan kemungkinan nilai `User`, `Snapshot`, dan `Other`). Metrik ini memiliki `FileSystemId`, `VolumeId`, `StorageTier`, dan `DataType` dimensi.

Topik

- [I/O Metrik jaringan](#)
- [Metrik kapasitas penyimpanan](#)
- [Metrik volume terperinci](#)

I/O Metrik jaringan

Semua metrik ini mengambil dua dimensi, `FileSystemId` dan `VolumeId`.

Metrik	Deskripsi
<code>DataReadBytes</code>	Jumlah byte (jaringan I/O) dibaca dari volume oleh klien. SumStatistik adalah jumlah total byte yang terkait dengan operasi baca selama periode

Metrik	Deskripsi
	yang ditentukan. Untuk menghitung throughput rata-rata (byte per detik) untuk suatu periode, bagilah Sum statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Byte Statistik valid: Sum
DataWriteBytes	Jumlah byte (jaringan I/O) yang ditulis ke volume oleh klien. SumStatistik adalah jumlah total byte yang terkait dengan operasi tulis selama periode yang ditentukan. Untuk menghitung throughput rata-rata (byte per detik) untuk suatu periode, bagilah Sum statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Byte Statistik valid: Sum
DataReadOperations	Jumlah operasi baca (jaringan I/O) pada volume oleh klien. SumStatistik adalah jumlah total operasi baca selama periode yang ditentukan. Untuk menghitung operasi baca rata-rata per detik untuk suatu periode, bagilah Sum statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: Sum

Metrik	Deskripsi
DataWriteOperations	Jumlah operasi tulis (jaringan I/O) pada volume oleh klien. SumStatistik adalah jumlah total operasi penulisan selama periode yang ditentukan. Untuk menghitung operasi tulis rata-rata per detik untuk suatu periode, bagilah Sum statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: Sum
MetadataOperations	Jumlah I/O operasi (jaringan I/O) dari aktivitas metadata oleh klien ke volume. SumStatistik adalah jumlah total operasi metadata selama periode yang ditentukan. Untuk menghitung rata-rata operasi metadata per detik untuk suatu periode, bagilah Sum statistik dengan jumlah detik dalam periode yang ditentukan. Unit: Hitungan Statistik valid: Sum

Metrik	Deskripsi
DataReadOperationTime	Jumlah total waktu yang dihabiskan dalam volume untuk operasi baca (jaringan I/O) dari klien yang mengakses data dalam volume. SumStatistik adalah jumlah detik yang dihabiskan oleh operasi baca selama periode yang ditentukan. Untuk menghitung latensi baca rata-rata untuk suatu periode, bagilah Sum statistik dengan DataReadOperations metrik selama periode yang sama. Sum Unit: detik Statistik valid: Sum
DataWriteOperationTime	Jumlah total waktu yang dihabiskan dalam volume untuk memenuhi operasi tulis (jaringan I/O) dari klien yang mengakses data dalam volume. SumStatistik adalah jumlah detik yang dihabiskan oleh operasi tulis selama periode yang ditentukan. Untuk menghitung latensi tulis rata-rata untuk suatu periode, bagilah Sum statistik dengan DataWriteOperations metrik selama periode yang sama. Sum Unit: detik Statistik valid: Sum

Metrik	Deskripsi
MetadataOperationTime	Jumlah total waktu yang dihabiskan dalam volume untuk memenuhi operasi metadata (jaringan I/O) dari klien yang mengakses data dalam volume. SumStatistik adalah jumlah detik yang dihabiskan oleh operasi baca selama periode yang ditentukan. Untuk menghitung latensi rata-rata untuk suatu periode, bagilah Sum statistik dengan MetadataOperations periode yang sama. Sum Unit: detik Statistik valid: Sum
CapacityPoolReadBytes	Jumlah byte yang dibaca (jaringan I/O) dari tingkat kumpulan kapasitas volume. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. SumStatistik adalah jumlah total byte yang dibaca dari tingkat kumpulan kapasitas volume selama periode tertentu. Untuk menghitung byte kumpulan kapasitas per detik, bagi Sum statistik dengan detik dalam periode tertentu. Unit: Byte Statistik valid: Sum

Metrik	Deskripsi
CapacityPoolReadOperations	Jumlah operasi baca (jaringan I/O) dari tingkat kumpulan kapasitas volume. Ini berarti permintaan baca kumpulan kapasitas. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. SumStatistik adalah jumlah total operasi baca dari tingkat kumpulan kapasitas volume selama periode tertentu. Untuk menghitung permintaan kumpulan kapasitas per detik, bagi Sum statistik dengan detik dalam periode tertentu. Unit: Hitungan Statistik valid: Sum
CapacityPoolWriteBytes	Jumlah byte yang ditulis (jaringan I/O) ke tingkat kumpulan kapasitas volume. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. SumStatistik adalah jumlah total byte yang ditulis ke tingkat kumpulan kapasitas volume selama periode tertentu. Untuk menghitung byte kumpulan kapasitas per detik, bagi Sum statistik dengan detik dalam periode tertentu. Unit: Byte Statistik valid: Sum

Metrik	Deskripsi
CapacityPoolWriteOperations	Jumlah operasi tulis (jaringan I/O) ke volume dari tier pool kapasitas. Ini diterjemahkan menjadi permintaan tulis. Untuk memastikan integritas data, ONTAP melakukan operasi baca pada kumpulan kapasitas segera setelah melakukan operasi tulis. SumStatistik adalah jumlah total operasi tulis ke tingkat kumpulan kapasitas volume selama periode tertentu. Untuk menghitung permintaan kumpulan kapasitas per detik, bagi Sum statistik dengan detik dalam periode tertentu. Unit: Hitungan Statistik valid: Sum

Metrik kapasitas penyimpanan

Semua metrik ini mengambil dua dimensi, `FileSystemId` dan `VolumeId`.

Metrik	Deskripsi
StorageCapacity	Ukuran volume dalam byte. Unit: Byte Statistik valid: Maximum
StorageUsed	Kapasitas penyimpanan logis yang digunakan dari volume. Unit: Byte Statistik valid: Average

Metrik	Deskripsi
StorageCapacityUtilization	Pemanfaatan kapasitas penyimpanan volume. Unit: Persen Statistik valid: Average
FilesUsed	File yang digunakan (jumlah file atau inode) pada volume. Unit: Hitungan Statistik valid: Average
FilesCapacity	Jumlah total inode yang dapat dibuat pada volume. Unit: Hitungan Statistik valid: Maximum

Metrik volume terperinci

Metrik volume terperinci membutuhkan lebih banyak dimensi daripada metrik volume, memungkinkan pengukuran data Anda yang lebih terperinci. Semua metrik volume rinci memiliki dimensi `FileSystemId`, `VolumeIdStorageTier`, dan `Data Type`.

- `StorageTierDimensi` menunjukkan tingkat penyimpanan yang diukur metrik, dengan kemungkinan nilai `All`, `SSD`, dan `StandardCapacityPool`.
- `Data TypeDimensi` menunjukkan jenis data yang diukur metrik, dengan kemungkinan nilai `All`, `User`, `Snapshot`, dan `Other`.

Tabel berikut mendefinisikan apa ukuran `StorageUsed` metrik untuk dimensi yang terdaftar.

Metrik	Deskripsi
StorageUsed	Jumlah ruang logis yang digunakan, dalam byte. Metrik ini mengukur berbagai jenis

Metrik	Deskripsi
	konsumsi ruang tergantung pada dimensi yang digunakan dengan metrik ini. Saat menyetel <code>StorageTier</code> ke <code>SSD</code> atau <code>StandardCapacityPool</code>, dan menyetel <code>DataType</code> ke <code>All</code>, metrik ini mengukur penggunaan ruang logis untuk volume ini untuk SSD dan tingkatan kumpulan kapasitas Anda. Saat menyetel <code>DataType</code> dimensi ke <code>UserSnapshot</code>, <code>Other</code>, atau, dan pengaturan <code>StorageTier</code> ke <code>All</code>, metrik ini mengukur penggunaan ruang logis untuk setiap jenis data masing-masing. Konsumsi Snapshot data mencakup cadangan snapshot, yang merupakan 5% dari ukuran volume secara default. Unit: Byte Statistik yang valid: Average, Minimum, dan Maximum
<code>StorageCapacityUtilization</code>	Persentase ruang disk fisik yang digunakan volume. Unit: Persen Statistik valid: Maximum

Pemantauan FSx untuk acara ONTAP EMS

Anda dapat memantau FSx peristiwa sistem file ONTAP menggunakan Sistem Manajemen Acara (EMS) asli NetApp ONTAP. Anda dapat melihat peristiwa ini menggunakan CLI NetApp ONTAP.

Topik

- [Ikhtisar acara EMS](#)
- [Melihat acara EMS](#)

- [Penerusan acara EMS ke server Syslog](#)

Ikhtisar acara EMS

Acara EMS adalah pemberitahuan yang dibuat secara otomatis yang mengingatkan Anda ketika kondisi yang telah ditentukan sebelumnya terjadi di sistem file ONTAP Anda FSx . Pemberitahuan ini memberi Anda informasi sehingga Anda dapat mencegah atau memperbaiki masalah yang dapat menyebabkan masalah yang lebih besar, seperti masalah otentikasi mesin virtual penyimpanan (SVM) atau volume penuh.

Secara default, peristiwa dicatat dalam log Sistem Manajemen Acara. Dengan menggunakan EMS, Anda dapat memantau peristiwa seperti perubahan kata sandi pengguna, konstituen dalam kapasitas penuh yang FlexGroup mendekati, Nomor Unit Logika (LUN) secara manual dibawa online atau offline, atau mengubah ukuran volume secara otomatis.

Untuk informasi selengkapnya tentang peristiwa ONTAP EMS, lihat [Referensi ONTAP EMS di Pusat Dokumentasi NetApp ONTAP](#). Untuk menampilkan kategori acara, gunakan panel navigasi kiri dokumen.

Note

Hanya beberapa pesan EMS ONTAP yang tersedia FSx untuk sistem file ONTAP. Untuk melihat daftar pesan EMS ONTAP yang tersedia, gunakan perintah pertunjukan katalog [acara NetApp](#) CLI ONTAP.

Deskripsi acara EMS berisi nama peristiwa, tingkat keparahan, kemungkinan penyebab, pesan log, dan tindakan korektif yang dapat membantu Anda memutuskan cara merespons. Misalnya, peristiwa [Wafli.vol.autosize.fail terjadi ketika ukuran otomatis volume gagal](#). Menurut deskripsi acara, tindakan korektif adalah meningkatkan ukuran maksimum volume saat mengatur ukuran otomatis.

Melihat acara EMS

Gunakan perintah NetApp ONTAP [CLI event log](#) show untuk menampilkan isi log peristiwa. Perintah ini tersedia jika Anda memiliki fsxadmin peran pada sistem file Anda. Sintaks perintah adalah sebagai berikut:

```
event log show [event_options]
```

Peristiwa terbaru terdaftar terlebih dahulu. Secara default, perintah ini menampilkan EMERGENCY, ALERT, dan peristiwa ERROR tingkat keparahan dengan informasi berikut:

- Waktu - Waktu acara.
- Node — Node tempat peristiwa terjadi.
- Keparahan — Tingkat keparahan acara. Untuk menampilkan NOTICE, INFORMATIONAL, atau peristiwa DEBUG tingkat keparahan, gunakan opsi. `-severity`
- Event — Nama dan pesan acara.

Untuk menampilkan informasi rinci tentang peristiwa, gunakan satu atau beberapa opsi acara yang tercantum dalam tabel berikut.

Opsi acara	Deskripsi
<code>-detail</code>	Menampilkan informasi acara tambahan.
<code>-detailtime</code>	Menampilkan informasi acara terperinci dalam urutan kronologis terbalik.
<code>-instance</code>	Menampilkan informasi rinci tentang semua bidang.
<code>-node <i>nodename</i> local</code>	Menampilkan daftar peristiwa untuk node yang Anda tentukan. Gunakan opsi ini <code>-seqnum</code> untuk menampilkan informasi terperinci.
<code>-seqnum <i>sequence_number</i></code>	Memilih peristiwa yang cocok dengan nomor ini dalam urutan. Gunakan dengan <code>-node</code> untuk menampilkan informasi rinci.

Opsi acara	Deskripsi
<code>-time</code> <i>MM/DD/YYYY HH:MM:SS</i>	Memilih peristiwa yang terjadi pada waktu tertentu ini. Gunakan format: MM/DD/YYYY HH: MM: SS [+ HH: MM]. Anda dapat menentukan rentang waktu dengan menggunakan <code>.</code> operator antara dua pernyataan waktu. <pre>event log show - time "04/17/2023 05:55:00".. "04/17/ 2023 06:10:00"</pre> Nilai waktu komparatif relatif terhadap waktu saat ini ketika Anda menjalankan perintah. Contoh berikut menunjukkan cara menampilkan hanya peristiwa yang terjadi dalam menit terakhir: <pre>event log show -time >1m</pre> Bidang bulan dan tanggal opsi ini tidak empuk nol. Bidang ini dapat berupa digit tunggal; misalnya, 4/1/2023 06:45:00.

Opsi acara	Deskripsi
<code>-severity <i>sev_level</i></code>	Memilih peristiwa yang cocok dengan <i>sev_level</i> nilai, yang harus menjadi salah satu dari berikut ini: • EMERGENCY — Gangguan • ALERT— Titik kegagalan tunggal • ERROR- Degradasi • NOTICE— Informasi • INFORMATIONAL — Informasi • DEBUG— Informasi debug Untuk menampilkan semua acara, tentukan tingkat keparahan sebagai berikut: <pre>event log show -severity <=DEBUG</pre>

Opsi acara	Deskripsi
<code>-ems-severity</code> <i>ems_sev_level</i>	Memilih peristiwa yang cocok dengan <i>ems_sev_level</i> nilai, yang harus menjadi salah satu dari berikut ini: • <code>NODE_FAULT</code> Korupsi data terdeteksi atau node tidak dapat menyediakan layanan klien. • <code>SVC_FAULT</code> — Kehilangan layanan sementara — biasanya kesalahan perangkat lunak sementara — terdeteksi. • <code>NODE_ERROR</code> — Kesalahan perangkat keras yang tidak langsung fatal terdeteksi. • <code>SVC_ERROR</code> — Kesalahan perangkat lunak yang tidak langsung fatal terdeteksi. • <code>WARNING</code>— Pesan prioritas tinggi yang tidak menunjukkan kesalahan. • <code>NOTICE</code>— Pesan prioritas normal yang tidak menunjukkan kesalahan. • <code>INFO</code>— Pesan prioritas rendah yang tidak menunjukkan kesalahan. • <code>DEBUG</code>— Pesan debugging. • <code>VAR</code>— Pesan dengan tingkat keparahan variabel, dipilih saat runtime.

Opsi acara	Deskripsi
	Untuk menampilkan semua acara, tentukan tingkat keparahan sebagai berikut: <pre>event log show -ems-severity <=DEBUG</pre>
<code>-source <i>text</i></code>	Memilih peristiwa yang cocok dengan <i>text</i> nilai. Sumbernya biasanya modul perangkat lunak.
<code>-message-name <i>message_name</i></code>	Memilih peristiwa yang cocok dengan <i>message_name</i> nilai. Nama pesan bersifat deskriptif, sehingga menyaring output dengan nama pesan menampilkan pesan dari jenis tertentu.
<code>-event <i>text</i></code>	Memilih peristiwa yang cocok dengan <i>text</i> nilai. eventBidang berisi teks lengkap acara, termasuk parameter apa pun.
<code>-kernel-generation-num <i>integer</i></code>	Memilih peristiwa yang cocok dengan <i>integer</i> nilai. Hanya peristiwa yang berasal dari kernel yang memiliki nomor pembuatan kernel.

Opsi acara	Deskripsi
<code>-kernel-sequence-num <i>integer</i></code>	Memilih peristiwa yang cocok dengan <i>integer</i> nilai. Hanya peristiwa yang berasal dari kernel yang memiliki nomor urut kernel.
<code>-action <i>text</i></code>	Memilih peristiwa yang cocok dengan <i>text</i> nilai. <code>action</code> Bidang ini menjelaskan tindakan korektif apa, jika ada, yang harus Anda ambil untuk memperbaiki situasi.
<code>-description <i>text</i></code>	Memilih peristiwa yang cocok dengan <i>text</i> nilai. <code>description</code> Bidang ini menjelaskan mengapa peristiwa itu terjadi dan apa artinya.
<code>-filter-name <i>filter_name</i></code>	Memilih peristiwa yang cocok dengan <i>filter_name</i> nilai. Hanya peristiwa yang disertakan oleh filter yang ada yang cocok dengan tampilan nilai ini.
<code>-fields <i>fieldname</i> ,...</code>	Menunjukkan bahwa output perintah juga mencakup bidang atau bidang yang ditentukan. Anda dapat menggunakan <code>-fields ?</code> untuk memilih bidang yang ingin Anda tentukan.

Untuk melihat acara EMS

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna [Menggunakan CLI NetApp ONTAP](#) Amazon FSx untuk NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Gunakan `event log show` perintah untuk menampilkan isi log peristiwa.

```
::> event log show
Time                Node          Severity      Event
-----
6/30/2023 13:54:19 node1         NOTICE      vifmgr.portup: A link up event was
received on node node1, port e0a.
6/30/2023 13:54:19 node1         NOTICE      vifmgr.portup: A link up event was
received on node node1, port e0d.
```

Untuk informasi tentang peristiwa EMS yang dikembalikan oleh `event log show` perintah, lihat [Referensi EMS ONTAP](#) di Pusat Dokumentasi NetApp ONTAP.

Penerusan acara EMS ke server Syslog

Anda dapat mengonfigurasi acara EMS untuk meneruskan pemberitahuan ke server Syslog. Penerusan acara EMS digunakan untuk pemantauan real-time sistem file Anda untuk menentukan dan mengisolasi akar penyebab untuk berbagai masalah. Jika lingkungan Anda belum berisi server Syslog untuk pemberitahuan acara, Anda harus membuatnya terlebih dahulu. DNS harus dikonfigurasi pada sistem file untuk menyelesaikan nama server Syslog.

Note

Tujuan Syslog Anda harus terletak di subnet utama yang digunakan oleh sistem file Anda.

Untuk mengonfigurasi peristiwa EMS untuk meneruskan pemberitahuan ke server Syslog

1. Untuk SSH ke NetApp CLI ONTAP sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian Panduan Pengguna [Menggunakan CLI NetApp ONTAP](#) Amazon FSx untuk NetApp ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Gunakan perintah [buat tujuan pemberitahuan acara](#) untuk membuat tujuan pemberitahuan acara dari jenis syslog, menentukan atribut berikut:
 - **dest_name**— Nama tujuan notifikasi yang akan dibuat (misalnya, syslog-ems). Nama tujuan pemberitahuan acara harus memiliki panjang 2 hingga 64 karakter. Karakter yang valid adalah karakter ASCII berikut: A-Z, a-z, 0-9, “_”, dan “-”. Nama harus dimulai dan diakhiri dengan: A-Z, a-z, atau 0-9.
 - **syslog_name**— Nama host server Syslog atau alamat IP yang mengirim pesan Syslog.
 - **transport_protocol**— Protokol yang digunakan untuk mengirim acara:
 - udp-unencrypted— Protokol Datagram Pengguna tanpa keamanan. Ini adalah protokol default.
 - tcp-unencrypted— Protokol Kontrol Transmisi tanpa keamanan.
 - tcp-encrypted— Protokol Kontrol Transmisi dengan Transport Layer Security (TLS). Ketika opsi ini ditentukan, FSx untuk ONTAP memverifikasi identitas host tujuan dengan memvalidasi sertifikatnya.
 - **port_number**— Port server Syslog tempat pesan Syslog dikirim ke. syslog-portParameter nilai default tergantung pada pengaturan untuk syslog-transport parameter. Jika syslog-transport diatur ke tcp-encrypted, nilai syslog-port defaultnya adalah 6514. Jika syslog-transport diatur ke tcp-unencrypted, syslog-port memiliki nilai default 601. Jika tidak, port default diatur ke 514.

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. Gunakan perintah [buat pemberitahuan acara](#) untuk membuat pemberitahuan baru dari serangkaian peristiwa yang ditentukan oleh filter peristiwa ke tujuan notifikasi yang dibuat pada langkah sebelumnya, dengan menentukan atribut berikut:
 - **node_name**— Nama filter acara. Peristiwa yang termasuk dalam filter acara diteruskan ke tujuan yang ditentukan dalam parameter. -destinations
 - **dest_name**— Nama tujuan notifikasi yang ada tempat pemberitahuan acara dikirim.

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. Jika Anda memilih TCP sebagai *transport_protocol*, Anda dapat menggunakan event notification destination check perintah untuk menghasilkan pesan pengujian dan memverifikasi pengaturan Anda berfungsi. Tentukan atribut berikut dengan perintah:

- *node_name*— Nama node (misalnya, FsxId07353f551e6b557b4-01).
- *dest_name*— Nama tujuan notifikasi yang ada tempat pemberitahuan acara dikirim.

```
::> set diag  
:*> event notification destination check -node node_name -destination-  
name dest_name
```

Pemantauan dengan Wawasan Infrastruktur Data

NetApp Data Infrastructure Insights (sebelumnya Cloud Insights) adalah NetApp layanan yang dapat Anda gunakan untuk memantau Amazon Anda FSx untuk sistem file NetApp ONTAP bersama solusi penyimpanan Anda yang lain. NetApp Dengan Data Infrastructure Insights, Anda dapat memantau konfigurasi, kapasitas, dan metrik kinerja dari waktu ke waktu untuk memahami tren beban kerja Anda dan merencanakan kinerja masa depan dan kebutuhan kapasitas penyimpanan. Anda juga dapat membuat peringatan berdasarkan kondisi metrik yang dapat diintegrasikan dengan alur kerja dan alat produktivitas yang ada.

Note

Wawasan Infrastruktur Data tidak didukung untuk sistem file generasi kedua dengan lebih dari satu pasangan HA.

Wawasan Infrastruktur Data menyediakan:

- Luasnya metrik dan log — Kumpulkan metrik konfigurasi, kapasitas, dan kinerja. Pahami tren beban kerja Anda dengan dasbor, peringatan, dan laporan yang telah ditentukan sebelumnya.

- Analitik pengguna dan perlindungan ransomware — Dengan snapshot Cloud Secure dan ONTAP Anda dapat mengaudit, mendeteksi, menghentikan, dan memperbaiki insiden kesalahan pengguna dan ransomware.
- SnapMirror pelaporan — Pahami SnapMirror hubungan Anda dan tetapkan peringatan tentang masalah replikasi.
- Perencanaan kapasitas - Memahami persyaratan sumber daya beban kerja lokal untuk membantu Anda memigrasikan beban kerja ke konfigurasi ONTAP yang lebih efisien FSx . Anda juga dapat menggunakan wawasan ini untuk merencanakan kapan lebih banyak kinerja atau kapasitas akan diperlukan untuk penerapan ONTAP Anda FSx .

Untuk informasi selengkapnya, lihat dokumentasi [Wawasan Infrastruktur Data di Dokumentasi](#) Produk NetApp ONTAP.

Pemantauan FSx untuk sistem file ONTAP menggunakan Harvest dan Grafana

NetApp Harvest adalah alat open source untuk mengumpulkan metrik kinerja dan kapasitas dari sistem ONTAP, dan kompatibel dengan FSx ONTAP. Anda dapat menggunakan Harvest with Grafana untuk solusi pemantauan open source.

Memulai Harvest dan Grafana

Bagian berikut merinci bagaimana Anda dapat mengatur dan mengonfigurasi Harvest dan Grafana untuk mengukur kinerja sistem file ONTAP dan pemanfaatan kapasitas penyimpanan Anda FSx .

Anda dapat memantau Amazon Anda FSx untuk sistem file NetApp ONTAP dengan menggunakan Harvest dan Grafana. NetApp Harvest memantau pusat ONTAP data dengan mengumpulkan metrik kinerja, kapasitas, dan perangkat keras dari FSx untuk sistem file ONTAP. Grafana menyediakan dasbor tempat Harvest metrik yang dikumpulkan dapat ditampilkan.

Dasbor Harvest yang Didukung

Amazon FSx untuk NetApp ONTAP memperlihatkan kumpulan metrik yang berbeda dari yang dilakukan di tempat. NetApp ONTAP Oleh karena itu, hanya out-of-the-box Harvest dasbor berikut yang diberi tag saat ini fsx didukung untuk digunakan dengan FSx ONTAP. Beberapa panel di dasbor ini mungkin kehilangan informasi yang tidak didukung.

- Panen: Metadata
- ONTAP: Agregat
- ONTAP: cDOT
- ONTAP: Kluster
- ONTAP: Kepatuhan
- ONTAP: Pusat Data
- ONTAP: Perlindungan Data
- ONTAP: LUN
- ONTAP: Jaringan
- ONTAP: Node
- ONTAP: Qtree
- ONTAP: Keamanan
- ONTAP: SnapMirror
- ONTAP: Tujuan SnapMirror
- ONTAP: Sumber SnapMirror
- ONTAP: SVM
- ONTAP: Volume
- ONTAP: Volume oleh SVM
- ONTAP: Volume Menyelam Dalam

HarvestDasbor berikut didukung oleh FSx untuk ONTAP, tetapi tidak diaktifkan secara default di Harvest

- ONTAP: FlexCache
- ONTAP: FlexGroup
- ONTAP: Klien NFS
- ONTAP: Monitor NFSv4 Storepool
- ONTAP: Pemecahan Masalah NFS
- ONTAP: Ruang nama NVMe
- ONTAP: SMB

- ONTAP: Beban kerja

Dasbor yang tidak didukung Harvest

HarvestDasbor berikut tidak didukung oleh FSx untuk ONTAP.

- ONTAP: Disk
- ONTAP: Operasi Layanan Eksternal
- ONTAP: Analisis Sistem File (FSA)
- ONTAP: Ruang Kepala
- ONTAP: Kesehatan
- ONTAP: Permintaan MAV
- ONTAP: MetroCluster
- ONTAP: Kekuasaan
- ONTAP: Rak
- ONTAP: Toko Objek S3

CloudFormation template

Untuk memulai, Anda dapat menerapkan CloudFormation template yang secara otomatis meluncurkan EC2 instance Amazon yang menjalankan Harvest dan Grafana. Sebagai masukan ke CloudFormation template, Anda menentukan `fsxadmin` pengguna dan titik akhir FSx manajemen Amazon untuk sistem file yang akan ditambahkan sebagai bagian dari penerapan ini. Setelah penerapan selesai, Anda dapat masuk ke dasbor Grafana untuk memantau sistem file Anda.

Solusi ini digunakan CloudFormation untuk mengotomatiskan penerapan solusi Harvest dan Grafana. Template membuat instance Amazon EC2 Linux dan menginstal perangkat lunak Harvest dan Grafana. Untuk menggunakan solusi ini, unduh [fsx-ontap-harvest-grafana CloudFormation template.template](#).

Note

Menerapkan solusi ini menimbulkan penagihan untuk layanan terkait. AWS Untuk informasi lebih lanjut, lihat halaman detail harga untuk layanan tersebut.

Jenis EC2 instans Amazon

Saat mengonfigurasi template, Anda memberikan jenis EC2 instans Amazon. NetAppRekomendasi untuk ukuran instans tergantung pada berapa banyak sistem file yang Anda pantau dan jumlah metrik yang Anda pilih untuk dikumpulkan. Dengan konfigurasi default, untuk setiap 10 sistem file yang Anda pantau, NetApp merekomendasikan:

- CPU: 2 core
- Memori: 1 GB
- Disk: 500 MB (sebagian besar digunakan oleh file log)

Berikut ini adalah beberapa konfigurasi sampel dan jenis t3 instance yang mungkin Anda pilih.

Sistem berkas	CPU	Disk	Jenis instans
Di bawah 10	2 inti	500 MB	t3.micro
10—40	4 inti	1000 MB	t3.xlarge
40+	8 inti	2000 MB	t3.2xlarge

Untuk informasi selengkapnya tentang jenis EC2 instans Amazon, lihat [Instans tujuan umum](#) di Panduan EC2 Pengguna Amazon.

Aturan port instance

Saat menyiapkan EC2 instans Amazon, pastikan port 3000 dan 9090 terbuka untuk lalu lintas masuk untuk grup keamanan tempat instans Amazon EC2 Harvest dan Grafana berada. Karena instance yang diluncurkan terhubung ke titik akhir melalui HTTPS, maka perlu menyelesaikan titik akhir, yang membutuhkan port 53 TCP/UDP untuk DNS. Selain itu, untuk mencapai titik akhir diperlukan port 443 TCP untuk HTTPS dan Akses Internet.

Prosedur penyebaran

Prosedur berikut mengkonfigurasi dan menyebarkan solusi. Harvest/Grafana Dibutuhkan sekitar lima menit untuk men-deploy. Sebelum memulai, Anda harus memiliki FSx sistem file ONTAP yang berjalan di Amazon Virtual Private Cloud (Amazon VPC) di akun AWS Anda, dan informasi parameter

untuk templat yang tercantum di bawah ini. Untuk informasi selengkapnya tentang membuat sistem file, lihat [Membuat sistem file](#).

Untuk meluncurkan tumpukan Harvest/Grafana solusi

1. Unduh [fsx-ontap-harvest-grafana CloudFormation template.template](#). Untuk informasi selengkapnya tentang membuat CloudFormation tumpukan, lihat [Membuat tumpukan di AWS CloudFormation konsol](#) di Panduan AWS CloudFormation Pengguna.

 Note

Secara default, template ini diluncurkan di Wilayah AS Timur (Virginia N.) AWS . Anda harus meluncurkan solusi ini Wilayah AWS di tempat Amazon FSx tersedia. Untuk informasi selengkapnya, lihat [FSx titik akhir dan kuota Amazon](#) di Referensi Umum AWS

2. Untuk Parameter, tinjau parameter untuk templat dan ubah sesuai kebutuhan sistem file Anda. Solusi ini menggunakan nilai default berikut.

Parameter	Default	Deskripsi
InstanceType	t3.micro	Jenis EC2 instans Amazon. Berikut ini adalah jenis t3 instance. • t3.micro • t3.small • t3.medium • t3.large • t3.xlarge • t3.2xlarge Untuk daftar lengkap nilai tipe EC2 instans Amazon yang diizinkan untuk parameter ini, lihat fsx-ontap-harvest-grafana .template.

Parameter	Default	Deskripsi
KeyPair	Tidak ada nilai default	Key pair yang digunakan untuk mengakses EC2 instans Amazon.
SecurityGroup	Tidak ada nilai default	ID grup Keamanan untuk Harvest/Grafana Instans. Pastikan port Inbound 3000 dan 9090, selain port 53 dan 443, terbuka dari klien yang ingin Anda gunakan untuk mengakses dasbor Grafana Anda.
Jenis Subnet	Tidak ada nilai default	Tentukan jenis subnet, salah satu public atau private. Gunakan public subnet untuk sumber daya yang harus terhubung ke internet, dan subnet pribadi untuk sumber daya yang tidak akan terhubung ke internet. Untuk informasi selengkapnya, lihat Jenis subnet di Panduan Pengguna Amazon VPC.

Parameter	Default	Deskripsi
Subnet	Tidak ada nilai default	Tentukan subnet yang sama dengan Amazon Anda FSx untuk subnet pilihan sistem file NetApp ONTAP. Anda dapat menemukan ID subnet Pilihan sistem file di FSx konsol Amazon, di tab Jaringan & keamanan di halaman detail sistem file FSx untuk ONTAP
LatestLinuxAmild	<code>/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2</code>	Versi terbaru dari Amazon Linux 2 AMI di berikan Wilayah AWS.
FSxEndPoint	Tidak ada nilai default	Alamat IP titik akhir Manajemen sistem file. Anda dapat menemukan alamat IP titik akhir manajemen sistem file di FSx konsol Amazon, di tab Administrasi halaman detail sistem file FSx untuk ONTAP.
SecretName	Tidak ada nilai default	AWS Secrets Manager nama rahasia yang berisi kata sandi untuk fsxadmin pengguna sistem file. Ini adalah kata sandi yang Anda berikan saat Anda membuat sistem file.

3. Pilih Selanjutnya.
4. Untuk Opsi, pilih Selanjutnya.

5. Untuk Meninjau, tinjau dan konfirmasi pengaturan yang baru. Anda harus memilih kotak pengecekan yang menyatakan bahwa templat menghasilkan sumber daya IAM.
6. Pilih Buat untuk men-deploy tumpukan.

Anda dapat melihat status tumpukan di CloudFormation konsol di kolom Status. Anda dapat melihat status CREATE_COMPLETE dalam waktu sekitar lima menit.

Masuk ke Grafana

Setelah penerapan selesai, gunakan browser Anda untuk masuk ke dasbor Grafana di IP dan port 3000 instance Amazon EC2 :

```
http://EC2_instance_IP:3000
```

Saat diminta, gunakan nama pengguna default Grafana admin () dan kata sandi pass (). Kami menyarankan Anda mengubah kata sandi Anda segera setelah Anda masuk.

Untuk informasi lebih lanjut, lihat halaman [NetApp Harvest](#) di GitHub.

Pemecahan Masalah Panen dan Grafana

Jika Anda menemukan data yang hilang yang disebutkan di dasbor Harvest dan Grafana atau mengalami kesulitan dalam mengatur Harvest dan Grafana FSx untuk ONTAP, periksa topik berikut untuk solusi potensial.

Topik

- [Dasbor SVM dan volume kosong](#)
- [CloudFormation tumpukan digulung kembali setelah batas waktu](#)

Dasbor SVM dan volume kosong

Jika CloudFormation tumpukan berhasil diterapkan dan dapat menghubungi Grafana tetapi SVM dan dasbor volume kosong, gunakan prosedur berikut untuk memecahkan masalah lingkungan Anda. Anda akan memerlukan akses SSH ke EC2 instans Amazon tempat Harvest dan Grafana digunakan.

1. SSH ke EC2 instans Amazon tempat klien Harvest dan Grafana Anda berjalan.

```
[~]$ ssh ec2-user@ec2_ip_address
```

2. Gunakan perintah berikut untuk membuka `harvest.yml` file dan:

- Verifikasi bahwa entri telah dibuat untuk instans ONTAP Anda FSx sebagai `Cluster-2`.
- Verifikasi bahwa entri untuk nama pengguna dan kata sandi cocok dengan `fsxadmin` kredensi Anda.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/harvest.yml
```

3. Jika bidang kata sandi kosong, buka file di editor dan perbarui dengan `fsxadmin` kata sandi, sebagai berikut:

```
[ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/harvest.yml
```

4. Pastikan kredensial `fsxadmin` pengguna disimpan di Secrets Manager dalam format berikut untuk penerapan di masa mendatang, ganti `fsxadmin_password` dengan kata sandi Anda.

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

CloudFormation tumpukan digulung kembali setelah batas waktu

Jika Anda tidak dapat menyebarkan CloudFormation tumpukan dengan sukses dan bergulir kembali dengan kesalahan, gunakan prosedur berikut untuk menyelesaikan masalah. Anda akan memerlukan akses SSH ke EC2 instance yang digunakan oleh tumpukan. CloudFormation

1. Pasang kembali CloudFormation tumpukan, pastikan rollback otomatis dinonaktifkan.
2. SSH ke EC2 instans Amazon tempat klien Harvest dan Grafana Anda berjalan.

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. Verfy bahwa wadah docker berhasil dimulai menggunakan perintah berikut.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

Dalam tanggapan Anda akan melihat lima kontainer sebagai berikut:

CONTAINER ID	IMAGE	COMMAND	CREATED	
STATUS		PORTS	NAMES	
6b9b3f2085ef	rahulguptajss/harvest	"bin/poller --config..."	8 minutes ago	
Restarting (1)	20 seconds ago		harvest_cluster-2	
3cf3e3623fde	rahulguptajss/harvest	"bin/poller --config..."	8 minutes ago	Up
About a minute			harvest_cluster-1	
708f3b7ef6f8	grafana/grafana	"/run.sh"	8 minutes ago	Up
8 minutes		0.0.0.0:3000->3000/tcp	harvest_grafana	
0febee61cab7	prom/alertmanager	"/bin/alertmanager -..."	8	
minutes ago	Up 8 minutes	0.0.0.0:9093->9093/tcp		
	harvest_prometheus_alertmanager			
1706d8cd5a0c	prom/prometheus	"/bin/prometheus --c..."	8 minutes ago	Up
8 minutes		0.0.0.0:9090->9090/tcp	harvest_prometheus	

4. Jika wadah docker tidak berjalan, periksa kegagalan dalam `/var/log/cloud-init-output.log` file sebagai berikut.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
PLAY [Manage Harvest]
*****

TASK [Gathering Facts] *****
ok: [localhost]

TASK [Verify images] *****
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
"changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
"changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
"changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
"changed": false, "item": "grafana/grafana",
```

```
"msg": "Error connecting: Error while fetching server API version: ('Connection
aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

```

```
PLAY RECAP *****
localhost                : ok=1    changed=0    unreachable=0    failed=1
skipped=0    rescued=0    ignored=0

```

5. Jika ada kegagalan, jalankan perintah berikut untuk menyebarkan kontainer Harvest dan Grafana.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
[ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
[ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
manage_harvest.yml
[ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
manage_harvest.yml --tags api

```

6. Validasi kontainer yang dimulai dengan sukses dengan menjalankan `sudo docker ps` dan menghubungkan ke URL Harvest dan Grafana Anda.

Pemantauan FSx Panggilan API ONTAP dengan AWS CloudTrail

Amazon FSx terintegrasi dengan AWS CloudTrail, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, atau AWS layanan di Amazon FSx. CloudTrail menangkap semua panggilan Amazon FSx API untuk Amazon FSx untuk NetApp ONTAP sebagai acara. Panggilan yang diambil termasuk panggilan dari FSx konsol Amazon dan dari 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. Anda juga dapat menentukan alamat IP untuk membuat permintaan, siapa yang membuat permintaan, kapan permintaan dibuat, dan detail tambahan.

Untuk mempelajari selengkapnya CloudTrail, lihat [Panduan AWS CloudTrail Pengguna](#).

FSx Informasi Amazon di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Saat aktivitas API terjadi di Amazon FSx, aktivitas tersebut direkam dalam suatu CloudTrail peristiwa bersama dengan peristiwa AWS layanan lainnya dalam riwayat Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat [Melihat peristiwa dengan Riwayat CloudTrail acara](#).

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, 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 AWS Wilayah. Jejak mencatat peristiwa dari semua AWS 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 topik berikut di Panduan Pengguna AWS CloudTrail :

- [Membuat jejak untuk Anda Akun AWS](#)
- [AWS integrasi layanan dengan CloudTrail Log](#)
- [Mengonfigurasi notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima file CloudTrail log dari beberapa wilayah](#) dan [Menerima file CloudTrail log dari beberapa akun](#)

Semua [panggilan Amazon FSx API](#) dicatat oleh CloudTrail. Misalnya, panggilan ke `CreateFileSystem` dan `TagResource` operasi 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 kredensial 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 CloudTrail UserIdentity](#) di AWS CloudTrail Panduan Pengguna.

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 manapun dan mencakup informasi tentang tindakan yang diminta, tanggal dan waktu tindakan, parameter permintaan, dan sebagainya. CloudTrail file log bukanlah jejak tumpukan yang diurutkan dari panggilan API publik, jadi file tersebut tidak muncul dalam urutan tertentu.

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan 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"
}
```

Bekerja dengan Microsoft Active Directory FSx untuk ONTAP

Amazon FSx bekerja dengan Microsoft Active Directory untuk berintegrasi dengan lingkungan yang ada. Active Directory adalah layanan direktori Microsoft yang digunakan untuk menyimpan informasi tentang objek di jaringan, dan untuk membantu administrator dan pengguna menemukan dan menggunakan informasi ini. Objek-objek ini biasanya mencakup sumber daya bersama, seperti server file dan pengguna jaringan dan akun komputer.

Anda dapat secara opsional bergabung dengan mesin virtual FSx penyimpanan ONTAP (SVMs) ke domain Active Directory Anda untuk memberikan otentikasi pengguna dan kontrol akses tingkat file dan folder. Klien blok pesan server (SMB) kemudian dapat menggunakan identitas pengguna yang ada di Active Directory untuk mengautentikasi diri mereka sendiri dan mengakses volume SVM. Pengguna Anda dapat menggunakan identitas mereka yang ada untuk mengontrol akses ke file dan folder individual. Selain itu, Anda dapat memigrasikan file dan folder yang ada serta konfigurasi daftar kontrol akses keamanan (ACL) ke Amazon FSx tanpa modifikasi apa pun.

Jika infrastruktur domain Microsoft Active Directory tidak tersedia, Anda dapat mengonfigurasi server Server Message Block (SMB) di workgroup pada SVM sebagai alternatif untuk menggabungkan SVM ke Microsoft Active Directory. Untuk informasi selengkapnya, lihat [Menyiapkan server SMB di workgroup](#).

Saat Anda bergabung dengan Amazon FSx untuk NetApp ONTAP ke Active Directory, Anda menggabungkan sistem file SVMs ke Active Directory secara independen. Ini berarti bahwa Anda dapat memiliki sistem file dengan beberapa SVMs yang bergabung ke Active Directory, dan lainnya SVMs yang tidak.

Setelah SVM bergabung ke Active Directory, Anda dapat memperbarui properti konfigurasi Active Directory berikut:

- Alamat IP server DNS
- Nama pengguna dan kata sandi akun layanan Direktori Aktif yang dikelola sendiri

Topik

- [Prasyarat untuk bergabung dengan SVM ke Microsoft AD yang dikelola sendiri](#)
- [Praktik terbaik untuk bekerja dengan Active Directory](#)

- [Cara kerja bergabung SVMs ke Microsoft Active Directory](#)
- [Mengelola konfigurasi SVM Active Directory](#)

Prasyarat untuk bergabung dengan SVM ke Microsoft AD yang dikelola sendiri

Sebelum Anda bergabung dengan FSx ONTAP SVM ke domain Microsoft AD yang dikelola sendiri, pastikan Direktori Aktif dan jaringan Anda memenuhi persyaratan yang dijelaskan di bagian berikut.

Topik

- [Persyaratan Direktori Aktif lokal](#)
- [Persyaratan konfigurasi jaringan](#)
- [Persyaratan akun layanan Direktori Aktif](#)

Persyaratan Direktori Aktif lokal

Pastikan Anda sudah memiliki iklan Microsoft lokal atau yang dikelola sendiri lainnya yang dapat Anda gunakan untuk bergabung dengan SVM. Direktori Aktif ini harus memiliki konfigurasi berikut:

- Tingkat fungsional domain pengontrol domain Active Directory berada di Windows Server 2000 atau lebih tinggi.
- Active Directory menggunakan nama domain yang tidak dalam format Single Label Domain (SLD). Amazon FSx tidak mendukung domain SLD.
- Jika Anda memiliki situs Active Directory yang ditentukan, pastikan subnet di VPC yang terkait dengan sistem file ONTAP FSx Anda didefinisikan di situs Active Directory yang sama, dan tidak ada konflik antara subnet VPC Anda dan subnet di situs Active Directory Anda.

Note

Jika Anda menggunakan Directory Service, FSx untuk ONTAP tidak mendukung bergabung SVMs ke Simple Active Directory.

Persyaratan konfigurasi jaringan

Pastikan Anda memiliki konfigurasi jaringan berikut dan informasi terkait yang tersedia untuk Anda.

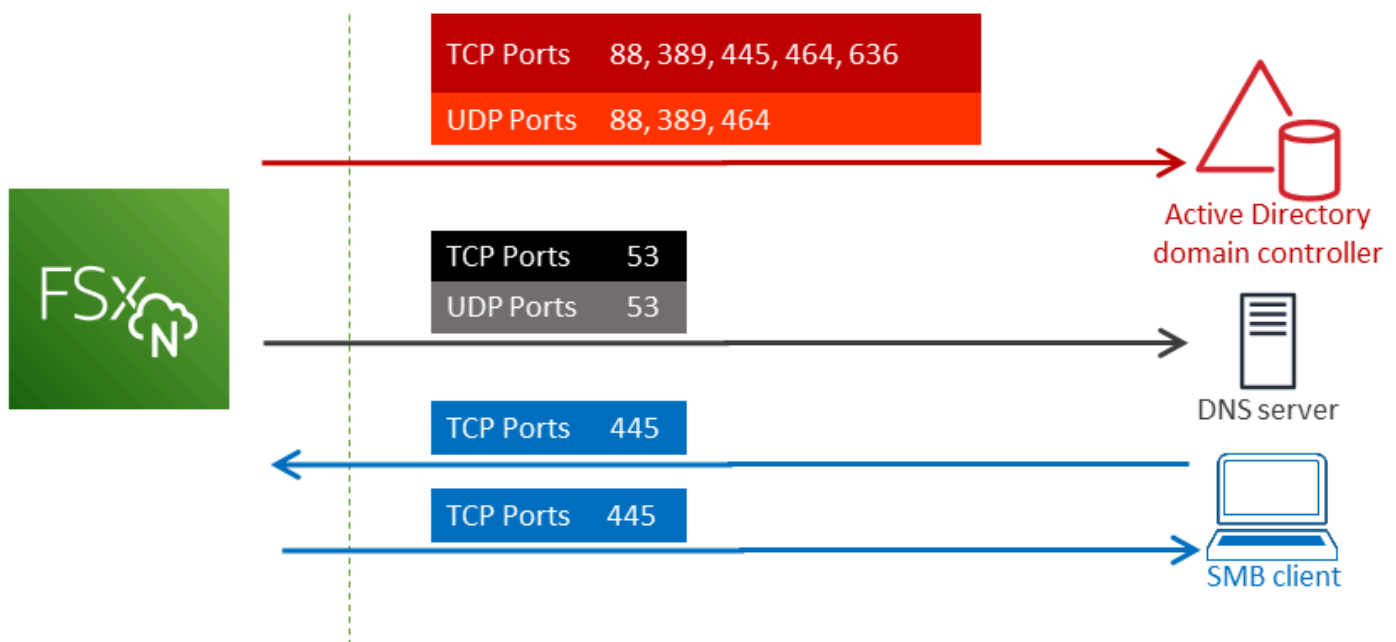
⚠ Important

Agar SVM dapat bergabung dengan Active Directory, Anda perlu memastikan bahwa port yang didokumentasikan dalam topik ini memungkinkan lalu lintas antara semua Active Directory Domain Controller dan kedua alamat IP iSCSI (iscsi_1 dan iscsi_2 logical interface ()) pada SVM. LIFs

- Server DNS dan alamat IP pengontrol domain Direktori Aktif.
- Konektivitas antara VPC Amazon tempat Anda membuat sistem file dan Direktori Aktif yang dikelola sendiri menggunakan [Direct Connect](#), [Site-to-Site VPN](#) atau [AWS Transit Gateway](#)
- Grup keamanan dan Jaringan VPC ACLs untuk subnet tempat Anda membuat sistem file harus mengizinkan lalu lintas pada port dan arah yang ditunjukkan pada diagram berikut.

FSx for ONTAP File Server port requirements

Configure VPC security groups that you've associated with your Amazon FSx file system, along with any VPC Network ACLs and ONTAP firewalls to allow network traffic on the following ports:



Peran setiap port dijelaskan dalam tabel berikut.

Protokol	Port	Peran
TCP/UDP	53	Sistem Nama Domain (DNS)
TCP/UDP	88	Autentikasi Kerberos
TCP/UDP	389	Protokol Akses Direktori Ringan (LDAP)
TCP	445	Pembagian file SMB Layanan Direktori
TCP/UDP	464	Ubah/Atur kata sandi
TCP	636	Protokol Akses Direktori Ringan di atas TLS/SSL (LDAPS)

- Aturan lalu lintas ini juga harus dicerminkan pada firewall yang berlaku untuk masing-masing pengontrol domain Active Directory, 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.

Persyaratan akun layanan Direktori Aktif

Pastikan Anda memiliki akun layanan di Microsoft AD yang dikelola sendiri yang telah mendelegasikan izin untuk bergabung dengan komputer ke domain. Akun layanan adalah akun pengguna di Direktori Aktif yang dikelola sendiri yang telah didelegasikan tugas-tugas tertentu.

Minimal, akun layanan harus didelegasikan izin berikut di OU tempat Anda bergabung dengan SVM:

- Kemampuan untuk mengatur ulang kata sandi
- Kemampuan untuk membatasi akun dari membaca dan menulis data
- Kemampuan untuk mengatur msDS-SupportedEncryptionTypes properti pada objek komputer
- Kemampuan tervalidasi untuk menulis ke nama host DNS
- Kemampuan tervalidasi untuk menulis ke nama utama layanan

- Kemampuan untuk membuat dan menghapus objek komputer
- Kemampuan tervalidasi untuk membaca dan menulis Pembatasan Akun

Ini mewakili serangkaian izin minimum yang diperlukan untuk menggabungkan objek komputer ke Direktori Aktif Anda. Untuk informasi selengkapnya, lihat topik dokumentasi Windows Server [Kesalahan: Akses ditolak ketika pengguna non-administrator yang telah didelegasikan kontrol mencoba menggabungkan komputer ke pengontrol domain](#).

Anda dapat menyimpan kredensi akun layanan Active Directory Anda di AWS Secrets Manager (disarankan) dan memberikan Amazon FSx dengan ARN rahasia untuk bergabung dengan Active Directory Anda, atau Anda dapat memberikan kredensial teks biasa.

Untuk mempelajari selengkapnya tentang membuat akun layanan dengan izin yang benar, lihat [Mendelegasikan izin ke akun layanan Amazon FSx Anda](#).

Important

Amazon FSx memerlukan akun layanan yang valid sepanjang masa hidup sistem FSx file Amazon Anda. Amazon FSx harus dapat sepenuhnya mengelola sistem file dan melakukan tugas yang mengharuskannya untuk berhenti bergabung dan bergabung kembali dengan sumber daya ke domain Direktori Aktif Anda. Tugas-tugas ini termasuk mengganti sistem file yang gagal atau SVM, atau menambal perangkat lunak NetApp ONTAP. Perbarui informasi konfigurasi Direktori Aktif Anda dengan Amazon FSx, termasuk kredensial akun layanan. Untuk mempelajari selengkapnya, lihat [Menjaga konfigurasi Direktori Aktif Anda diperbarui dengan Amazon FSx](#).

Jika ini adalah pertama kalinya Anda menggunakan AWS dan FSx untuk ONTAP, pastikan Anda menyelesaikan langkah penyiapan awal sebelum memulai integrasi Active Directory. Untuk informasi selengkapnya, lihat [Menyiapkan FSx untuk ONTAP](#).

Important

Jangan pindahkan objek komputer yang dibuat FSx Amazon di OU setelah Anda SVMs dibuat, atau hapus Direktori Aktif Anda saat SVM Anda bergabung dengannya. Melakukannya akan menyebabkan Anda SVMs menjadi salah konfigurasi.

Praktik terbaik untuk bekerja dengan Active Directory

Berikut adalah beberapa saran dan panduan yang harus Anda pertimbangkan saat bergabung dengan Amazon FSx untuk NetApp ONTAP SVMs ke Microsoft Active Directory yang dikelola sendiri. Perhatikan bahwa ini direkomendasikan sebagai praktik terbaik, tetapi tidak diwajibkan.

Topik

- [Mendelegasikan izin ke akun layanan Amazon FSx Anda](#)
- [Menjaga konfigurasi Direktori Aktif Anda diperbarui dengan Amazon FSx](#)
- [Menggunakan grup keamanan untuk membatasi lalu lintas dalam VPC](#)
- [Membuat aturan grup keamanan keluar untuk antarmuka jaringan sistem file Anda](#)
- [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#)

Mendelegasikan izin ke akun layanan Amazon FSx Anda

Pastikan untuk mengonfigurasi akun layanan yang Anda berikan ke Amazon FSx dengan izin minimum yang diperlukan. Selain itu, pisahkan Unit Organisasi (OU) dari masalah pengontrol domain lainnya.

Untuk bergabung dengan Amazon FSx SVMs ke domain Anda, pastikan akun layanan telah mendelegasikan izin. Anggota grup Admin Domain memiliki izin yang cukup untuk melakukan tugas ini. Namun, sebagai praktik terbaik, gunakan akun layanan yang hanya memiliki izin minimum yang diperlukan untuk melakukan ini. Prosedur berikut menunjukkan cara mendelegasikan hanya izin yang diperlukan FSx untuk bergabung ONTAP SVMs ke domain Anda.

Lakukan prosedur ini pada mesin yang bergabung dengan direktori Anda dan menginstal snap-in Active Directory User and Computers MMC.

Untuk membuat akun layanan untuk domain Microsoft Active Directory

1. Pastikan Anda masuk sebagai administrator domain untuk domain Microsoft 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 Tambahkan untuk menambahkan pengguna tertentu atau grup tertentu untuk Pengguna dan grup yang dipilih, lalu pilih Selanjutnya.
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 Selanjutnya.
10. Di bawah Tampilkan izin ini, pastikan bahwa Umum dan Properti spesifik dipilih.
11. Untuk Izin, pilih:
 - Setel Ulang Kata Sandi
 - Baca dan tulis Pembatasan Akun
 - Menulis tervalidasi ke nama host DNS
 - Menulis tervalidasi ke nama utama layanan
 - Tulis MSDs- SupportedEncryptionTypes
12. Pilih Selanjutnya, dan kemudian pilih Selesai.
13. Tutup snap-in Active Directory User and Computers MMC.

Important

Jangan pindahkan objek komputer yang FSx dibuat Amazon di OU setelah Anda SVMs dibuat. Melakukannya akan menyebabkan Anda SVMs menjadi salah konfigurasi.

Menjaga konfigurasi Direktori Aktif Anda diperbarui dengan Amazon FSx

Untuk ketersediaan Amazon yang tidak terputus FSx SVMs, perbarui konfigurasi Active Directory (AD) SVM yang dikelola sendiri saat Anda mengubah pengaturan AD yang dikelola sendiri.

Misalnya, ketika AD Anda menggunakan kebijakan pengaturan ulang kata sandi berbasis waktu. Dalam hal ini, segera setelah kata sandi diatur ulang, pastikan untuk memperbarui kata sandi akun layanan dengan Amazon FSx. Untuk melakukan ini, gunakan FSx konsol Amazon, Amazon FSx API, atau AWS CLI. Demikian pula, jika alamat IP server DNS berubah untuk domain Active Directory Anda, segera setelah perubahan terjadi perbarui alamat IP server DNS dengan Amazon. FSx

Jika ada masalah dengan konfigurasi AD yang dikelola sendiri yang diperbarui, status SVM akan beralih ke Salah Konfigurasi. Status ini menampilkan pesan kesalahan dan tindakan yang disarankan di samping deskripsi SVM di konsol, API, dan CLI. Jika terjadi masalah dengan konfigurasi AD SVM Anda, pastikan untuk mengambil tindakan korektif yang disarankan untuk properti konfigurasi. Jika masalah teratasi, verifikasi bahwa status SVM Anda berubah menjadi Dibuat.

Untuk informasi selengkapnya, lihat [Memperbarui konfigurasi SVM Active Directory yang ada menggunakan Konsol Manajemen AWS, AWS CLI, dan API](#) dan [Ubah konfigurasi Active Directory menggunakan ONTAP CLI](#).

Menggunakan grup keamanan untuk membatasi lalu lintas dalam VPC

Untuk membatasi lalu lintas jaringan di virtual private cloud (VPC) Anda, Anda dapat menerapkan prinsip pengurangan hak istimewa dalam VPC Anda. Dengan kata lain, Anda dapat membatasi izin ke yang minimum yang diperlukan. Untuk melakukannya, gunakan aturan grup keamanan. Untuk mempelajari selengkapnya, lihat [Grup keamanan Amazon VPC](#).

Membuat aturan grup keamanan keluar untuk antarmuka jaringan sistem file Anda

Untuk keamanan yang lebih besar, pertimbangkan untuk mengkonfigurasi grup keamanan dengan aturan lalu lintas keluar. Aturan ini harus mengizinkan lalu lintas keluar hanya ke pengontrol domain AD yang dikelola sendiri atau dalam subnet atau grup keamanan. Terapkan grup keamanan ini ke VPC yang terkait dengan elastic network interface sistem FSx file Amazon Anda. Untuk mempelajari selengkapnya, lihat [Kontrol Akses Sistem File dengan Amazon VPC](#).

Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager

Anda dapat menggunakan AWS Secrets Manager untuk menyimpan dan mengelola domain Microsoft Active Directory bergabung dengan kredensial akun layanan dengan aman. Pendekatan ini menghilangkan kebutuhan untuk menyimpan kredensial sensitif dalam teks biasa dalam kode aplikasi atau file konfigurasi, memperkuat postur keamanan Anda.

Anda juga dapat mengonfigurasi kebijakan IAM untuk mengelola akses ke rahasia Anda, dan menyiapkan kebijakan rotasi otomatis untuk kata sandi Anda.

Simpan kredensial Direktori Aktif di AWS Secrets Manager (Konsol)

Langkah 1: Buat kunci KMS

Buat kunci KMS untuk mengenkripsi dan mendekripsi kredensial Active Directory Anda di Secrets Manager.

Untuk membuat kunci

Note

Untuk Encryption Key, buat kunci baru, jangan gunakan kunci KMS AWS default. Pastikan untuk membuat AWS KMS key di Wilayah yang sama yang berisi SVM yang ingin Anda gabungkan ke Direktori Aktif Anda.

1. Buka AWS KMS konsol di <https://console.aws.amazon.com/kms>.
2. Pilih Buat kunci.
3. Untuk Tipe Kunci, pilih Simetris.
4. Untuk Penggunaan Kunci, pilih Enkripsi dan dekripsi.
5. Untuk opsi Lanjutan, lakukan hal berikut:
 - a. Untuk Asal materi kunci, pilih KMS.
 - b. Untuk Regionalitas, pilih kunci Wilayah Tunggal dan pilih Berikutnya.
6. Pilih Berikutnya.
7. Untuk Alias, berikan nama untuk kunci KMS.
8. (Opsional) Untuk Deskripsi, berikan deskripsi kunci KMS.
9. (Opsional) Untuk Tag, berikan tag untuk kunci KMS dan pilih Berikutnya.
10. (Opsional) Untuk administrator Key, berikan pengguna IAM dan peran yang diizinkan untuk mengelola kunci ini.
11. Untuk penghapusan Kunci, simpan kotak yang dipilih untuk Izinkan administrator kunci untuk menghapus kunci ini dan pilih Berikutnya.
12. (Opsional) Untuk pengguna Kunci, berikan pengguna IAM dan peran yang berwenang untuk menggunakan kunci ini dalam operasi kriptografi. Pilih Berikutnya.
13. Untuk kebijakan Kunci, pilih Edit dan sertakan yang berikut ini ke Pernyataan kebijakan FSx untuk mengizinkan Amazon menggunakan kunci KMS dan pilih Berikutnya. Pastikan untuk

mengganti *us-west-2* ke Wilayah AWS tempat sistem file digunakan dan *123456789012* ke Akun AWS ID Anda.

```
{
  "Sid": "Allow FSx to use the KMS key",
  "Version": "2012-10-17",
  "Effect": "Allow",
  "Principal": {
    "Service": "fsx.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "secretsmanager.us-west-2.amazonaws.com",
      "aws:SourceAccount": "123456789012"
    },
    "ArnLike": {
      "aws:SourceArn": [
        "arn:aws:fsx:us-west-2:123456789012:file-system/*",
        "arn:aws:fsx:us-west-2:123456789012:storage-virtual-machine/fs-*/
svm-*"
      ]
    }
  }
}
```

14. Pilih Selesai.

Note

Anda dapat mengatur kontrol akses yang lebih terperinci dengan memodifikasi Resource dan `aws:SourceArn` bidang untuk menargetkan rahasia dan sistem file tertentu.

Langkah 2: Buat AWS Secrets Manager rahasia

Untuk membuat rahasia

1. Buka konsol Secrets Manager di <https://console.aws.amazon.com/secretsmanager/>.
2. Pilih Simpan rahasia baru.
3. Untuk Tipe rahasia, pilih Tipe rahasia lainnya.
4. Untuk pasangan kunci/nilai, lakukan hal berikut untuk menambahkan dua kunci Anda:
 - a. Untuk kunci pertama, masukkan CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME.
 - b. Untuk nilai kunci pertama, masukkan hanya nama pengguna (tanpa awalan domain) dari pengguna AD.
 - c. Untuk kunci kedua, masukkan CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD.
 - d. Untuk nilai kunci kedua, masukkan kata sandi yang Anda buat untuk pengguna AD di domain Anda.
5. Untuk kunci Enkripsi, masukkan ARN dari kunci KMS yang Anda buat pada langkah sebelumnya dan pilih Berikutnya.
6. Untuk Nama rahasia, masukkan nama deskriptif yang akan membantu Anda menemukan rahasia Anda nanti.
7. (Opsional) Untuk Deskripsi, masukkan deskripsi untuk nama rahasia.
8. Untuk izin Sumber Daya, pilih Edit.

Tambahkan kebijakan berikut ke kebijakan izin untuk mengizinkan Amazon FSx menggunakan rahasia, lalu pilih Berikutnya. Pastikan untuk mengganti *us-west-2* ke Wilayah AWS tempat sistem file digunakan dan *123456789012* ke Akun AWS ID Anda.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "fsx.amazonaws.com"
      },
      "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
      ],
    }
  ]
}
```

```

    "Resource": "arn:aws:secretsmanager:us-west-2:123456789012:secret:*",
    "Condition": {
      "StringEquals": {
        "aws:SourceAccount": "123456789012"
      },
      "ArnLike": {
        "aws:SourceArn": [
          "arn:aws:fsx:us-west-2:123456789012:file-system/*",
          "arn:aws:fsx:us-west-2:123456789012:storage-virtual-
machine/fs-*/svm-*"
        ]
      }
    }
  }
]
}

```

9. (Opsional) Anda dapat mengonfigurasi Secrets Manager untuk memutar kredensial Anda secara otomatis. Pilih Berikutnya.
10. Pilih Selesai.

Simpan kredensial Direktori Aktif di (AWS Secrets Manager CLI)

Langkah 1: Buat kunci KMS

Buat kunci KMS untuk mengenkripsi dan mendekripsi kredensial Active Directory Anda di Secrets Manager.

Untuk membuat kunci KMS, gunakan AWS CLI perintah [create-key](#).

Dalam perintah ini, atur `--policy` parameter untuk menentukan kebijakan kunci yang mendefinisikan izin untuk kunci KMS. Kebijakan tersebut harus mencakup yang berikut:

- Prinsip layanan untuk Amazon FSx, yaitu `fsx.amazonaws.com`.
- Tindakan KMS yang diperlukan: `kms:Decrypt` dan `kms:DescribeKey`.
- Pola ARN sumber daya untuk Anda Wilayah AWS dan akun.
- Kunci kondisi yang membatasi penggunaan kunci:
 - `kms:ViaService` untuk memastikan permintaan datang melalui Secrets Manager.
 - `aws:SourceAccount` untuk membatasi ke akun Anda.
 - `aws:SourceArn` untuk membatasi sistem FSx file Amazon tertentu.

Contoh berikut membuat kunci KMS enkripsi simetris dengan kebijakan yang memungkinkan Amazon menggunakan kunci FSx untuk operasi dekripsi dan deskripsi kunci. Perintah secara otomatis mengambil Akun AWS ID dan Region Anda, lalu mengonfigurasi kebijakan kunci dengan nilai-nilai ini untuk memastikan kontrol akses yang tepat antara Amazon FSx, Secrets Manager, dan kunci KMS. Pastikan AWS CLI lingkungan Anda berada di wilayah yang sama dengan SVM yang akan bergabung dengan Active Directory.

```
# Set region and get Account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Create Key
KMS_KEY_ARN=$(aws kms create-key --policy "{
  \"Version\": \"2012-10-17\",
  \"Statement\": [
    {
      \"Sid\": \"Enable IAM User Permissions\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"AWS\": \"arn:aws:iam::$ACCOUNT_ID:root\"
      },
      \"Action\": \"kms:*\",
      \"Resource\": \"*\"
    },
    {
      \"Sid\": \"Allow FSx to use the KMS key\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"Service\": \"fsx.amazonaws.com\"
      },
      \"Action\": [
        \"kms:Decrypt\",
        \"kms:DescribeKey\"
      ],
      \"Resource\": \"*\",
      \"Condition\": {
        \"StringEquals\": {
          \"kms:ViaService\": \"secretsmanager.$REGION.amazonaws.com\",
          \"aws:SourceAccount\": \"$ACCOUNT_ID\"
        },
        \"ArnLike\": {
          \"aws:SourceArn\": [
            \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\",
```



```

        \\"arn:aws:fsx:$REGION:$ACCOUNT_ID:storage-virtual-machine/fs-*/svm-*\"}]
    }
  }
}
]" --query 'KeyMetadata.Arn' --output text)

echo "KMS Key ARN: $KMS_KEY_ARN"

```

Note

Anda dapat mengatur kontrol akses yang lebih terperinci dengan memodifikasi Resource dan `aws:SourceArn` bidang untuk menargetkan rahasia dan sistem file tertentu.

Langkah 2: Buat AWS Secrets Manager rahasia

Untuk membuat rahasia bagi Amazon FSx untuk mengakses Active Directory Anda, gunakan AWS CLI perintah [create-secret](#) dan atur parameter berikut:

- `--name`: Pengidentifikasi rahasia Anda.
- `--description`: Deskripsi tujuan rahasia.
- `--kms-key-id`: ARN dari kunci KMS yang Anda buat di [Langkah 1](#) untuk mengenkripsi rahasia saat istirahat.
- `--secret-string`: String JSON yang berisi kredensi AD Anda dalam format berikut:
 - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`: Nama pengguna akun layanan AD Anda tanpa awalan domain, seperti `svc-fsx`. Jangan berikan awalan domain, seperti `CORP\svc-fsx`.
 - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`: Kata sandi akun layanan AD Anda
- `--region`: Wilayah AWS Tempat SVM Anda akan dibuat. Ini default ke wilayah yang dikonfigurasi jika tidak `AWS_REGION` disetel.

Setelah membuat rahasia, lampirkan kebijakan sumber daya menggunakan [put-resource-policy](#) perintah, dan atur parameter berikut:

- `--secret-id`: Nama atau ARN rahasia untuk melampirkan kebijakan. Contoh berikut menggunakan **FSxSecret** sebagai `--secret-id`.

- `--region`: Sama Wilayah AWS seperti rahasiamu.
- `--resource-policy`: Dokumen kebijakan JSON yang memberikan FSx izin Amazon untuk mengakses rahasia. Kebijakan tersebut harus mencakup yang berikut:
 - Prinsip layanan untuk Amazon FSx, yaitu **`fsx.amazonaws.com`**.
 - Tindakan Secrets Manager yang diperlukan: `secretsmanager:GetSecretValue` dan `secretsmanager:DescribeSecret`.
 - Pola ARN sumber daya untuk Anda Wilayah AWS dan akun.
 - Kunci kondisi berikut yang membatasi akses:
 - `aws:SourceAccount` untuk membatasi ke akun Anda.
 - `aws:SourceArn` untuk membatasi sistem FSx file Amazon tertentu.

Contoh berikut membuat rahasia dengan format yang diperlukan dan melampirkan kebijakan sumber daya yang FSx memungkinkan Amazon menggunakan rahasia tersebut. Contoh ini secara otomatis mengambil Akun AWS ID dan Wilayah Anda, lalu mengonfigurasi kebijakan sumber daya dengan nilai-nilai ini untuk memastikan kontrol akses yang tepat antara Amazon FSx dan rahasia.

Pastikan untuk mengganti `KMS_KEY_ARN` dengan ARN dari kunci yang Anda buat di [Langkah 1](#) `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`, dan `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD` dengan kredensial akun layanan Active Directory Anda. Selain itu, verifikasi bahwa AWS CLI lingkungan Anda dikonfigurasi untuk wilayah yang sama dengan SVM yang akan bergabung dengan Active Directory.

```
# Set region and get account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Replace with your KMS key ARN from Step 1
KMS_KEY_ARN="arn:aws:kms:us-east-2:123456789012:key/1234542f-d114-555b-9ade-
fec3c9200d8e"

# Replace with your Active Directory credentials
AD_USERNAME="Your_Username"
AD_PASSWORD="Your_Password"

# Create the secret
SECRET_ARN=$(aws secretsmanager create-secret \
  --name "FSxSecret" \
  --description "Secret for FSx access" \
```

```

--kms-key-id "$KMS_KEY_ARN" \
--secret-string "{\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME\":\"$AD_USERNAME\",
\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD\":\"$AD_PASSWORD\"}" \
--region "$REGION" \
--query 'ARN' \
--output text)

echo "Secret created with ARN: $SECRET_ARN"

# Attach the resource policy with proper formatting
aws secretsmanager put-resource-policy \
--secret-id "FSxSecret" \
--region "$REGION" \
--resource-policy "{
  \"Version\": \"2012-10-17\",
  \"Statement\": [
    {
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"Service\": \"fsx.amazonaws.com\"
      },
      \"Action\": [
        \"secretsmanager:GetSecretValue\",
        \"secretsmanager:DescribeSecret\"
      ],
      \"Resource\": \"$SECRET_ARN\",
      \"Condition\": {
        \"StringEquals\": {
          \"aws:SourceAccount\": \"$ACCOUNT_ID\"
        },
        \"ArnLike\": {
          \"aws:SourceArn\": [
            \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\",
            \"arn:aws:fsx:$REGION:$ACCOUNT_ID:storage-virtual-machine/fs-*/svm-*\"
          ]
        }
      }
    }
  ]
}"

echo "Resource policy attached successfully"

```

 Note

Anda dapat mengatur kontrol akses yang lebih terperinci dengan memodifikasi Resource dan `aws:SourceArn` bidang untuk menargetkan rahasia dan sistem file tertentu.

Cara kerja bergabung SVMs ke Microsoft Active Directory

Organisasi Anda mungkin mengelola identitas dan perangkat menggunakan Active Directory, baik lokal maupun di cloud. Dengan FSx untuk ONTAP, Anda dapat bergabung SVMs langsung ke domain Active Directory yang ada dengan cara berikut:

- Bergabung baru SVMs ke Active Directory saat pembuatan:
 - Menggunakan opsi Buat Standar di FSx konsol Amazon untuk membuat sistem file ONTAP baru FSx, Anda dapat menggabungkan SVM default ke Direktori Aktif yang dikelola sendiri. Untuk informasi selengkapnya, lihat [Untuk membuat sistem file \(konsol\)](#).
 - Menggunakan FSx konsol Amazon, AWS CLI, atau Amazon FSx API untuk membuat SVM baru pada sistem file ONTAP FSx yang sudah ada. Untuk informasi selengkapnya, lihat [Membuat mesin virtual penyimpanan \(SVM\)](#).
- Bergabung SVMs dengan Active Directory:
 - Menggunakan Konsol Manajemen AWS, AWS CLI, dan API untuk menggabungkan SVM ke Direktori Aktif, dan mencoba kembali menggabungkan SVM ke Direktori Aktif jika upaya awal untuk bergabung gagal. Anda juga dapat memperbarui beberapa properti konfigurasi Active Directory untuk SVMs yang sudah bergabung ke Active Directory. Untuk informasi selengkapnya, lihat [Mengelola konfigurasi SVM Active Directory](#).
 - Menggunakan NetApp ONTAP CLI atau REST API untuk bergabung, mencoba kembali bergabung, dan memutuskan konfigurasi SVM Active Directory. Untuk informasi selengkapnya, lihat [Memperbarui konfigurasi SVM Active Directory menggunakan CLI NetApp](#).

 Important

- Amazon FSx hanya mendaftarkan catatan DNS untuk SVM jika Anda menggunakan Microsoft DNS sebagai layanan DNS default. Jika Anda menggunakan DNS pihak ketiga, Anda harus mengatur entri DNS secara manual untuk Amazon FSx SVMs setelah Anda membuatnya.

- Jika Anda menggunakan AWS Managed Microsoft AD, Anda harus menentukan grup seperti Administrator AWS Delegasi, FSx Administrator AWS Delegasi, atau grup kustom dengan izin yang didelegasikan ke OU.

Saat Anda bergabung FSx untuk ONTAP SVM langsung ke Direktori Aktif yang dikelola sendiri, SVM berada di hutan Direktori Aktif yang sama (wadah paling logis teratas dalam konfigurasi Direktori Aktif yang berisi domain, pengguna, dan komputer) dan dalam domain Direktori Aktif yang sama dengan pengguna dan sumber daya yang ada, termasuk server file yang ada.

Informasi yang dibutuhkan saat bergabung dengan SVM ke Active Directory

Anda harus memberikan informasi berikut tentang Active Directory saat menggabungkan SVM ke Active Directory, terlepas dari operasi API yang Anda pilih:

- Nama NetBIOS dari objek komputer Active Directory yang akan dibuat untuk SVM Anda. Ini adalah nama SVM di Active Directory, yang harus unik dalam Active Directory Anda. Jangan gunakan nama NetBIOS dari domain rumah. Nama NetBIOS tidak boleh melebihi 15 karakter.
- Nama domain yang sepenuhnya memenuhi syarat (FQDN) dari Direktori Aktif Anda. FQDN tidak dapat melebihi 255 karakter.

Note

FQDN tidak dapat dalam format Single Label Domain (SLD). Amazon FSx tidak mendukung domain SLD.

- Hingga tiga alamat IP server DNS atau host domain untuk domain Anda.

Alamat IP server DNS dan alamat IP pengontrol domain Direktori Aktif dapat berada dalam rentang alamat IP apa pun, kecuali:

- Alamat IP yang bertentangan dengan alamat IP milik Amazon Web Services di dalamnya. Wilayah AWS Untuk daftar alamat AWS IP menurut Wilayah, lihat [rentang alamat AWS IP](#).
- Alamat IP dalam rentang blok CIDR berikut: 198.19.0.0/16
- Kredensi untuk akun layanan Direktori Aktif yang FSx digunakan Amazon untuk bergabung dengan SVM ke domain Anda. Anda dapat memberikan ini sebagai:

- Opsi 1: AWS Secrets Manager rahasia ARN - Rahasia yang berisi nama pengguna dan kata sandi untuk akun layanan di domain Direktori Aktif Anda. Untuk informasi selengkapnya, lihat [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).
- Opsi 2: Kredensi Plaintext
 - Nama pengguna akun layanan — Nama pengguna akun layanan di Microsoft Active Directory yang ada. Jangan sertakan awalan atau akhiran domain. Misalnya, untuk `EXAMPLE\ADMIN`, gunakan saja `ADMIN`.
 - Kata sandi akun layanan — Kata sandi untuk akun layanan.
- (Opsional) Unit Organisasi (OU) di domain tempat Anda bergabung dengan SVM.

Note

Jika Anda menggabungkan SVM Anda ke AWS Directory Service Active Directory, Anda harus memberikan OU yang berada dalam OU default yang Directory Service membuat objek direktori yang terkait AWS dengan. Ini karena Directory Service tidak menyediakan akses ke `Computers` OU default Active Directory Anda. Misalnya, jika domain Active Directory Anda `example.com`, Anda dapat menentukan OU berikut: `OU=Computers,OU=example,DC=example,DC=com`.

- (Opsional) Grup domain tempat Anda mendelegasikan wewenang untuk melakukan tindakan administratif pada sistem file Anda. Misalnya, grup domain ini mungkin mengelola berbagi file SMB Windows, 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.

Mengelola konfigurasi SVM Active Directory

Bagian ini menjelaskan cara menggunakan,, FSx API Konsol Manajemen AWS AWS CLI, dan CLI ONTAP untuk melakukan hal berikut:

- Bergabung dengan SVM yang ada ke Active Directory
- Memodifikasi konfigurasi SVM Active Directory yang ada
- Menghapus SVMs dari Direktori Aktif

Untuk menghapus SVM dari Active Directory, Anda harus menggunakan NetApp ONTAP CLI.

Topik

- [Bergabung SVMs ke Active Directory menggunakan Konsol Manajemen AWS, AWS CLI dan API](#)
- [Memperbarui konfigurasi SVM Active Directory yang ada menggunakan Konsol Manajemen AWS, AWS CLI, dan API](#)
- [Memperbarui konfigurasi SVM Active Directory menggunakan CLI NetApp](#)

Bergabung SVMs ke Active Directory menggunakan Konsol Manajemen AWS, AWS CLI dan API

Gunakan prosedur berikut untuk menggabungkan SVM yang ada ke Active Directory. Dalam prosedur ini, SVM belum bergabung dengan Active Directory.

Untuk bergabung dengan SVM ke Active Directory ()Konsol Manajemen AWS

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Pilih SVM yang ingin Anda gabungkan ke Active Directory:
 - Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file ONTAP dengan SVM yang ingin Anda perbarui.
 - Pilih tab Storage virtual machines.

—Atau—

 - Untuk menampilkan daftar semua yang tersedia SVMs, di panel navigasi kiri, perluas ONTAP dan pilih mesin virtual Penyimpanan. Daftar semua SVMs di akun Anda di Wilayah AWS ditampilkan.

Pilih SVM yang ingin Anda gabungkan ke Active Directory dari daftar.
3. Di kanan atas panel Ringkasan SVM, pilih Tindakan > Gabung/Perbarui Direktori Aktif. Jendela Join SVM ke Active Directory muncul.
4. Masukkan informasi berikut untuk Active Directory tempat Anda bergabung dengan SVM:
 - Nama NetBIOS dari objek komputer Active Directory yang akan dibuat untuk SVM Anda. Ini adalah nama SVM di Active Directory, yang harus unik dalam Active Directory Anda. Jangan gunakan nama NetBIOS dari domain rumah. Nama NetBIOS tidak boleh melebihi 15 karakter.

- Nama domain yang sepenuhnya memenuhi syarat (FQDN) dari Direktori Aktif Anda. Nama domain tidak boleh melebihi 255 karakter.
- Alamat IP server DNS — Alamat IPv4 atau IPv6 alamat server DNS untuk domain Anda.
- Kredensi akun layanan - Pilih cara memberikan kredensi akun layanan Anda:
 - Opsi 1: AWS Secrets Manager rahasia ARN - Rahasia yang berisi nama pengguna dan kata sandi untuk akun layanan di domain Direktori Aktif Anda. Untuk informasi selengkapnya, lihat [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).
 - Opsi 2: Kredensi Plaintext
 - Nama pengguna akun layanan — Nama pengguna akun layanan di Microsoft Active Directory yang ada. Jangan sertakan awalan atau akhiran domain. Misalnya, untuk `EXAMPLE\ADMIN`, gunakan saja `ADMIN`.
 - Kata sandi akun layanan — Kata sandi untuk akun layanan.
 - Konfirmasi kata sandi — Kata sandi untuk akun layanan.
 - Dikelola di Secrets Manager (default) - Berikan ARN rahasia Secrets Manager yang berisi kredensial akun layanan Anda. Rahasiannya harus berisi pasangan `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME` kunci-nilai dan `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`.
 - (Opsional) Unit Organisasi (OU) - Nama jalur terhormat dari unit organisasi tempat Anda ingin bergabung dengan SVM Anda.
 - Grup administrator sistem file yang didelegasikan — Nama grup di Direktori Aktif Anda yang dapat mengelola sistem file Anda.

Jika Anda menggunakan AWS Managed Microsoft AD, Anda harus menentukan grup seperti Administrator AWS Delegasi, FSx Administrator AWS Delegasi, atau grup kustom dengan izin yang didelegasikan ke OU.

Jika Anda bergabung ke Active Directory yang dikelola sendiri, gunakan nama grup di Active Directory Anda. Grup default adalah `Domain Admins`.

5. Pilih Gabung Active Directory untuk bergabung dengan SVM ke Active Directory menggunakan konfigurasi yang Anda berikan.

Untuk bergabung dengan SVM ke Active Directory (AWS CLI)

- Untuk menggabungkan SVM ONTAP ke Active Directory, gunakan perintah [update-storage-virtual-machine](#) CLI (atau operasi [UpdateStorageVirtualMachine](#) API yang setara), seperti yang ditunjukkan pada contoh berikut. FSx

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
  SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
  \
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Setelah berhasil membuat mesin virtual penyimpanan, Amazon FSx mengembalikan deskripsinya dalam format JSON, seperti yang ditunjukkan pada contoh berikut.

```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  },
  "CreationTime": 1625066825.306,
  "Endpoints": {
    "Management": {
      "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
      "IpAddresses": ["198.19.0.4"]
    },
    "Nfs": {
```

```

    "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
    "IpAddresses": ["198.19.0.4"],
  },
  "Smb": {
    "DnsName": "amznfsx12345",
    "IpAddresses": ["198.19.0.4"],
  },
  "SmbWindowsInterVpc": {
    "IpAddresses": ["198.19.0.5", "198.19.0.6"],
  },
  "Iscsi": {
    "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com",
    "IpAddresses": ["198.19.0.7", "198.19.0.8"],
  },
  },
  "FileSystemId": "fs-0123456789abcdef0",
  "Lifecycle": "CREATED",
  "Name": "vol1",
  "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/fs-0123456789abcdef0/svm-abcdef0123456789a",
  "StorageVirtualMachineId": "svm-abcdef0123456789a",
  "Subtype": "default",
  "Tags": [],
}
}

```

Memperbarui konfigurasi SVM Active Directory yang ada menggunakan Konsol Manajemen AWS, AWS CLI, dan API

Gunakan prosedur berikut untuk memperbarui konfigurasi Active Directory dari SVM yang sudah bergabung ke Active Directory.

Untuk memperbarui konfigurasi SVM Active Directory ()Konsol Manajemen AWS

1. Buka FSx konsol Amazon di <https://console.aws.amazon.com/fsx/>.
2. Pilih SVM yang akan diperbarui sebagai berikut:

- Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file ONTAP dengan SVM yang ingin Anda perbarui.
- Pilih tab Storage virtual machines.

—Atau—

- Untuk menampilkan daftar semua yang SVMs tersedia, di panel navigasi kiri, perluas ONTAP dan pilih mesin virtual Penyimpanan.

Pilih SVM yang ingin Anda perbarui dari daftar.

3. Pada panel Ringkasan SVM, pilih Tindakan > Gabung/Perbarui Direktori Aktif. Jendela konfigurasi Update SVM Active Directory muncul.
4. Anda dapat memperbarui properti konfigurasi Active Directory berikut di jendela ini.
 - Alamat IP server DNS — Alamat IPv4 atau IPv6 alamat server DNS untuk domain Anda.
 - Kredensi akun layanan - Pilih cara memberikan kredensi akun layanan Anda:
 - Opsi 1: AWS Secrets Manager rahasia ARN - Rahasia yang berisi nama pengguna dan kata sandi untuk akun layanan di domain Direktori Aktif Anda. Untuk informasi selengkapnya, lihat [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).
 - Opsi 2: Kredensi Plaintext
 - Nama pengguna akun layanan — Nama pengguna akun layanan di Microsoft Active Directory yang ada. Jangan sertakan awalan atau akhiran domain. Misalnya, untukEXAMPLE\ADMIN, gunakan sajaADMIN.
 - Kata sandi akun layanan — Kata sandi untuk akun layanan.
 - Konfirmasi kata sandi — Kata sandi untuk akun layanan.
5. Setelah Anda memasukkan pembaruan, pilih Perbarui Direktori Aktif untuk membuat perubahan.

Gunakan prosedur berikut untuk memperbarui konfigurasi Active Directory dari SVM yang sudah bergabung ke Active Directory.

Untuk memperbarui konfigurasi SVM Active Directory (AWS CLI)

- Untuk memperbarui konfigurasi Direktori Aktif SVM dengan AWS CLI atau API, gunakan perintah [update-storage-virtual-machine](#)CLI (atau operasi API yang [UpdateStorageVirtualMachines](#)setara), seperti yang ditunjukkan pada contoh berikut.

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration \
  SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
  Password="password", \
  DnsIps=["10.0.1.18"]}'
```

Memperbarui konfigurasi SVM Active Directory menggunakan CLI NetApp

Anda dapat menggunakan CLI NetApp ONTAP untuk bergabung dan memutuskan sambungan SVM Anda ke Active Directory, dan untuk memodifikasi konfigurasi SVM Active Directory yang ada.

Bergabung dengan SVM ke Active Directory menggunakan ONTAP CLI

Anda dapat bergabung yang ada SVMs ke Direktori Aktif menggunakan CLI ONTAP, seperti yang dijelaskan dalam prosedur berikut. Anda dapat melakukan ini bahkan jika SVM Anda sudah bergabung ke Active Directory.

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Buat entri DNS untuk Active Directory Anda dengan memberikan nama DNS direktori lengkap (corp.example.com) dan setidaknya satu alamat IP server DNS.

```
::>vserver services name-service dns create -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1, dns_ip_2
```

Untuk memverifikasi koneksi ke server DNS Anda, jalankan perintah berikut. Ganti *svm_name* dengan informasi Anda sendiri.

```
FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name
```

Vserver	Name Server	Name Server	Status	Status Details

```
-----
svm_name      172.31.14.245  up           Response time (msec): 0
svm_name      172.31.25.207  up           Response time (msec): 1
2 entries were displayed.
```

- Untuk menggabungkan SVM Anda ke Active Directory, jalankan perintah berikut. Perhatikan bahwa Anda harus menentukan `computer_name` yang belum ada di Active Directory Anda dan memberikan nama DNS direktori untuk-domain. Untuk-OU, masukkan OUs yang Anda inginkan untuk bergabung dengan SVM, serta nama DNS lengkap dalam format DC.

```
::>vserver cifs create -vserver svm_name -cifs-server computer_name -
domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
```

Untuk memverifikasi status koneksi Active Directory Anda, jalankan perintah berikut:

```
::>vserver cifs check -vserver svm_name

Vserver : svm_name
Cifs NetBIOS Name : svm_netBIOS_name
Cifs Status : Running
Site : Default-First-Site-Name
Node Name      DC Server Name  DC Server IP   Status   Status Details
-----
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245  up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245  up       Response time (msec): 20
2 entries were displayed.
```

- Jika Anda tidak dapat mengakses berbagi setelah bergabung, tentukan apakah akun yang Anda gunakan untuk mengakses berbagi memiliki izin. Misalnya, jika Anda menggunakan Admin akun default (administrator yang didelegasikan) dengan Direktori Aktif AWS terkelola, Anda harus menjalankan perintah berikut di ONTAP. `netbios_domain` Sesuai dengan nama domain Active Directory Anda (untuk `corp.example.com`, yang `netbios_domain` digunakan di sini adalah `example`).

```
FsxId0123456789a:>vserver cifs users-and-groups local-group add-members -vserver
svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

Ubah konfigurasi Active Directory menggunakan ONTAP CLI

Anda dapat menggunakan CLI ONTAP untuk memodifikasi konfigurasi Active Directory yang ada.

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Jalankan perintah berikut untuk menurunkan server CIFS SVM sementara:

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Jika Anda perlu memodifikasi entri DNS Active Directory Anda, jalankan perintah berikut:

```
::>vserver services name-service dns modify -vserver svm_name -  
domains corp.example.com -name-servers dns_ip_1,dns_ip_2
```

Anda dapat memvalidasi status koneksi ke server DNS Active Directory menggunakan perintah.

```
vserver services name-service dns check -vserver svm_name
```

```
::>vserver services name-service dns check -vserver svm_name
```

Vserver	Name Server	Status	Status Details
svmciaad	dns_ip_1	up	Response time (msec): 1
svmciaad	dns_ip_2	up	Response time (msec): 1

2 entries were displayed.

4. Jika Anda perlu memodifikasi konfigurasi Active Directory itu sendiri, Anda dapat mengubah bidang yang ada dengan menggunakan perintah berikut, menggantikan:
 - *computer_name*, jika Anda ingin memodifikasi nama NetBIOS (akun mesin) SVM.
 - *domain_name*, jika Anda ingin mengubah nama domain. Ini harus sesuai dengan entri domain DNS yang dicatat dalam Langkah 3 bagian ini (*corp.example.com*).
 - *organizational_unit*, jika Anda ingin memodifikasi OU (OU=Computers, OU=example, DC=corp, DC=example, DC=com).

Anda harus memasukkan kembali kredensi Active Directory yang Anda gunakan untuk bergabung dengan perangkat ini ke Active Directory.

```
::>vserver cifs modify -vserver svm_name -cifs-server computer_name -  
domain domain_name -OU organizational_unit
```

Anda dapat memverifikasi status koneksi koneksi Direktori Aktif Anda menggunakan `vserver cifs check -vserver svm_name` perintah.

5. Ketika Anda selesai memodifikasi Active Directory dan konfigurasi DNS Anda, bawalah server CIFS kembali dengan menjalankan perintah berikut:

```
::>vserver cifs modify -vserver svm_name -status-admin up
```

Berhenti bergabung dengan Active Directory dari SVM Anda menggunakan ONTAP NetApp CLI

CLI NetApp ONTAP juga dapat digunakan untuk memutuskan sambungan SVM Anda dari Active Directory dengan mengikuti langkah-langkah di bawah ini:

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Hapus server CIFS yang melepaskan perangkat Anda dari Active Directory dengan menjalankan perintah berikut. Agar ONTAP menghapus akun mesin untuk SVM Anda, berikan kredensial yang awalnya Anda gunakan untuk bergabung dengan SVM ke Direktori Aktif.

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Jika Anda perlu memodifikasi entri DNS Active Directory Anda, jalankan perintah berikut:

```
FsxId0123456789a::vserver cifs delete -vserver svm_name
```

In order to delete an Active Directory machine account for the CIFS server, you must supply the name and password of a Windows account with sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

Enter the user name: *user_name*

Enter the password:

Warning: There are one or more shares associated with this CIFS server
Do you really want to delete this CIFS server and all its shares? {y|n}: *y*

4. Hapus server DNS untuk Active Directory Anda dengan menjalankan perintah berikut:

```
::vserver services name-service dns delete -vserver svm_name
```

Jika Anda melihat peringatan seperti berikut—menunjukkan bahwa dns harus dihapus sebagai ns-switch —dan Anda tidak berencana untuk bergabung kembali dengan perangkat ini ke Direktori Aktif, Anda dapat menghapus entri. ns-switch

Warning: "DNS" is present as one of the sources in one or more ns-switch databases but no valid DNS configuration was found for Vserver
"svm_name". Remove "DNS" from ns-switch using the "vserver services name-service ns-switch" command. Configuring "DNS" as a source
in the ns-switch setting when there is no valid configuration can cause protocol access issues.

5. (Opsional) Hapus ns-switch entri dns dengan menjalankan perintah berikut. Verifikasi urutan sumber, lalu hapus dns entri untuk hosts database dengan memodifikasi sources sehingga hanya berisi sumber lain yang terdaftar. Dalam contoh ini, satu-satunya sumber lainnya adalah files.

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts
```

```

                Vserver: svm_name
Name Service Switch Database: hosts
    Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts  
-sources files
```


6. (Opsional) Hapus dns entri dengan memodifikasi host database untuk disertakan saja `files.sources`

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts  
-sources files
```

Bermigrasi ke Amazon FSx untuk NetApp ONTAP

Bagian berikut memberikan informasi tentang cara memigrasi sistem file NetApp ONTAP yang ada ke Amazon FSx untuk NetApp ONTAP.

Note

Jika Anda berencana menggunakan kebijakan All tiering untuk memigrasikan data Anda ke tingkat kumpulan kapasitas, ingatlah bahwa metadata file selalu disimpan di tingkat SSD, dan semua data pengguna baru pertama kali ditulis ke tingkat SSD. Ketika data ditulis ke tingkat SSD, proses tiering latar belakang akan mulai meningkatkan data Anda ke penyimpanan kumpulan kapasitas, tetapi proses tiering tidak langsung dan menghabiskan sumber daya jaringan. Anda perlu mengukur tingkat SSD Anda untuk memperhitungkan metadata file (3-7% dari ukuran data pengguna), sebagai buffer untuk data pengguna sebelum berjenjang ke penyimpanan kolam kapasitas. Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan tingkat SSD Anda.

Saat memigrasikan data, pastikan untuk memantau tingkat SSD Anda menggunakan [metrik sistem CloudWatch File](#) untuk memastikan bahwa itu tidak mengisi lebih cepat daripada proses tiering dapat memindahkan data ke penyimpanan kumpulan kapasitas.

Topik

- [Migrasi ke FSx untuk ONTAP menggunakan NetApp SnapMirror](#)
- [Migrasi ke FSx untuk ONTAP menggunakan AWS DataSync](#)

Migrasi ke FSx untuk ONTAP menggunakan NetApp SnapMirror

Anda dapat memigrasi sistem file NetApp ONTAP Anda ke Amazon FSx untuk NetApp ONTAP menggunakan NetApp SnapMirror.

NetApp SnapMirror menggunakan replikasi tingkat blok antara dua sistem file ONTAP, mereplikasi data dari volume sumber tertentu ke volume tujuan. Sebaiknya gunakan SnapMirror untuk memigrasikan sistem file ONTAP on-premise ke NetApp ONTAP. FSx NetApp SnapMirror replikasi tingkat blok cepat dan efisien bahkan untuk sistem file dengan:

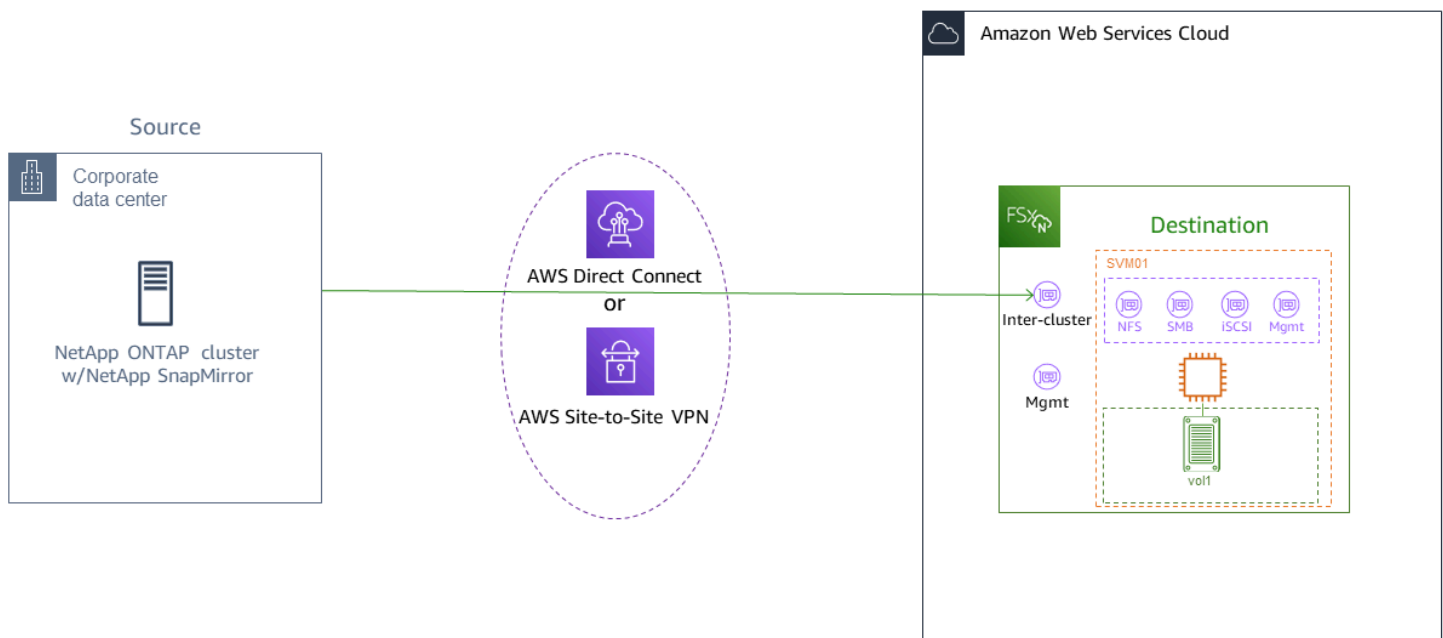
- Struktur direktori yang kompleks

- Lebih dari 50 juta file
- Ukuran file yang sangat kecil (sesuai urutan kilobyte)

Saat Anda menggunakan migrasi SnapMirror ke FSx ONTAP, data yang tidak digandakan dan dikompresi tetap berada di status tersebut, yang mengurangi waktu transfer dan mengurangi jumlah bandwidth yang diperlukan untuk migrasi. Snapshot yang ada pada volume ONTAP sumber dipertahankan saat dimigrasikan ke volume tujuan. Memigrasi sistem file NetApp ONTAP lokal Anda ke FSx ONTAP melibatkan tugas tingkat tinggi berikut:

1. Buat volume tujuan di Amazon FSx.
2. Kumpulkan antarmuka logis sumber dan tujuan (LIFs).
3. Membangun cluster peering antara sumber dan sistem file tujuan.
4. Buat hubungan peering SVM.
5. Ciptakan SnapMirror hubungan.
6. Pertahankan klaster tujuan yang diperbarui.
7. Potong ke sistem file ONTAP Anda FSx .

Diagram berikut menggambarkan skenario migrasi yang dijelaskan di bagian ini.



Topik

- [Sebelum Anda mulai](#)

- [Buat volume tujuan](#)
- [Rekam sumber dan tujuan antar cluster LIFs](#)
- [Membangun cluster peering antara sumber dan tujuan](#)
- [Buat hubungan peering SVM](#)
- [Ciptakan SnapMirror hubungan](#)
- [Transfer data ke sistem file ONTAP Anda FSx](#)
- [Memotong ke Amazon FSx](#)

Sebelum Anda mulai

Sebelum Anda mulai menggunakan prosedur yang dijelaskan di bagian berikut, pastikan Anda telah memenuhi prasyarat berikut:

- FSx untuk ONTAP memprioritaskan lalu lintas klien daripada tugas latar belakang termasuk tiering data, efisiensi penyimpanan, dan pencadangan. Saat memigrasikan data, dan sebagai praktik terbaik secara umum, kami menyarankan Anda memantau kapasitas tingkat SSD Anda untuk memastikan pemanfaatannya tidak melebihi 80%. Anda dapat memantau pemanfaatan tingkat SSD Anda menggunakan [metrik sistem CloudWatch File](#). Untuk informasi selengkapnya, lihat [Metrik volume](#).
- Jika Anda menyetel kebijakan tingkatan data volume tujuan All saat memigrasikan data, semua metadata file disimpan di tingkat penyimpanan SSD utama. Metadata file selalu disimpan di tingkat primer berbasis SSD, terlepas dari kebijakan tingkatan data volume. Kami menyarankan Anda mengasumsikan rasio 1:10 untuk tingkat primer: kapasitas kapasitas kapasitas kapasitas kapasitas penyimpanan tingkat.
- Sistem file sumber dan tujuan terhubung dalam VPC yang sama, atau berada di jaringan yang diintegrasikan menggunakan Amazon VPC Peering, Transit Gateway, atau AWS Direct Connect Site-to-Site VPN. Untuk informasi lebih lanjut, lihat [Mengakses data dari dalam AWS Cloud](#) dan [Apa itu VPC peering?](#) di Panduan Peering VPC Amazon.
- Grup keamanan VPC untuk sistem file ONTAP memiliki aturan masuk dan keluar yang memungkinkan ICMP serta TCP pada port 443, 10000, 11104, dan 11105 untuk titik akhir antar-cluster Anda (). FSx LIFs
- Verifikasi bahwa volume sumber dan tujuan menjalankan versi NetApp ONTAP yang kompatibel sebelum membuat hubungan perlindungan SnapMirror data. Untuk informasi selengkapnya, lihat [Versi ONTAP yang kompatibel untuk SnapMirror hubungan](#) dalam dokumentasi NetApp pengguna

ONTAP. Prosedur yang disajikan di sini menggunakan sistem file NetApp ONTAP on-premise untuk sumbernya.

- Sistem file NetApp ONTAP lokal (sumber) Anda menyertakan lisensi. SnapMirror
- Anda telah membuat tujuan FSx untuk sistem file ONTAP dengan SVM, tetapi Anda belum membuat volume tujuan. Untuk informasi selengkapnya, lihat [Membuat sistem file](#).

Perintah dalam prosedur ini menggunakan alias klaster, SVM, dan volume berikut:

- *FSx-Dest*— ID cluster tujuan (FSx) (dalam format FSx IDabcdef1234567890A).
- *OnPrem-Source*— ID cluster sumber.
- *DestSVM*— nama SVM tujuan.
- *SourceSVM*— nama sumber SVM.
- Baik nama volume sumber dan tujuan adalah `vol1`.

 Note

Sistem file FSx untuk ONTAP disebut sebagai cluster di semua perintah CLI ONTAP.

Prosedur di bagian ini menggunakan perintah CLI NetApp ONTAP berikut.

- [volume membuat](#) perintah
- perintah [cluster](#)
- perintah [rekan vserver](#)
- [perintah snapmirror](#)

Anda akan menggunakan CLI NetApp ONTAP untuk membuat dan mengelola konfigurasi pada SnapMirror sistem file ONTAP FSx Anda. Untuk informasi selengkapnya, lihat [Menggunakan CLI NetApp ONTAP](#).

Buat volume tujuan

Anda dapat membuat volume tujuan perlindungan data (DP) menggunakan FSx konsol Amazon, FSx API Amazon AWS CLI, dan Amazon, selain NetApp ONTAP CLI dan REST API. Untuk informasi

tentang membuat volume tujuan menggunakan FSx konsol Amazon dan AWS CLI, lihat [Membuat volume](#).

 Note

ONTAP tidak mempertahankan penghematan kompresi pasca-proses yang dicapai pada sumber dalam volume DP tujuan ketika kebijakan tingkatan volume tujuan adalah. All Untuk mempertahankan penghematan kompresi pasca-proses, Anda harus mengatur kebijakan tingkatan volume tujuan Auto dan mengaktifkan sistem file tujuan untuk menerapkan kembali penghematan kompresi pasca-proses inactive-data-compression di tujuan.

Dalam prosedur berikut, Anda akan menggunakan CLI NetApp ONTAP untuk membuat volume tujuan pada sistem file ONTAP FSx Anda. Anda akan memerlukan fsxadmin kata sandi dan alamat IP atau nama DNS dari port manajemen sistem file.

1. Buat sesi SSH dengan sistem file tujuan menggunakan pengguna fsxadmin dan kata sandi yang Anda tetapkan saat Anda membuat sistem file.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Buat volume pada cluster tujuan yang memiliki kapasitas penyimpanan yang setidaknya sama dengan kapasitas penyimpanan volume sumber. Gunakan -type DP untuk menunjuknya sebagai tujuan untuk suatu SnapMirror hubungan.

Jika Anda berencana untuk menggunakan tiering data, kami sarankan Anda -tiering-policy menyetelnya. all Ini memastikan bahwa data Anda segera ditransfer ke penyimpanan kolom kapasitas dan mencegah Anda kehabisan kapasitas pada tingkat SSD Anda. Setelah migrasi, Anda dapat beralih -tiering-policy keauto.

 Note

Metadata file selalu disimpan di tingkat primer berbasis SSD, terlepas dari kebijakan tingkatan data volume.

```
FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -  
type DP -tiering-policy all
```

Rekam sumber dan tujuan antar cluster LIFs

SnapMirror menggunakan inter-cluster logical interface (LIFs), masing-masing dengan alamat IP yang unik, untuk memfasilitasi transfer data antara cluster sumber dan tujuan.

1. FSx Untuk tujuan sistem file ONTAP, Anda dapat mengambil titik akhir Inter-cluster - alamat IP dari FSx konsol Amazon dengan menavigasi ke tab Administrasi di halaman detail sistem file Anda.
2. Untuk cluster NetApp ONTAP sumber, ambil alamat IP LIF antar-cluster menggunakan CLI ONTAP. Jalankan perintah berikut:

```
OnPrem-Source::> network interface show -role intercluster
```

Logical Vserver	Interface	Status	Network Address/Mask
FSx-Dest	inter_1	up/up	10.0.0.36/24
	inter_2	up/up	10.0.1.69/24

Note

Untuk sistem file Single-AZ generasi kedua, ada dua alamat IP antar-cluster untuk setiap pasangan ketersediaan tinggi (HA). Simpan nilai-nilai ini untuk nanti.

Simpan alamat `inter_1` dan `inter_2` IP. Mereka direferensikan dalam FSx-Dest as `dest_inter_1` dan `dest_inter_2` dan untuk OnPrem-Source as `source_inter_1` dan `source_inter_2`.

Membangun cluster peering antara sumber dan tujuan

Menetapkan hubungan peer cluster pada cluster tujuan dengan menyediakan alamat IP antar-cluster. Anda juga perlu membuat frasa sandi yang harus Anda masukkan saat Anda membuat cluster peering di cluster sumber.

1. Siapkan peering pada cluster tujuan menggunakan perintah berikut. Untuk sistem file Single-AZ generasi kedua, Anda harus memberikan setiap alamat IP antar-cluster.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-  
addrs source_inter_1,source_inter_2
```

Enter the passphrase:

Confirm the passphrase:

Notice: Now use the same passphrase in the "cluster peer create" command in the other cluster.

2. Selanjutnya, buat hubungan rekan cluster pada cluster sumber. Anda harus memasukkan frasa sandi yang Anda buat di atas untuk mengautentikasi. Untuk sistem file Single-AZ generasi kedua, Anda harus memberikan setiap alamat IP antar-cluster.

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-  
addrs dest_inter_1,dest_inter_2
```

Enter the passphrase:

Confirm the passphrase:

3. Verifikasi peering berhasil menggunakan perintah berikut pada cluster sumber. Dalam output, Availability harus diatur ke Available.

```
OnPrem-Source::> cluster peer show
```

Peer Cluster Name	Availability	Authentication
-----	-----	-----
FSx-Dest	Available	ok

Buat hubungan peering SVM

Dengan cluster peering didirikan, langkah selanjutnya adalah mengintip. SVMs Buat hubungan peering SVM pada cluster tujuan (FSx-Dest) menggunakan perintah. `vserver peer` Alias tambahan yang digunakan dalam perintah berikut adalah sebagai berikut:

- **DestLocalName**— ini adalah nama yang digunakan untuk mengidentifikasi SVM tujuan saat mengkonfigurasi SVM mengintip pada sumber SVM.
- **SourceLocalName**— ini adalah nama yang digunakan untuk mengidentifikasi sumber SVM saat mengkonfigurasi SVM mengintip pada SVM tujuan.

1. Gunakan perintah berikut untuk membuat hubungan peering SVM antara sumber dan tujuan. SVMs

```
FSx-Dest::> vservers peer create -vservers DestSVM -peer-vservers SourceSVM -peer-cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName
```

```
Info: [Job 207] 'vservers peer create' job queued
```

2. Terima hubungan peering di cluster sumber:

```
OnPrem-Source::> vservers peer accept -vservers SourceSVM -peer-vservers DestSVM -local-name DestLocalName
```

```
Info: [Job 211] 'vservers peer accept' job queued
```

3. Verifikasi status peering SVM menggunakan perintah berikut; Peer State harus diatur ke peered dalam respons.

```
OnPrem-Source::> vservers peer show
```

	Peer	Peer	Peer	Peering	Remote
Vserver	Vserver	State	Cluster	Applications	Vserver
-----	-----	-----	-----	-----	-----
svm01	destsvm1	peered	FSx-Dest	snapmirror	svm01

Ciptakan SnapMirror hubungan

Sekarang Anda telah mengintip sumber dan tujuan SVMs, langkah selanjutnya adalah membuat dan menginisialisasi SnapMirror hubungan pada cluster tujuan.

Note

Setelah Anda membuat dan menginisialisasi SnapMirror hubungan, volume tujuan hanya dibaca sampai hubungan terputus.

- Gunakan [snapmirror create](#) perintah untuk membuat SnapMirror hubungan pada cluster tujuan. `snapmirror create` Perintah harus digunakan dari SVM tujuan.

Anda dapat secara opsional menggunakan `-throttle` untuk mengatur bandwidth maksimum (dalam KB/detik) untuk hubungan. SnapMirror

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-path DestSVM:vol1 -vserver DestSVM -throttle unlimited
```

```
Operation succeeded: snapmirror create for the relationship with destination "DestSVM:vol1".
```

Transfer data ke sistem file ONTAP Anda FSx

Sekarang setelah Anda membuat SnapMirror hubungan, Anda dapat mentransfer data ke sistem file tujuan.

1. Anda dapat mentransfer data ke sistem file tujuan dengan menjalankan perintah berikut pada sistem file tujuan.

Note

Setelah Anda menjalankan perintah ini, SnapMirror mulai mentransfer snapshot data dari volume sumber ke volume tujuan.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-path SourceLocalName:vol1
```

2. Jika Anda memigrasikan data yang sedang digunakan secara aktif, Anda harus memperbarui kluster tujuan agar tetap disinkronkan dengan cluster sumber Anda. Untuk melakukan pembaruan satu kali ke cluster tujuan, jalankan perintah berikut.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

3. Anda juga dapat menjadwalkan pembaruan setiap jam atau harian sebelum menyelesaikan migrasi dan memindahkan klien Anda ke FSx ONTAP. Anda dapat membuat jadwal SnapMirror pembaruan menggunakan [snapmirror modify](#) perintah.

```
FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
```

Memotong ke Amazon FSx

Untuk mempersiapkan pemotongan ke sistem file FSx ONTAP Anda, lakukan hal berikut:

- Putuskan sambungan semua klien yang menulis ke cluster sumber.
 - Lakukan SnapMirror transfer akhir untuk memastikan tidak ada kehilangan data saat memotong.
 - Putuskan SnapMirror hubungan.
 - Connect semua klien ke sistem file ONTAP Anda FSx .
1. Untuk memastikan bahwa semua data dari cluster sumber ditransfer ke FSx sistem file ONTAP, lakukan transfer Snapmirror akhir.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. Pastikan migrasi data selesai dengan memverifikasi yang Mirror State disetel keSnapmirrored, dan Relationship Status disetel keIdle. Anda juga harus memastikan bahwa Last Transfer End Timestamp tanggalnya seperti yang diharapkan, seperti yang ditunjukkan kapan transfer terakhir ke volume tujuan terjadi.
3. Jalankan perintah berikut untuk menunjukkan SnapMirror status.

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp
```

Source Path	Destination Path	Mirror State	Relationship Status	Last Transfer End Timestamp
Svm01:vol1	svm02:DestVol	Snapmirrored	Idle	09/02 09:02:21

4. Nonaktifkan SnapMirror transfer future apa pun dengan menggunakan snapmirror quiesce perintah.

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. Verifikasi bahwa Relationship Status telah berubah menjadi Quiesced pengguna snapmirror show.

```
FSx-Dest::> snapmirror show
```

Source	Destination	Mirror	Relationship

Path	Path	State	Status
-----	-----	-----	-----
sourcesvm1:vol1	svm01:DestVol	Snapmirrored	Quiesced

6. Selama migrasi, volume tujuan hanya-baca. Untuk mengaktifkan baca/tulis, Anda perlu memutuskan SnapMirror hubungan dan memotong ke sistem file ONTAP Anda FSx . Putuskan SnapMirror hubungan menggunakan perintah berikut.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1
```

```
Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. Setelah SnapMirror replikasi selesai dan Anda telah memutuskan SnapMirror hubungan, Anda dapat memasang volume untuk membuat data tersedia.

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

Volume sekarang tersedia dengan data dari volume sumber yang sepenuhnya dimigrasikan ke volume tujuan Volume juga tersedia bagi klien untuk membaca dan menulis kepadanya. Jika sebelumnya Anda mengatur tiering-policy volume iniall, Anda dapat mengubahnya menjadi auto atau snapshot-only dan data Anda akan secara otomatis bertransisi antar tingkatan penyimpanan sesuai dengan pola akses. Untuk membuat data ini dapat diakses oleh klien dan aplikasi, lihat [Mengakses data FSx ONTAP Anda](#).

Migrasi ke FSx untuk ONTAP menggunakan AWS DataSync

Sebaiknya gunakan AWS DataSync untuk mentransfer data antara FSx untuk sistem file ONTAP dan sistem file non-ONTAP, termasuk FSx untuk Lustre, untuk OpenZFS, FSx untuk Windows FSx File Server, Amazon EFS, Amazon S3, dan filer lokal. Jika Anda mentransfer file antara FSx ONTAP dan NetApp ONTAP, sebaiknya gunakan [NetApp SnapMirror](#) AWS DataSync adalah layanan transfer data yang menyederhanakan, mengotomatisasi, dan mempercepat pemindahan dan replikasi data antara sistem penyimpanan yang dikelola sendiri dan layanan AWS penyimpanan melalui internet atau. Direct Connect DataSync dapat mentransfer data dan metadata sistem file Anda, seperti kepemilikan, stempel waktu, dan izin akses.

Anda dapat menggunakan DataSync untuk mentransfer file antara dua FSx untuk sistem file ONTAP, dan juga memindahkan data ke sistem file di AWS akun yang berbeda Wilayah AWS atau. Anda juga dapat menggunakan DataSync dengan FSx untuk sistem file ONTAP 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 DataSync, lokasi adalah titik akhir untuk sistem file FSx untuk ONTAP. Untuk informasi tentang skenario transfer tertentu, lihat [Bekerja dengan lokasi](#) di Panduan AWS DataSync Pengguna.

Note

Jika Anda berencana menggunakan kebijakan All tiering untuk memigrasikan data Anda ke tingkat kumpulan kapasitas, ingatlah bahwa metadata file selalu disimpan di tingkat SSD, dan semua data pengguna baru pertama kali ditulis ke tingkat SSD. Ketika data ditulis ke tingkat SSD, proses tiering latar belakang akan mulai meningkatkan data Anda ke penyimpanan kumpulan kapasitas, tetapi proses tiering tidak langsung dan menghabiskan sumber daya jaringan. Anda perlu mengukur tingkat SSD Anda untuk memperhitungkan metadata file (3-7% dari ukuran data pengguna), sebagai buffer untuk data pengguna sebelum berjenjang ke penyimpanan kolam kapasitas. Kami menyarankan Anda untuk tidak melebihi 80% pemanfaatan SSD.

Saat memigrasikan data, pastikan untuk memantau tingkat SSD Anda menggunakan [metrik sistem CloudWatch File](#) untuk memastikan bahwa itu tidak mengisi lebih cepat daripada proses tiering dapat memindahkan data ke penyimpanan kumpulan kapasitas. Anda juga dapat membatasi DataSync transfer ke tingkat yang lebih rendah dari tingkat tiering yang terjadi untuk memastikan bahwa tingkat SSD Anda tidak melebihi penggunaan 80%. Misalnya, untuk sistem file dengan kapasitas throughput minimal 512 MBps, MBps throttle 200 biasanya akan menyeimbangkan transfer data dan tingkat tiering data.

Prasyarat

Untuk memigrasikan data ke penyiapan ONTAP, Anda memerlukan server dan jaringan yang memenuhi persyaratan. FSx DataSync Untuk mempelajari lebih lanjut, lihat [Persyaratan untuk DataSync](#) di Panduan AWS DataSync Pengguna.

Langkah-langkah dasar untuk memigrasi file menggunakan DataSync

Mentransfer file dari sumber ke tujuan menggunakan DataSync melibatkan langkah-langkah dasar berikut:

- Unduh dan gunakan agen di lingkungan Anda dan aktifkan (tidak diperlukan jika mentransfer antar Layanan AWS).

- Buat lokasi sumber dan tujuan.
- Buat tugas.
- Jalankan tugas untuk mentransfer file dari sumber ke tujuan.

Untuk informasi selengkapnya, lihat topik berikut di Panduan Pengguna AWS DataSync :

- [Transfer data antara penyimpanan yang dikelola sendiri dan AWS](#)
- [Membuat lokasi untuk Amazon FSx untuk NetApp ONTAP](#)

Keamanan di Amazon FSx untuk NetApp ONTAP

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan dari cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di AWS Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi efektivitas keamanan kami sebagai bagian dari [Program AWS Kepatuhan Program AWS Kepatuhan](#). Untuk mempelajari tentang program kepatuhan yang berlaku untuk Amazon FSx untuk NetApp ONTAP, lihat [AWS Layanan dalam Lingkup berdasarkan AWS Layanan Program Kepatuhan](#).
- Keamanan di cloud — Tanggung jawab Anda ditentukan oleh AWS layanan yang Anda gunakan. Anda juga bertanggung jawab atas faktor lain, yang mencakup sensitivitas data Anda, persyaratan perusahaan Anda, serta undang-undang dan peraturan yang berlaku.

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

Topik

- [Perlindungan data di Amazon FSx untuk NetApp ONTAP](#)
- [Manajemen identitas dan akses untuk Amazon FSx untuk NetApp ONTAP](#)
- [AWS kebijakan terkelola untuk Amazon FSx untuk NetApp ONTAP](#)
- [Kontrol Akses Sistem File dengan Amazon VPC](#)
- [Validasi Kepatuhan untuk Amazon FSx untuk NetApp ONTAP](#)
- [Amazon FSx untuk NetApp ONTAP dan antarmuka titik akhir VPC \(AWS PrivateLink\)](#)
- [Ketahanan di Amazon FSx untuk ONTAP NetApp](#)
- [Keamanan infrastruktur di Amazon FSx untuk NetApp ONTAP](#)
- [Gunakan NetApp ONTAP Vscan dengan FSx untuk ONTAP](#)

- [ONTAP peran dan pengguna](#)

Perlindungan data di Amazon FSx untuk NetApp ONTAP

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Amazon FSx untuk NetApp ONTAP. 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 kredensial dan mengatur pengguna individu dengan AWS IAM Identity Center atau AWS Identity and Access Management (IAM). Dengan cara itu, setiap pengguna hanya diberi izin yang diperlukan untuk memenuhi tanggung jawab tugasnya. Kami juga menyarankan supaya Anda mengamankan data dengan cara-cara berikut:

- Gunakan autentikasi multi-faktor (MFA) pada setiap akun.
- Gunakan SSL/TLS untuk berkomunikasi dengan AWS sumber daya. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail. Untuk informasi tentang penggunaan CloudTrail jejak untuk menangkap AWS aktivitas, lihat [Bekerja dengan CloudTrail jejak](#) di AWS CloudTrail Panduan Pengguna.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola tingkat lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-3 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi selengkapnya tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-3](#).

Kami sangat merekomendasikan agar Anda tidak pernah memasukkan informasi identifikasi yang sensitif, seperti nomor rekening pelanggan Anda, ke dalam tanda atau bidang isian bebas seperti

bidang Nama. Ini termasuk saat Anda bekerja dengan Amazon FSx 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 ONTAP

Amazon FSx untuk NetApp ONTAP mendukung enkripsi data saat istirahat dan enkripsi data dalam perjalanan. Enkripsi data saat istirahat diaktifkan secara otomatis saat membuat sistem FSx file Amazon. Amazon FSx untuk NetApp ONTAP mendukung enkripsi berbasis Kerberos dalam perjalanan melalui protokol NFS dan SMB jika Anda mengakses data di Storage Virtual Machine (SVM) yang digabungkan ke Active Directory atau ke domain menggunakan Lightweight Directory Access Protocol (LDAP).

Kapan menggunakan enkripsi

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.

Untuk informasi selengkapnya tentang enkripsi data dengan Amazon FSx untuk NetApp ONTAP, lihat [Enkripsi data saat tidak digunakan](#) dan [Mengenkripsi data dalam perjalanan](#).

Enkripsi data saat tidak digunakan

Semua sistem file Amazon FSx untuk NetApp ONTAP dan cadangan 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. Semua backup secara otomatis dienkripsi pada saat pembuatan, dan secara otomatis didekripsi ketika cadangan dikembalikan ke volume baru. 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 kunci KMS untuk mengenkripsi sistem file Anda dan cadangan volume apa pun. Anda memilih kunci KMS yang digunakan untuk mengenkripsi dan mendekripsi sistem file dan cadangan volume (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:

- AWS-Managed KMS key - Ini adalah kunci KMS default, dan gratis untuk digunakan.
- Kunci KMS yang dikelola 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 KMS, lihat [Membuat Kunci](#) di Panduan AWS Key Management Service Pengembang.

 Important

Amazon hanya FSx menerima kunci KMS enkripsi simetris. Anda tidak dapat menggunakan kunci KMS asimetris dengan Amazon FSx.

Jika Anda menggunakan kunci KMS 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 KMS 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 dan Mengaktifkan dan menonaktifkan kunci](#) di Panduan Pengembang AWS Key Management Service.

Kebijakan FSx utama Amazon 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 dan cadangan terenkripsi saat istirahat:

- kms:Encrypt – (Opsional) Mengenkripsi plaintext ke ciphertext. Izin ini termasuk dalam kebijakan kunci default.
- kms:Decrypt – (Wajib) Mendekripsi ciphertext. Ciphertext adalah teks biasa yang sebelumnya telah dienkripsi. Izin ini termasuk dalam kebijakan kunci default.
- kms: ReEncrypt — (Opsional) Mengenkripsi data di sisi server dengan yang baru AWS KMS key, 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 lebih lanjut tentang hibah, lihat [Menggunakan Pemberian](#) di Panduan Developer AWS Key Management Service . 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 dalam perjalanan

Topik ini menjelaskan berbagai opsi yang tersedia untuk mengenkripsi data file Anda saat sedang dalam perjalanan antara sistem file FSx untuk ONTAP dan klien yang terhubung. Ini juga memberikan panduan untuk membantu Anda memilih metode enkripsi mana yang paling cocok untuk alur kerja Anda.

Semua data yang mengalir di Wilayah AWS seluruh jaringan AWS global secara otomatis dienkripsi pada lapisan fisik sebelum meninggalkan fasilitas yang AWS aman. Semua lalu lintas antara Availability Zones dienkripsi. Lapisan enkripsi tambahan, termasuk yang tercantum di bagian ini, memberikan perlindungan tambahan. Untuk informasi selengkapnya tentang cara AWS menyediakan perlindungan untuk data yang mengalir di seluruh Zona Tersedia Wilayah AWS, dan instans, lihat [Enkripsi saat transit di](#) Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.

Amazon FSx untuk NetApp ONTAP mendukung metode berikut untuk mengenkripsi data dalam perjalanan antara FSx untuk sistem file ONTAP dan klien yang terhubung:

- [Enkripsi berbasis Nitro otomatis atas semua protokol dan klien yang didukung yang berjalan pada jenis instans Amazon EC2 Linux dan Windows yang didukung.](#)
- Enkripsi berbasis Kerberos melalui protokol NFS dan SMB.
- IPsec enkripsi berbasis melalui protokol NFS, iSCSI, dan SMB

Semua metode yang didukung untuk mengenkripsi data dalam perjalanan menggunakan algoritme kriptografi AES-256 standar industri yang menyediakan enkripsi kekuatan perusahaan.

Topik

- [Memilih metode untuk mengenkripsi data dalam perjalanan](#)
- [Mengekripsi data dalam perjalanan dengan AWS Sistem Nitro](#)
- [Mengekripsi data dalam perjalanan dengan enkripsi berbasis Kerberos](#)
- [Mengekripsi data dalam perjalanan dengan enkripsi IPsec](#)
- [Mengaktifkan enkripsi data SMB dalam perjalanan](#)
- [Mengkonfigurasi IPsec menggunakan otentikasi PSK](#)
- [Mengkonfigurasi IPsec menggunakan otentikasi sertifikat](#)

Memilih metode untuk mengenkripsi data dalam perjalanan

Bagian ini memberikan informasi yang dapat membantu Anda memutuskan enkripsi mana yang didukung dalam metode transit yang terbaik untuk alur kerja Anda. Lihat kembali bagian ini saat Anda menjelajahi opsi yang didukung yang dijelaskan secara rinci di bagian berikut.

Ada beberapa faktor yang perlu dipertimbangkan ketika memilih bagaimana Anda akan mengenkripsi data dalam perjalanan antara sistem file ONTAP Anda FSx dan klien yang terhubung. Faktor-faktor ini meliputi:

- Sistem file FSx untuk ONTAP Anda berjalan di. Wilayah AWS
- Jenis instance yang dijalankan klien.
- Lokasi klien yang mengakses sistem file Anda.
- Persyaratan kinerja jaringan.
- Protokol data yang ingin Anda enkripsi.
- Jika Anda menggunakan Microsoft Active Directory.

Wilayah AWS

Sistem file Anda berjalan menentukan apakah Anda dapat menggunakan enkripsi berbasis Amazon Nitro atau tidak. Wilayah AWS Untuk informasi selengkapnya, lihat [Mengenkripsi data dalam perjalanan dengan AWS Sistem Nitro](#).

Jenis contoh klien

[Anda dapat menggunakan enkripsi berbasis Amazon Nitro jika klien yang mengakses sistem file Anda berjalan di salah satu jenis instans Amazon EC2 Mac, Linux, atau Windows yang didukung, dan alur kerja Anda memenuhi semua persyaratan lain untuk menggunakan enkripsi berbasis Nitro.](#) Tidak ada persyaratan jenis instance klien untuk menggunakan Kerberos atau IPsec enkripsi.

Lokasi klien

Lokasi klien yang mengakses data sehubungan dengan lokasi sistem file Anda memengaruhi metode enkripsi in-transit yang tersedia untuk digunakan. Anda dapat menggunakan salah satu metode enkripsi yang didukung jika klien dan sistem file berada di VPC yang sama. Hal yang sama berlaku jika klien dan sistem file berada di peered VPCs, selama lalu lintas tidak melewati perangkat atau layanan jaringan virtual, seperti gateway transit. Enkripsi berbasis Nitro bukanlah pilihan yang tersedia jika klien tidak berada dalam VPC yang sama atau diintip, atau jika lalu lintas melewati perangkat atau layanan jaringan virtual.

Performa jaringan

Menggunakan enkripsi berbasis Amazon Nitro tidak berdampak pada kinerja jaringan. Ini karena instans Amazon EC2 yang didukung menggunakan kemampuan pembongkaran perangkat keras Sistem Nitro yang mendasarinya untuk secara otomatis mengenkripsi lalu lintas dalam transit antar instans.

Menggunakan Kerberos atau IPsec enkripsi berdampak pada kinerja jaringan. Ini karena kedua metode enkripsi ini berbasis perangkat lunak, yang mengharuskan klien dan server untuk

menggunakan sumber daya komputasi untuk mengenkripsi dan mendekripsi lalu lintas dalam transit.

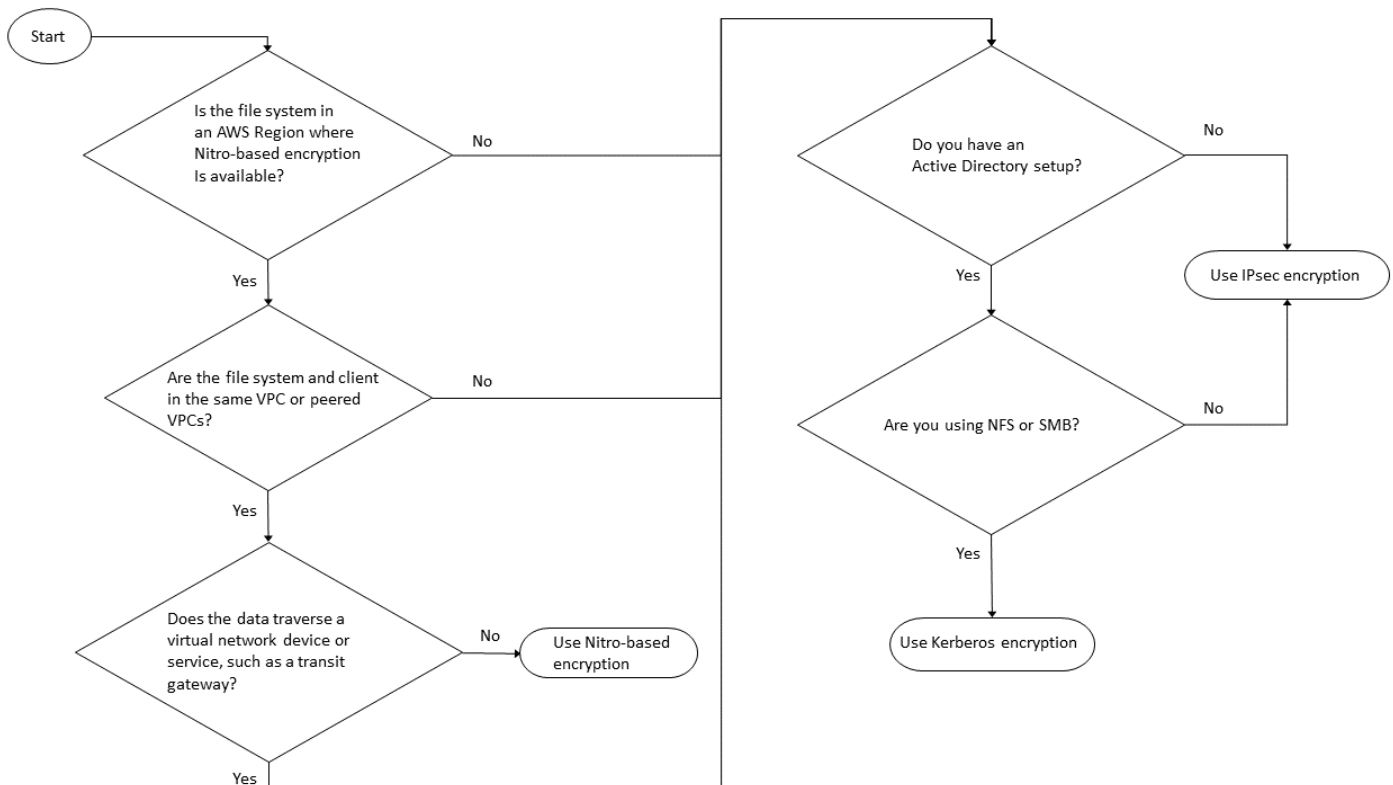
Protokol data

Anda dapat menggunakan enkripsi dan IPsec enkripsi berbasis Amazon Nitro dengan semua protokol yang didukung — NFS, SMB, dan iSCSI. Anda dapat menggunakan enkripsi Kerberos dengan protokol NFS dan SMB (dengan Active Directory).

Active Directory

Jika Anda menggunakan Microsoft Active Directory, Anda dapat menggunakan [enkripsi Kerberos melalui protokol](#) NFS dan SMB.

Gunakan diagram berikut untuk membantu Anda memutuskan metode enkripsi dalam transit mana yang akan digunakan.



IPsec enkripsi adalah satu-satunya pilihan yang tersedia ketika semua kondisi berikut berlaku untuk alur kerja Anda:

- Anda menggunakan protokol NFS, SMB, atau iSCSI.
- Alur kerja Anda tidak mendukung penggunaan enkripsi berbasis Amazon Nitro.

- Anda tidak menggunakan domain Microsoft Active Directory.

Mengenkripsi data dalam perjalanan dengan AWS Sistem Nitro

Dengan enkripsi berbasis NITRO, data dalam transit dienkripsi secara otomatis saat klien yang mengakses sistem file Anda berjalan pada jenis instans Amazon EC2 [Linux](#) atau [Windows](#) yang didukung di Wilayah AWS mana data tersebut tersedia untuk ONTAP. FSx

Menggunakan enkripsi berbasis Amazon Nitro tidak berdampak pada kinerja jaringan. Ini karena instans Amazon EC2 yang didukung menggunakan kemampuan pembongkaran perangkat keras Sistem Nitro yang mendasarinya untuk secara otomatis mengenkripsi lalu lintas dalam transit antar instans.

Enkripsi berbasis Nitro diaktifkan secara otomatis ketika jenis instance klien yang didukung berada di VPC yang sama Wilayah AWS dan di VPC yang sama atau di VPC yang diintegrasikan dengan VPC sistem file. Selain itu, jika klien berada dalam VPC peered, maka data tidak dapat melintasi perangkat atau layanan jaringan virtual (seperti gateway transit) agar enkripsi berbasis NITRO diaktifkan secara otomatis. Untuk informasi selengkapnya tentang enkripsi berbasis Nitro, lihat bagian Enkripsi dalam perjalanan dari Panduan Pengguna Amazon EC2 [untuk jenis instans](#) Linux [atau](#) Windows.

Tabel berikut merinci enkripsi berbasis Nitro Wilayah AWS yang tersedia.

Support untuk enkripsi berbasis Nitro

Generasi	Jenis deployment	Wilayah AWS
Sistem file generasi pertama ¹	Tunggal-AZ 1 Multi-AZ 1	AS Timur (Virginia N.), AS Timur (Ohio), AS Barat (Oregon), Eropa (Irlandia)
Sistem file generasi kedua	Tunggal-AZ 2 Multi-AZ 2	AS Timur (Virginia N.), AS Timur (Ohio), AS Barat (California N.), AS Barat (Oregon), Eropa (Frankfurt), Eropa (Irlandia), Asia Pasifik (Sydney)

¹ Sistem file generasi pertama yang dibuat pada atau setelah 28 November 2022 mendukung enkripsi in-transit berbasis Nitro dalam daftar. Wilayah AWS

Untuk informasi selengkapnya tentang Wilayah AWS tempat FSx ONTAP tersedia, lihat [Amazon FSx untuk Harga NetApp ONTAP](#).

Untuk informasi selengkapnya tentang spesifikasi kinerja FSx untuk sistem file ONTAP, lihat [Dampak kapasitas throughput terhadap performa](#).

Mengenkripsi data dalam perjalanan dengan enkripsi berbasis Kerberos

[Jika Anda menggunakan Microsoft Active Directory, Anda dapat menggunakan enkripsi berbasis Kerberos melalui protokol NFS dan SMB untuk mengenkripsi data dalam transit untuk volume anak yang SVMs digabungkan ke Microsoft Active Directory.](#)

Mengenkripsi data dalam perjalanan melalui NFS menggunakan Kerberos

Enkripsi data dalam transit menggunakan Kerberos didukung untuk NFSv3 dan protokol. NFSv4 Untuk mengaktifkan enkripsi dalam perjalanan menggunakan Kerberos untuk protokol NFS, lihat [Menggunakan Kerberos dengan NFS untuk keamanan yang kuat](#) di Pusat Dokumentasi. NetApp ONTAP

Mengenkripsi data dalam perjalanan melalui SMB menggunakan Kerberos

Mengenkripsi data dalam perjalanan melalui protokol SMB didukung pada berbagi file yang dipetakan pada instance komputasi yang mendukung protokol SMB 3.0 atau yang lebih baru. Ini termasuk semua Microsoft Windows versi dari Microsoft Windows Server 2012 dan yang lebih baru, dan Microsoft Windows 8 dan yang lebih baru. Ketika diaktifkan, FSx untuk ONTAP secara otomatis mengenkripsi data dalam perjalanan menggunakan enkripsi SMB saat Anda mengakses sistem file Anda tanpa perlu memodifikasi aplikasi Anda.

FSx untuk ONTAP SMB mendukung enkripsi 128 dan 256 bit, yang ditentukan oleh permintaan sesi klien. Untuk deskripsi tingkat enkripsi yang berbeda, lihat bagian Mengatur tingkat keamanan otentikasi minimum server SMB dari [Kelola SMB dengan CLI di Pusat Dokumentasi](#). NetApp ONTAP

Note

Klien menentukan algoritma enkripsi. Otentikasi NTLM dan Kerberos bekerja dengan enkripsi 128 dan 256 bit. Server SMB FSx untuk ONTAP menerima semua permintaan klien Windows standar, dan kontrol granular ditangani oleh Kebijakan Grup Microsoft atau pengaturan Registri.

Anda menggunakan ONTAP CLI untuk mengelola enkripsi dalam pengaturan transit FSx untuk ONTAP SVMs dan volume. Untuk mengakses NetApp ONTAP CLI, buat sesi SSH pada SVM tempat Anda membuat enkripsi dalam pengaturan transit, seperti yang dijelaskan dalam [Mengelola SVMs dengan ONTAP CLI](#)

Untuk petunjuk tentang cara mengaktifkan enkripsi SMB pada SVM atau volume, lihat [Mengaktifkan enkripsi data SMB dalam perjalanan](#)

Mengenkripsi data dalam perjalanan dengan enkripsi IPsec

FSx untuk ONTAP mendukung penggunaan IPsec protokol dalam mode transportasi untuk memastikan data terus aman dan terenkripsi, saat dalam perjalanan. IPsec menawarkan end-to-end enkripsi data dalam transit antara klien dan FSx untuk sistem file ONTAP untuk semua lalu lintas IP yang didukung - protokol NFS, iSCSI, dan SMB. Dengan IPsec enkripsi, Anda membuat IPsec terowongan antara SVM FSx untuk ONTAP yang dikonfigurasi dengan IPsec diaktifkan, dan IPsec klien yang berjalan pada klien yang terhubung yang mengakses data.

Kami menyarankan Anda menggunakan IPsec untuk mengenkripsi data dalam perjalanan melalui protokol NFS, SMB, dan iSCSI saat mengakses data Anda dari klien yang tidak mendukung [enkripsi berbasis NITRO, dan jika klien Anda dan tidak bergabung ke Active Directory, yang diperlukan untuk enkripsi berbasis](#) SVMs Kerberos. IPsec enkripsi adalah satu-satunya pilihan yang tersedia untuk mengenkripsi data dalam perjalanan untuk lalu lintas iSCSI ketika klien iSCSI Anda tidak mendukung enkripsi berbasis Nitro.

Untuk IPsec otentikasi, Anda dapat menggunakan kunci pra-bersama (PSKs) atau sertifikat. Jika Anda menggunakan PSK, IPsec klien yang Anda gunakan harus mendukung Internet Key Exchange versi 2 (IKEv2) dengan PSK. Langkah-langkah tingkat tinggi untuk mengonfigurasi IPsec enkripsi pada ONTAP dan klien adalah sebagai berikut: FSx

1. Aktifkan dan konfigurasikan IPsec pada sistem file Anda.
2. Instal dan konfigurasikan IPsec pada klien Anda
3. Konfigurasikan IPsec untuk beberapa akses klien

Untuk informasi selengkapnya tentang cara mengonfigurasi IPsec menggunakan PSK, lihat [Mengkonfigurasi keamanan IP \(IPsec\) melalui enkripsi kawat](#) di pusat NetApp ONTAP dokumentasi.

Untuk informasi selengkapnya tentang cara mengonfigurasi IPsec menggunakan sertifikat, lihat [Mengkonfigurasi IPsec menggunakan otentikasi sertifikat](#).

Mengaktifkan enkripsi data SMB dalam perjalanan

Secara default, saat Anda membuat SVM, enkripsi SMB dimatikan. Anda dapat mengaktifkan enkripsi SMB yang diperlukan pada saham individu, atau pada SVM, yang menyalakannya untuk semua saham di SVM tersebut.

Note

Ketika enkripsi SMB yang diperlukan diaktifkan pada SVM atau berbagi, klien SMB yang tidak mendukung enkripsi tidak dapat terhubung ke SVM atau berbagi itu.

Untuk memerlukan enkripsi SMB untuk lalu lintas SMB yang masuk pada SVM

Gunakan prosedur berikut untuk meminta enkripsi SMB pada SVM menggunakan CLINetApp ONTAP.

1. Untuk terhubung ke titik akhir manajemen SVM dengan SSH, gunakan nama pengguna vsadmin dan kata sandi vsadmin yang Anda atur saat membuat SVM. Jika Anda tidak menetapkan kata sandi vsadmin, gunakan nama pengguna fsxadmin dan kata sandi fsxadmin. Anda dapat SSH ke SVM dari klien yang berada di VPC yang sama dengan sistem file, menggunakan alamat IP endpoint manajemen atau nama DNS.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

Perintah dengan nilai sampel:

```
ssh vsadmin@198.51.100.10
```

Perintah SSH menggunakan nama DNS endpoint manajemen:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

Perintah SSH menggunakan contoh nama DNS:

```
ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-east-2.aws.com
```

Password: **vsadmin-password**

This is your first recorded login.
FsxIdabcdef01234567892::>

- Gunakan perintah [vserver cifs security modify](#) NetApp ONTAP CLI untuk meminta enkripsi SMB untuk lalu lintas SMB masuk ke SVM.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
```

- Untuk berhenti memerlukan enkripsi SMB untuk lalu lintas SMB yang masuk, gunakan perintah berikut.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required false
```

- Untuk melihat `is-smb-encryption-required` pengaturan saat ini pada SVM, gunakan perintah [vserver cifs security show](#) NetApp ONTAP CLI:

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-----  -
vs1      true
```

Untuk informasi selengkapnya tentang mengelola enkripsi SMB di SVM, lihat [Mengonfigurasi enkripsi SMB yang diperlukan di server SMB untuk transfer data melalui SMB](#) di Pusat Dokumentasi. NetApp ONTAP

Untuk mengaktifkan enkripsi SMB pada volume

Gunakan prosedur berikut untuk mengaktifkan enkripsi SMB pada bagian menggunakan NetApp ONTAP CLI.

- Buat koneksi shell aman (SSH) ke titik akhir manajemen SVM seperti yang dijelaskan dalam [Mengelola SVMs dengan ONTAP CLI](#)
- Gunakan perintah NetApp ONTAP CLI berikut untuk membuat berbagi SMB baru dan memerlukan enkripsi SMB saat mengakses bagian ini.

```
vserver cifs share create -vserver vserver_name -share-name share_name -  
path share_path -share-properties encrypt-data
```

Untuk informasi lebih lanjut, lihat [vserver cifs share created](#) di halaman manual NetApp ONTAP CLI Command.

3. Untuk memerlukan enkripsi SMB pada berbagi SMB yang ada, gunakan perintah berikut.

```
vserver cifs share properties add -vserver vserver_name -share-name share_name -  
share-properties encrypt-data
```

Untuk informasi lebih lanjut, lihat [vserver cifs share created](#) di halaman manual NetApp ONTAP CLI Command.

4. Untuk mematikan enkripsi SMB pada berbagi SMB yang ada, gunakan perintah berikut.

```
vserver cifs share properties remove -vserver vserver_name -share-name share_name -  
share-properties encrypt-data
```

Untuk informasi lebih lanjut, lihat [vserver cifs share properties removed](#) di halaman manual NetApp ONTAP CLI Command.

5. Untuk melihat is-smb-encryption-required pengaturan saat ini pada berbagi SMB, gunakan perintah NetApp ONTAP CLI berikut:

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -  
fields share-properties
```

Jika salah satu properti yang dikembalikan oleh perintah adalah `encrypt-data` properti, maka properti tersebut menentukan bahwa enkripsi SMB harus digunakan saat mengakses share ini.

Untuk informasi lebih lanjut, lihat [vserver cifs share properties show](#) di halaman manual NetApp ONTAP CLI Command.

Mengkonfigurasi IPsec menggunakan otentikasi PSK

Jika Anda menggunakan PSK untuk otentikasi, langkah-langkah untuk mengonfigurasi IPsec enkripsi pada ONTAP dan klien adalah sebagai berikut: FSx

1. Aktifkan dan konfigurasi IPsec pada sistem file Anda.
2. Instal dan konfigurasi IPsec pada klien Anda
3. Konfigurasi IPsec untuk beberapa akses klien

Untuk detail tentang mengonfigurasi IPsec menggunakan PSK, lihat [Mengonfigurasi keamanan IP \(IPsec\) melalui enkripsi kawat](#) di pusat NetApp ONTAP dokumentasi.

Mengkonfigurasi IPsec menggunakan otentikasi sertifikat

Topik berikut memberikan instruksi untuk mengkonfigurasi IPsec enkripsi menggunakan otentikasi sertifikat pada sistem file FSx untuk ONTAP dan klien yang menjalankan Libreswan. IPsec Solusi ini menggunakan AWS Certificate Manager dan AWS Private Certificate Authority membuat otoritas sertifikat pribadi dan untuk menghasilkan sertifikat.

Langkah-langkah tingkat tinggi untuk mengonfigurasi IPsec enkripsi menggunakan otentikasi sertifikat FSx untuk sistem file ONTAP dan klien yang terhubung adalah sebagai berikut:

1. Memiliki otoritas sertifikat untuk menerbitkan sertifikat.
2. Menghasilkan dan mengekspor sertifikat CA untuk sistem file dan klien.
3. Instal sertifikat dan konfigurasi IPsec pada instance klien.
4. Instal sertifikat dan konfigurasi IPsec pada sistem file Anda.
5. Tentukan database kebijakan keamanan (SPD).
6. Konfigurasi IPsec untuk beberapa akses klien.

Membuat dan menginstal sertifikat CA

Untuk otentikasi sertifikat, Anda perlu membuat dan menginstal sertifikat dari otoritas sertifikat pada sistem file ONTAP Anda FSx dan klien yang akan mengakses data pada sistem file Anda. Contoh berikut digunakan AWS Private Certificate Authority untuk mengatur otoritas sertifikat pribadi, dan menghasilkan sertifikat untuk menginstal pada sistem file dan klien. Dengan menggunakan AWS Private Certificate Authority, Anda dapat membuat hierarki root dan subordinate certificate authority (CAs) yang sepenuhnya AWS dihosting untuk penggunaan internal oleh organisasi Anda. Proses ini memiliki lima langkah:

1. Membuat Private Certificate Authority (CA) menggunakan AWS Private CA
2. Keluarkan dan instal sertifikat root pada CA pribadi

3. Minta sertifikat pribadi AWS Certificate Manager untuk sistem file dan klien Anda
4. Ekspor sertifikat untuk sistem file dan klien.

Untuk informasi selengkapnya, lihat [Administrasi CA pribadi](#) di Panduan AWS Private Certificate Authority Pengguna.

Untuk membuat CA pribadi root

1. Saat Anda membuat CA, Anda harus menentukan konfigurasi CA dalam file yang Anda berikan. Perintah berikut menggunakan editor teks Nano untuk membuat `ca_config.txt` file, yang menentukan informasi berikut:

- Nama algoritme
- Algoritma penandatanganan yang digunakan CA untuk menandatangani
- Informasi subjek X.500

```
$ > nano ca_config.txt
```

Editor teks muncul.

2. Edit file dengan spesifikasi untuk CA Anda.

```
{
  "KeyAlgorithm":"RSA_2048",
  "SigningAlgorithm":"SHA256WITHRSA",
  "Subject":{
    "Country":"US",
    "Organization":"Example Corp",
    "OrganizationalUnit":"Sales",
    "State":"WA",
    "Locality":"Seattle",
    "CommonName":"*.ec2.internal"
  }
}
```

3. Simpan dan tutup file, keluar dari editor teks. Untuk informasi selengkapnya, lihat [Prosedur untuk membuat CA](#) di Panduan AWS Private Certificate Authority Pengguna.
4. Gunakan perintah [create-certificate-authority](#) AWS Private CA CLI untuk membuat CA pribadi.

```
~/home > aws acm-pca create-certificate-authority \
--certificate-authority-configuration file://ca_config.txt \
--certificate-authority-type "R00T" \
--idempotency-token 01234567 --region aws-region
```

Jika berhasil, perintah ini mengeluarkan Amazon Resource Name (ARN) dari CA.

```
{
  "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Untuk membuat dan menginstal sertifikat untuk root pribadi CA (AWS CLI)

1. Buat permintaan penandatanganan sertifikat (CSR) menggunakan perintah `get-certificate-authority-csr` AWS CLI.

```
$ aws acm-pca get-certificate-authority-csr \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --output text \
    --endpoint https://acm-pca.aws-region.amazonaws.com \
    --region eu-west-1 > ca.csr
```

File yang dihasilkan `.csr`, file PEM yang dikodekan dalam format base64, memiliki tampilan sebagai berikut.

-----BEGIN CERTIFICATE-----
MIICiTCCAFICCD6m7oRw0uX0jANBgkqhkiG9w0BAQUFADCBiDELMAKGA1UEBhMC
VVMxCzAJBgNVBAGTAldBMRAwDgYDVQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWf6
b24xFDASBgNVBASTC0lBTSBDb25zb2x1MRIwEAYDVQQDEw1lUZXN0Q2l5YWMxHZA
BgkqhkiG9w0BCQEWEG5vb25lQGfYXpvi5jb20wHhcnMTENDI1MjA0NTIxWhcn
MTIwNDI0MjA0NTIxWjCBiDELMAKGA1UEBhMCVVMxCzAJBgNVBAGTAldBMRAwDgYD
VQQHEwdTZWF0dGx1MQ8wDQYDVQQKEwZBbWf6b24xFDASBgNVBASTC0lBTSBDb25z
b2x1MRIwEAYDVQQDEw1lUZXN0Q2l5YWMxHZAuBgkqhkiG9w0BCQEWEG5vb25lQGfY
Xpvi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLyGVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITx0USQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb30hjZnzcVQAARHhd1QWIMm2nrAqMBAAEWdQYJKoZIhvcNAQEFBQADgYEATCu4

```
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJI1J00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp3780D8uTs7fLvJx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----
```

Untuk informasi selengkapnya, lihat [Menginstal sertifikat CA root](#) di Panduan AWS Private Certificate Authority Pengguna.

- Gunakan [issue-certificate](#) AWS CLI perintah untuk menerbitkan dan menginstal sertifikat root pada CA pribadi Anda.

```
$ aws acm-pca issue-certificate \
  --certificate-authority-arn arn:aws:acm-pca:aws-
  region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
  --csr file://ca.csr \
  --signing-algorithm SHA256WITHRSA \
  --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
  --validity Value=3650,Type=DAYS --region aws-region
```

- Unduh sertifikat root menggunakan [get-certificate](#) AWS CLI perintah.

```
$ aws acm-pca get-certificate \
  --certificate-authority-arn arn:aws:acm-pca:aws-
  region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
  --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
  authority/12345678-1234-1234-1234-123456789012/certificate/
  abcdef0123456789abcdef0123456789 \
  --output text --region aws-region > rootCA.pem
```

- Instal sertifikat root pada CA pribadi Anda menggunakan [import-certificate-authority-certificate](#) AWS CLI perintah.

```
$ aws acm-pca import-certificate-authority-certificate \
  --certificate-authority-arn arn:aws:acm-pca:aws-
  region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
  --certificate file://rootCA.pem --region aws-region
```

Menghasilkan dan mengeksport sistem file dan sertifikat klien

- Gunakan [request-certificate](#) AWS CLI perintah untuk meminta AWS Certificate Manager sertifikat untuk digunakan pada sistem file dan klien Anda.


```
$ aws acm request-certificate \
  --domain-name *.ec2.internal \
  --idempotency-token 12345 \
  --region aws-region \
  --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

Jika permintaan berhasil, ARN dari sertifikat yang dikeluarkan dikembalikan.

2. Untuk keamanan, Anda harus menetapkan frasa sandi untuk kunci pribadi saat mengekspornya. Buat frasa sandi dan simpan dalam file bernama `passphrase.txt`
3. Gunakan [export-certificate](#) AWS CLI perintah untuk mengekspor sertifikat pribadi yang dikeluarkan sebelumnya. File yang diekspor berisi sertifikat, rantai sertifikat, dan kunci RSA 2048-bit pribadi terenkripsi yang terkait dengan kunci publik yang disematkan dalam sertifikat. Untuk keamanan, Anda harus menetapkan frasa sandi untuk kunci pribadi saat mengekspornya. Contoh berikut adalah untuk instance Linux EC2.

```
$ aws acm export-certificate \
  --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
  --passphrase $(cat passphrase.txt | base64) --region aws-region >
  exported_cert.json
```

4. Gunakan `jq` perintah berikut untuk mengekstrak kunci pribadi dan sertifikat dari respons JSON.

```
$ passphrase=$(cat passphrase.txt | base64)
cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
```

5. Gunakan `openssl` perintah berikut untuk mendekripsi kunci pribadi dari respons JSON. Setelah memasukkan perintah, Anda diminta untuk frasa sandi.

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

Menginstal dan mengonfigurasi Libreswan pada klien Amazon IPsec Linux 2

Bagian berikut memberikan petunjuk untuk menginstal dan mengonfigurasi Libreswan IPsec pada instans Amazon EC2 yang menjalankan Amazon Linux 2.

Untuk menginstal dan mengkonfigurasi Libreswan

1. Connect ke instans EC2 Anda menggunakan SSH. Untuk petunjuk spesifik tentang cara melakukannya, lihat [Connect ke instans Linux menggunakan klien SSH](#) di Panduan Pengguna Amazon Elastic Compute Cloud untuk Instans Linux.
2. Jalankan perintah berikut untuk menginstall libreswan:

```
$ sudo yum install libreswan
```

3. (Opsional) Saat memverifikasi IPsec di langkah selanjutnya, properti ini mungkin ditandai tanpa pengaturan ini. Kami menyarankan untuk menguji pengaturan Anda terlebih dahulu tanpa pengaturan ini. Jika koneksi Anda bermasalah, kembali ke langkah ini dan buat perubahan berikut.

Setelah instalasi selesai, gunakan editor teks pilihan Anda untuk menambahkan entri berikut ke file. `/etc/sysctl.conf`

```
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
```

Simpan perubahan dan keluar dari editor teks.

4. Terapkan perubahan.

```
$ sudo sysctl -p
```

5. Verifikasi IPsec konfigurasi.

```
$ sudo ipsec verify
```

Verifikasi bahwa versi yang Libreswan Anda instal sedang berjalan.

6. Inisialisasi database IPsec NSS.

```
$ sudo ipsec checknss
```

Untuk menginstal sertifikat pada klien

1. Salin [sertifikat yang Anda](#) buat untuk klien ke direktori kerja pada instans EC2. Anda
2. Ekspor sertifikat yang dihasilkan sebelumnya ke dalam format yang kompatibel dengan `libreswan`.

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \  
-certfile rootCA.pem -out certkey.p12 -name fsx
```

3. Impor kunci yang diformat ulang, berikan frasa sandi saat diminta.

```
$ sudo ipsec import certkey.p12
```

4. Buat file IPsec konfigurasi menggunakan editor teks pilihan.

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

Tambahkan entri berikut ke file konfigurasi:

```
conn fsxn  
    authby=rsasig  
    left=172.31.77.6  
    right=198.19.254.13  
    auto=start  
    type=transport  
    ikev2=insist  
    keyexchange=ike  
    ike=aes256-sha2_384;dh20  
    esp=aes_gcm_c256  
    leftcert=fsx  
    leftrsasigkey=%cert  
    leftid=%fromcert  
    rightid=%fromcert  
    rightrsasigkey=%cert
```

Anda akan mulai IPsec pada klien setelah mengkonfigurasi IPsec pada sistem file Anda.

Mengkonfigurasi IPsec pada sistem file Anda

Bagian ini memberikan petunjuk tentang menginstal sertifikat pada sistem file FSx ONTAP Anda, dan mengonfigurasi IPsec.

Untuk menginstal sertifikat pada sistem file Anda

1. Salin sertifikat root (`rootCA.pem`), sertifikat klien (`cert.pem`) dan file kunci (`decrypted.key`) yang didekripsi ke sistem file Anda. Anda perlu mengetahui frasa sandi untuk sertifikat.
2. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti `management_endpoint_ip` dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

3. Gunakan `cat` pada klien (bukan pada sistem file Anda) untuk daftar konten `rootCA.pem`, `cert.pem` dan `decrypted.key` file sehingga Anda dapat menyalin output dari setiap file dan menempelkannya ketika diminta dalam langkah-langkah berikut.

```
$ > cat cert.pem
```

Salin isi sertifikat.

4. Anda harus menginstal semua sertifikat CA yang digunakan selama autentikasi bersama, termasuk sisi OnTAP dan sisi klien CAs, ke manajemen ONTAP sertifikat kecuali sudah diinstal (seperti halnya Root-CA yang ditandatangani sendiri ONTAP).

Gunakan perintah `security certificate install` NetApp CLI sebagai berikut untuk menginstal sertifikat klien:

```
FSxID123:: > security certificate install -vserver dx -type client -cert-name  
ipsec-client-cert
```

```
Please enter Certificate: Press <Enter> when done
```

Tempel konten `cert.pem` file yang Anda salin sebelumnya dan tekan Enter.

```
Please enter Private Key: Press <Enter> when done
```

Tempel di isi decrypted.key file, dan tekan enter.

```
Do you want to continue entering root and/or intermediate certificates {y|n}:
```

Masukkan n untuk menyelesaikan memasukkan sertifikat klien.

5. Buat dan instal sertifikat untuk digunakan oleh SVM. Penerbit CA sertifikat ini harus sudah diinstal ONTAP dan ditambahkan ke IPsec.

Gunakan perintah berikut untuk menginstal sertifikat root.

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name  
ipsec-ca-cert
```

```
Please enter Certificate: Press <Enter> when done
```

Tempel di isi rootCA.pem file, dan tekan enter.

6. Untuk memastikan bahwa CA yang diinstal berada dalam jalur pencarian IPsec CA selama otentikasi, tambahkan manajemen ONTAP sertifikat CAs ke IPsec modul menggunakan perintah “security ipsec ca-certificate add”.

Masukkan perintah berikut untuk menambahkan sertifikat root.

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. Masukkan perintah berikut untuk membuat IPsec kebijakan yang diperlukan dalam database kebijakan keamanan (SPD).

```
security ipsec policy create -vserver dr -name policy-name -local-ip-  
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action  
ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity  
"CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. Gunakan perintah berikut untuk menunjukkan IPsec kebijakan untuk mengonfirmasi sistem file.

```
FSxID123:: > security ipsec policy show -vserver dr -instance
```

```
Vserver: dr
Policy Name: promise
Local IP Subnets: 198.19.254.13/32
Remote IP Subnets: 172.31.0.0/16
Local Ports: 0-0
Remote Ports: 0-0
Protocols: any
Action: ESP_TRA
Cipher Suite: SUITEB_GCM256
IKE Security Association Lifetime: 86400
IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
Is Policy Enabled: true
Local Identity: CN=*.ec2.internal
Remote Identity: CN=*.ec2.internal
Authentication Method: PKI
Certificate for Local Identity: ipsec-client-cert
```

IPsec Mulai dari klien

Sekarang IPsec dikonfigurasi pada kedua FSx untuk sistem file ONTAP dan klien, Anda dapat mulai IPsec pada klien.

1. Connect ke sistem klien Anda menggunakan SSH.
2. Mulai IPsec.

```
$ sudo ipsec start
```

3. Periksa status IPsec.

```
$ sudo ipsec status
```

4. Pasang volume pada sistem file Anda.

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. Verifikasi IPsec pengaturan dengan menunjukkan koneksi terenkripsi pada sistem file FSx ONTAP Anda.

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
```

```
FsxId08ac16c7ec2781a58:> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
```

Vserver	Policy Name	Local Address	Remote Address	Initiator-SPI	State
dr	<i>policy-name</i>	198.19.254.13	172.31.77.6	551c55de57fe8976	ESTABLISHED
fsx	<i>policy-name</i>	198.19.254.38	172.31.65.193	4fd3f22c993e60c5	ESTABLISHED

2 entries were displayed.

Menyiapkan IPsec untuk banyak klien

Ketika sejumlah kecil klien perlu memanfaatkan IPsec, menggunakan entri SPD tunggal untuk setiap klien sudah cukup. Namun, ketika ratusan atau bahkan ribuan klien perlu memanfaatkan IPsec, kami sarankan Anda menggunakan IPsec beberapa konfigurasi klien.

FSx untuk ONTAP mendukung menghubungkan beberapa klien di banyak jaringan ke satu alamat IP SVM dengan IPsec diaktifkan. Anda dapat melakukannya dengan menggunakan subnet konfigurasi atau `Allow all clients` konfigurasi, yang dijelaskan dalam prosedur berikut:

Untuk mengkonfigurasi IPsec untuk beberapa klien menggunakan konfigurasi subnet

Untuk memungkinkan semua klien pada subnet tertentu (192.168.134.0/24 misalnya) untuk terhubung ke alamat IP SVM tunggal menggunakan entri kebijakan SPD tunggal, Anda harus menentukan dalam bentuk subnet. `remote-ip-subnets` Selain itu, Anda harus menentukan `remote-identity` bidang dengan identitas sisi klien yang benar.

Important

Saat menggunakan otentikasi sertifikat, setiap klien dapat menggunakan sertifikat unik mereka sendiri atau sertifikat bersama untuk mengautentikasi. FSx untuk ONTAP IPsec memeriksa validitas sertifikat berdasarkan yang CAs diinstal pada toko kepercayaan lokalnya. FSx untuk ONTAP juga mendukung pemeriksaan daftar pencabutan sertifikat (CRL).

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

- Gunakan perintah `security ipsec policy create` NetApp ONTAP CLI sebagai berikut, ganti *sample* nilai dengan nilai spesifik Anda.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -remote-identity client_side_identity
```

Untuk mengkonfigurasi IPsec untuk beberapa klien menggunakan konfigurasi izinkan semua klien

Untuk mengizinkan klien mana pun, terlepas dari alamat IP sumbernya, untuk terhubung ke alamat IP IPsec berkemampuan SVM, gunakan kartu `0.0.0.0/0` liar saat menentukan bidang. `remote-ip-subnets`

Selain itu, Anda harus menentukan `remote-identity` bidang dengan identitas sisi klien yang benar. Untuk otentikasi sertifikat, Anda dapat memasukkan `ANYTHING`.

Juga, ketika kartu liar `0.0.0.0/0` digunakan, Anda harus mengonfigurasi nomor port lokal atau jarak jauh tertentu untuk digunakan. Misalnya, port NFS 2049.

- Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

- Gunakan perintah `security ipsec policy create` NetApp ONTAP CLI sebagai berikut, ganti *sample* nilai dengan nilai spesifik Anda.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
```



```
-cert-name my_nfs_server_cert -local-identity ontap_side_identity \  
-local-ports 2049 -remote-identity client_side_identity
```

Manajemen identitas dan akses untuk Amazon FSx untuk NetApp ONTAP

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 menggunakan sumber daya Amazon. FSx IAM adalah Layanan AWS yang dapat Anda gunakan tanpa biaya tambahan.

Topik

- [Audiens](#)
- [Mengautentikasi dengan identitas](#)
- [Mengelola akses menggunakan kebijakan](#)
- [Bagaimana Amazon FSx untuk NetApp ONTAP bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk Amazon untuk ONTAP FSx NetApp](#)
- [Memecahkan masalah Amazon FSx untuk identitas dan akses NetApp ONTAP](#)
- [Menggunakan peran terkait layanan untuk Amazon FSx](#)
- [Menggunakan tag dengan Amazon FSx](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda berdasarkan peran Anda:

- Pengguna layanan - minta izin dari administrator Anda jika Anda tidak dapat mengakses fitur (lihat [Memecahkan masalah Amazon FSx untuk identitas dan akses NetApp ONTAP](#))
- Administrator layanan - tentukan akses pengguna dan mengirimkan permintaan izin (lihat [Bagaimana Amazon FSx untuk NetApp ONTAP bekerja dengan IAM](#))
- Administrator IAM - tulis kebijakan untuk mengelola akses (lihat [Contoh kebijakan berbasis identitas untuk Amazon untuk ONTAP FSx NetApp](#))

Mengautentikasi dengan identitas

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

Anda dapat masuk sebagai identitas federasi menggunakan kredensial dari sumber identitas seperti AWS IAM Identity Center (Pusat Identitas IAM), autentikasi masuk tunggal, atau kredensial. Google/Facebook Untuk informasi selengkapnya tentang cara masuk, lihat [Cara masuk ke Akun AWS Anda](#) dalam Panduan Pengguna AWS Sign-In .

Untuk akses terprogram, AWS sediakan SDK dan CLI untuk menandatangani permintaan secara kriptografis. Untuk informasi selengkapnya, lihat [AWS Signature Version 4 untuk permintaan API](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang disebut pengguna Akun AWS root yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Untuk tugas yang memerlukan kredensial pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas terfederasi

Sebagai praktik terbaik, mewajibkan pengguna manusia untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS menggunakan kredensial sementara.

Identitas federasi adalah pengguna dari direktori perusahaan Anda, penyedia identitas web, atau Directory Service yang mengakses Layanan AWS menggunakan kredensial dari sumber identitas. Identitas terfederasi mengambil peran yang memberikan kredensial sementara.

Untuk manajemen akses terpusat, kami menyarankan AWS IAM Identity Center. Untuk informasi selengkapnya, lihat [Apa itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dengan izin khusus untuk satu orang atau aplikasi. Sebaiknya gunakan kredensial sementara alih-alih pengguna IAM dengan kredensial jangka panjang. Untuk informasi selengkapnya, lihat [Mewajibkan pengguna manusia untuk menggunakan federasi dengan](#)

[penyedia identitas untuk mengakses AWS menggunakan kredensial sementara](#) di Panduan Pengguna IAM.

[Grup IAM](#) menentukan kumpulan pengguna IAM dan mempermudah pengelolaan izin untuk pengguna dalam jumlah besar. Untuk mempelajari selengkapnya, lihat [Kasus penggunaan untuk pengguna IAM](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dengan izin khusus yang menyediakan kredensial sementara. Anda dapat mengambil peran dengan [beralih dari pengguna ke peran IAM \(konsol\)](#) atau dengan memanggil operasi AWS CLI atau AWS API. Untuk informasi selengkapnya, lihat [Metode untuk mengambil peran](#) dalam Panduan Pengguna IAM.

Peran IAM berguna untuk akses pengguna terfederasi, izin pengguna IAM sementara, akses lintas akun, akses lintas layanan, dan aplikasi yang berjalan di Amazon EC2. Untuk informasi selengkapnya, lihat [Akses sumber daya lintas akun di IAM](#) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan menentukan izin saat dikaitkan dengan identitas atau sumber daya. AWS mengevaluasi kebijakan ini ketika kepala sekolah membuat permintaan. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk informasi selengkapnya tentang dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Menggunakan kebijakan, administrator menentukan siapa yang memiliki akses ke apa dengan mendefinisikan principal mana yang dapat melakukan tindakan pada sumber daya apa, dan dalam kondisi apa.

Secara default, pengguna dan peran tidak memiliki izin. Administrator IAM membuat kebijakan IAM dan menambahkannya ke peran, yang kemudian dapat diambil oleh pengguna. Kebijakan IAM mendefinisikan izin terlepas dari metode yang Anda gunakan untuk melakukan operasinya.

Kebijakan berbasis identitas

Kebijakan berbasis identitas adalah dokumen kebijakan izin JSON yang Anda lampirkan ke identitas (pengguna, grup, atau peran). Kebijakan ini mengontrol tindakan apa yang bisa dilakukan oleh identitas tersebut, terhadap sumber daya yang mana, dan dalam kondisi apa. Untuk mempelajari

cara membuat kebijakan berbasis identitas, lihat [Tentukan izin IAM kustom dengan kebijakan yang dikelola pelanggan](#) dalam Panduan Pengguna IAM.

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

Kebijakan berbasis sumber daya

Kebijakan berbasis sumber daya adalah dokumen kebijakan JSON yang Anda lampirkan ke sumber daya. Contohnya termasuk kebijakan kepercayaan peran IAM dan kebijakan bucket Amazon S3. Dalam layanan yang mendukung kebijakan berbasis sumber daya, administrator layanan dapat menggunakannya untuk mengontrol akses ke sumber daya tertentu. Anda harus [menentukan principal](#) dalam kebijakan berbasis sumber daya.

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

Jenis-jenis kebijakan lain

AWS mendukung jenis kebijakan tambahan yang dapat menetapkan izin maksimum yang diberikan oleh jenis kebijakan yang lebih umum:

- Batasan izin – Menetapkan izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas kepada entitas IAM. Untuk informasi selengkapnya, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCPs) — Tentukan izin maksimum untuk organisasi atau unit organisasi di AWS Organizations. Untuk informasi selengkapnya, lihat [Kebijakan kontrol layanan](#) dalam Panduan Pengguna AWS Organizations .
- Kebijakan kontrol sumber daya (RCPs) — Tetapkan izin maksimum yang tersedia untuk sumber daya di akun Anda. Untuk informasi selengkapnya, lihat [Kebijakan kontrol sumber daya \(RCPs\)](#) di Panduan AWS Organizations Pengguna.
- Kebijakan sesi – Kebijakan lanjutan yang diteruskan sebagai parameter saat membuat sesi sementara untuk peran atau pengguna terfederasi. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

Bagaimana Amazon FSx untuk NetApp ONTAP bekerja dengan IAM

Sebelum Anda menggunakan IAM untuk mengelola akses ke Amazon FSx, pelajari fitur IAM apa yang tersedia untuk digunakan dengan Amazon FSx.

Fitur IAM yang dapat Anda gunakan dengan Amazon FSx untuk NetApp ONTAP

Fitur IAM	FSx Dukungan Amazon
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACLs	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Amazon FSx dan AWS layanan lainnya dengan sebagian besar fitur IAM, lihat [AWS layanan yang bekerja dengan IAM di Panduan Pengguna IAM](#).

Kebijakan berbasis identitas untuk Amazon 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. 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 Amazon FSx

Untuk melihat contoh kebijakan FSx berbasis identitas Amazon, lihat. [Contoh kebijakan berbasis identitas untuk Amazon untuk ONTAP FSx NetApp](#)

Kebijakan berbasis sumber daya di Amazon FSx

Mendukung kebijakan berbasis sumber daya: Tidak

Tindakan kebijakan untuk Amazon FSx

Mendukung tindakan kebijakan: Ya

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

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Sertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar FSx tindakan Amazon, lihat [Tindakan yang ditentukan oleh Amazon FSx](#) di Referensi Otorisasi Layanan.

Tindakan kebijakan di Amazon 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 FSx berbasis identitas Amazon, lihat. [Contoh kebijakan berbasis identitas untuk Amazon untuk ONTAP FSx NetApp](#)

Sumber daya kebijakan untuk Amazon FSx

Mendukung sumber daya kebijakan: Ya

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

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis FSx sumber daya Amazon dan jenisnya ARNs, lihat Sumber [daya yang ditentukan oleh Amazon FSx](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang ditentukan oleh Amazon](#). FSx

Untuk melihat contoh kebijakan FSx berbasis identitas Amazon, lihat. [Contoh kebijakan berbasis identitas untuk Amazon untuk ONTAP FSx NetApp](#)

Kunci kondisi kebijakan untuk Amazon FSx

Mendukung kunci kondisi kebijakan khusus layanan: Yes

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

Elemen `Condition` menentukan ketika pernyataan dieksekusi berdasarkan kriteria yang ditetapkan. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Untuk melihat daftar kunci FSx kondisi Amazon, lihat [Kunci kondisi untuk Amazon FSx](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh Amazon FSx](#).

Untuk melihat contoh kebijakan FSx berbasis identitas Amazon, lihat [Contoh kebijakan berbasis identitas untuk Amazon untuk ONTAP FSx NetApp](#)

Daftar kontrol akses (ACLs) di Amazon FSx

Mendukung ACLs: Tidak

Kontrol akses berbasis atribut (ABAC) dengan Amazon FSx

Mendukung ABAC (tanda dalam kebijakan): Ya

Kontrol akses berbasis atribut (ABAC) adalah strategi otorisasi yang menentukan izin berdasarkan atribut tanda. Anda dapat melampirkan tag ke entitas dan AWS sumber daya IAM, lalu merancang kebijakan ABAC untuk mengizinkan operasi saat tag prinsipal cocok dengan tag pada sumber daya.

Untuk mengendalikan akses berdasarkan tanda, berikan informasi tentang tanda di [elemen kondisi](#) dari kebijakan menggunakan kunci kondisi `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, atau `aws:TagKeys`.

Jika sebuah layanan mendukung ketiga kunci kondisi untuk setiap jenis sumber daya, nilainya adalah Ya untuk layanan tersebut. Jika suatu layanan mendukung ketiga kunci kondisi untuk hanya beberapa jenis sumber daya, nilainya adalah Parsial.

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

Untuk informasi selengkapnya tentang menandai FSx sumber daya Amazon, lihat [Menandai sumber daya Amazon FSx](#).

Untuk melihat contoh kebijakan berbasis identitas untuk membatasi akses ke sumber daya berdasarkan tag pada sumber daya tersebut, lihat [Menggunakan tag untuk mengontrol akses ke FSx sumber daya Amazon Anda](#).

Menggunakan kredensial Sementara dengan Amazon FSx

Mendukung kredensial sementara: Ya

Kredensi sementara menyediakan akses jangka pendek ke AWS sumber daya dan secara otomatis dibuat saat Anda menggunakan federasi atau beralih peran. AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensi sementara alih-alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#) dan [Layanan AWS yang berfungsi dengan IAM](#) dalam Panduan Pengguna IAM.

Teruskan sesi akses untuk Amazon FSx

Mendukung sesi akses terusan (FAS): Ya

Sesi akses terusan (FAS) menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses terusan](#).

Peran layanan untuk Amazon FSx

Mendukung peran layanan: Tidak

Peran terkait layanan untuk Amazon 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 peran FSx terkait layanan Amazon, lihat.

[Menggunakan peran terkait layanan untuk Amazon FSx](#)

Contoh kebijakan berbasis identitas untuk Amazon untuk ONTAP FSx NetApp

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi FSx sumber daya Amazon. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM.

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

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Amazon FSx, termasuk format ARNs untuk setiap jenis sumber daya, lihat [Kunci tindakan, sumber daya, dan kondisi untuk Amazon FSx](#) di Referensi Otorisasi Layanan.

Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan FSx konsol Amazon](#)
- [Mengizinkan pengguna melihat izin mereka sendiri](#)

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus FSx sumber daya Amazon di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi

selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan dengan IAM Access Analyzer](#) dalam Panduan Pengguna IAM.
- Memerlukan otentikasi multi-faktor (MFA) - Jika Anda memiliki skenario yang mengharuskan pengguna IAM atau pengguna root di Anda, Akun AWS aktifkan MFA untuk keamanan tambahan. Untuk meminta MFA ketika operasi API dipanggil, tambahkan kondisi MFA pada kebijakan Anda. Untuk informasi selengkapnya, lihat [Amankan akses API dengan MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan di IAM](#) dalam Panduan Pengguna IAM.

Menggunakan FSx konsol Amazon

Untuk mengakses konsol Amazon FSx untuk NetApp ONTAP, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang FSx sumber daya Amazon di Anda Akun AWS. Jika Anda membuat kebijakan berbasis identitas yang lebih ketat

daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

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

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan FSx konsol Amazon, lampirkan juga kebijakan `AmazonFSxConsoleReadOnlyAccess` AWS terkelola ke entitas. Untuk informasi selengkapnya, lihat [Menambah izin untuk pengguna](#) dalam Panduan Pengguna IAM.

Anda dapat melihat `AmazonFSxConsoleReadOnlyAccess` dan kebijakan layanan FSx terkelola Amazon lainnya di [AWS kebijakan terkelola untuk Amazon FSx untuk NetApp ONTAP](#).

Mengizinkan pengguna melihat izin mereka sendiri

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

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

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

Memecahkan masalah Amazon FSx untuk identitas dan akses NetApp ONTAP

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

Topik

- [Saya tidak berwenang untuk melakukan tindakan di Amazon FSx](#)
- [Saya tidak berwenang untuk melakukan iam: PassRole](#)
- [Saya ingin mengizinkan orang di luar saya Akun AWS mengakses FSx sumber daya Amazon saya](#)

Saya tidak berwenang untuk melakukan tindakan di Amazon 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 bahwa Anda tidak diizinkan untuk melakukan `iam:PassRole` tindakan, kebijakan Anda harus diperbarui agar Anda dapat meneruskan peran ke Amazon FSx.

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 di Amazon FSx. 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 mengakses FSx sumber daya Amazon saya

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

Untuk mempelajari selengkapnya, periksa referensi berikut:

- Untuk mengetahui apakah Amazon FSx mendukung fitur-fitur ini, lihat [Bagaimana Amazon FSx untuk NetApp ONTAP 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 peran terkait layanan untuk Amazon FSx

Amazon FSx menggunakan peran AWS Identity and Access Management [terkait layanan](#) (IAM). Peran terkait layanan adalah jenis peran IAM unik yang ditautkan langsung ke Amazon. FSx Peran terkait layanan telah ditentukan sebelumnya oleh Amazon FSx dan mencakup semua izin yang diperlukan layanan untuk memanggil AWS layanan lain atas nama Anda.

Peran terkait layanan membuat pengaturan Amazon FSx lebih mudah karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Amazon FSx mendefinisikan izin peran terkait layanannya, dan kecuali ditentukan lain, hanya Amazon yang FSx 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 FSx sumber daya Amazon Anda karena Anda tidak dapat secara tidak sengaja menghapus izin untuk mengakses sumber daya.

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 untuk Amazon FSx

Amazon FSx 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, dan menerbitkan sistem file dan metrik volume. CloudWatch

Untuk pembaruan kebijakan ini, silakan lihat [Amazon FSx ServiceRolePolicy](#).

Detail izin

Izin AWSService RoleForAmazon FSx peran ditentukan oleh kebijakan FSx ServiceRolePolicy AWS terkelola Amazon. Ini AWSService RoleForAmazon FSx memiliki izin berikut:

Note

AWSServiceRoleForAmazonFSx Ini digunakan oleh semua jenis sistem FSx file Amazon; beberapa izin yang terdaftar tidak berlaku FSx untuk ONTAP.

- **ds**— Memungkinkan Amazon FSx untuk melihat, mengotorisasi, dan tidak mengotorisasi aplikasi di direktori Anda. Directory Service
- **ec2**— Memungkinkan Amazon FSx 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.
 - Tetapkan IPv6 alamat ke antarmuka jaringan pelanggan yang memiliki `AmazonFSx.FileSystemId` tag.
 - Batalkan IPv6 alamat dari antarmuka jaringan pelanggan yang memiliki tag `AmazonFSx.FileSystemId`
 - 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 Amazon FSx mempublikasikan titik data metrik ke CloudWatch bawah FSx namespace AWS/.
- **route53**— Memungkinkan Amazon FSx untuk mengaitkan VPC Amazon dengan zona host pribadi.

JSON

```
{
  "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"
      }
    }
  }
]
```

Setiap pembaruan untuk kebijakan ini dijelaskan dalam [Amazon 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, lihat [Izin Peran Tertaut Layanan di Panduan](#) Pengguna IAM.

Membuat peran terkait layanan untuk Amazon FSx

Anda tidak perlu membuat peran terkait layanan secara manual. Saat Anda membuat sistem file di Konsol Manajemen AWS, IAM CLI, atau IAM API, FSx Amazon 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, Amazon FSx membuat peran terkait layanan untuk Anda lagi.

Mengedit peran terkait layanan untuk Amazon FSx

Amazon FSx tidak mengizinkan Anda mengedit peran `AWSService RoleForAmazon FSx` 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 untuk Amazon FSx

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 FSx layanan Amazon menggunakan peran saat Anda mencoba 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 `AWSServiceRoleForAmazonFSx`. Untuk informasi selengkapnya, lihat [Menghapus Peran Terkait Layanan](#) di Panduan Pengguna IAM.

Wilayah yang didukung untuk peran FSx terkait layanan Amazon

Amazon FSx mendukung penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi selengkapnya, lihat [AWS Wilayah dan Titik Akhir](#).

Menggunakan tag dengan Amazon FSx

Anda dapat menggunakan tag untuk mengontrol akses ke FSx sumber daya Amazon dan menerapkan kontrol akses berbasis atribut (ABAC). Untuk menerapkan tag ke FSx sumber daya Amazon selama pembuatan, pengguna harus memiliki izin AWS Identity and Access Management (IAM) tertentu.

Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat

Dengan beberapa tindakan FSx Amazon API yang membuat sumber daya, Anda dapat menentukan tag saat membuat sumber daya. Anda dapat menggunakan tag sumber daya ini untuk menerapkan kontrol akses berbasis atribut (ABAC). Untuk informasi lebih lanjut, lihat [Untuk apa ABAC? AWS](#) di Panduan Pengguna IAM.

Agar pengguna dapat menandai sumber daya pada pembuatan, mereka harus memiliki izin untuk menggunakan tindakan yang membuat sumber daya, seperti `fsx:CreateFileSystem`, `fsx:CreateStorageVirtualMachine`, atau `fsx:CreateVolume`. Jika tag ditentukan dalam tindakan pembuatan sumber daya, IAM melakukan otorisasi tambahan pada `fsx:TagResource` tindakan untuk memverifikasi apakah pengguna memiliki izin untuk membuat tag. Oleh karena itu, para pengguna juga harus memiliki izin eksplisit untuk menggunakan tindakan `fsx:TagResource`.

Contoh kebijakan berikut memungkinkan pengguna untuk membuat sistem file dan penyimpanan mesin virtual (SVMs) dan menerapkan tag untuk mereka selama pembuatan di tertentu Akun AWS.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:CreateStorageVirtualMachine",
        "fsx:TagResource"
      ],
      "Resource": [
        "arn:aws:fsx:region:account-id:file-system/*",
        "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
  ]
}
```

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/*"
}
]
```

`fsx:TagResource` tindakan dievaluasi hanya jika tag diterapkan selama tindakan pembuatan sumber daya. Oleh karena itu, pengguna yang memiliki izin untuk membuat sumber daya (dengan asumsi tidak ada kondisi penandaan) tidak memerlukan izin untuk menggunakan `fsx:TagResource` tindakan jika tidak ada tag 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, lihat [Menandai sumber daya Amazon FSx](#). Untuk informasi selengkapnya tentang penggunaan tag untuk mengontrol akses ke FSx sumber daya Amazon, lihat [Menggunakan 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 IAM berdasarkan tag. Anda dapat memberikan kontrol ini dengan dua cara:

- Anda dapat mengontrol akses ke FSx sumber daya Amazon berdasarkan tag pada sumber daya tersebut.
- Anda dapat mengontrol tag mana 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, lihat [Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat](#). Untuk informasi selengkapnya tentang menandai sumber daya, lihat [Menandai sumber daya Amazon FSx](#).

Mengontrol akses berdasarkan tag pada sumber daya

Untuk mengontrol tindakan 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 Contoh kebijakan - Buat sistem file hanya ketika tag tertentu digunakan

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 contoh - Buat cadangan hanya Amazon FSx untuk volume NetApp ONTAP dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat cadangan hanya FSx untuk volume ONTAP yang ditandai dengan pasangan nilai kunci, key=Department value=Finance Cadangan dibuat dengan tagDepartment=Finance.

JSON

```
{
  "Version": "2012-10-17",
```

```

    "Statement": [
      {
        "Effect": "Allow",
        "Action": [
          "fsx:CreateBackup"
        ],
        "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
        "Condition": {
          "StringEquals": {
            "aws:ResourceTag/Department": "Finance"
          }
        }
      },
      {
        "Effect": "Allow",
        "Action": [
          "fsx:TagResource",
          "fsx:CreateBackup"
        ],
        "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
        "Condition": {
          "StringEquals": {
            "aws:RequestTag/Department": "Finance"
          }
        }
      }
    ]
  }
}

```

Example Contoh kebijakan - Buat volume dengan tag tertentu dari cadangan dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat volume yang ditandai

Department=Finance hanya dari backup yang ditandai dengan. Department=Finance

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [

```



```

        "fsx:CreateVolumeFromBackup",
        "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateVolumeFromBackup"
    ],
    "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/Department": "Finance"
        }
    }
}
]
}

```

Example Contoh 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.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx>DeleteFileSystem"
      ],

```

```

    "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Department": "Finance"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/Department": "Finance"
      }
    }
  }
]
}

```

Example Contoh kebijakan - Hapus volume dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk menghapus hanya volume yang ditandai. Department=Finance Jika mereka membuat cadangan akhir, maka itu harus ditandai dengan Department=Finance.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx>DeleteVolume"
      ],
      "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
      "Condition": {
        "StringEquals": {

```

```

        "aws:ResourceTag/Department": "Finance"
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Department": "Finance"
        }
      }
    }
  ]
}

```

AWS kebijakan terkelola untuk Amazon FSx untuk NetApp ONTAP

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, pembaruan 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 untuk Amazon FSx](#) 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 untuk Amazon FSx](#).

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. 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. Konsol Manajemen AWS

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. 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).
- secretsmanager— Memungkinkan kepala sekolah untuk membuat daftar rahasia AWS Secrets Manager untuk memilih kredensial akun layanan bergabung dengan domain.
- iamMemberikan 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. Konsol Manajemen AWS

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 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
- secretsmanager— Memungkinkan kepala sekolah untuk membuat daftar rahasia AWS Secrets Manager untuk memilih kredensial akun layanan bergabung dengan domain.
- 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 untuk Amazon FSx untuk NetApp ONTAP](#).

Ubah	Deskripsi	Date
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>secretsmanager:ListSecrets</code> yang memungkinkan kepala sekolah untuk membuat daftar rahasia AWS Secrets Manager untuk memilih kredensial akun layanan bergabung dengan domain.	November 5, 2025
Amazon FSx ConsoleReadOnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>secretsmanager:ListSecrets</code> yang memungkinkan kepala sekolah untuk membuat daftar rahasia AWS Secrets Manager untuk memilih kredensial akun layanan bergabung dengan domain.	November 3, 2025
Amazon FSx ServiceRolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>ec2:AssignIpv6Addresses</code> yang memungkinkan prinsipal untuk menetapkan IPv6 alamat ke antarmuka jaringan pelanggan yang memiliki tag <code>AmazonFSx.FileSystemId</code>	Juli 22, 2025
Amazon FSx ServiceRolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>ec2:UnassignIpv6Addresses</code> yang	Juli 22, 2025

Ubah	Deskripsi	Date
	memungkinkan prinsipal untuk membatalkan penetapan IPv6 alamat dari antarmuka jaringan pelanggan yang memiliki tag. AmazonFSx .FileSystemId	
Amazon FSx ConsoleFu llAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, fsx:CreateAndAttachS3AccessPoint yang memungkinkan prinsipal untuk membuat titik akses S3 dan melampirkannya ke volume. FSx	Juni 25, 2025
Amazon FSx ConsoleFu llAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, fsx:DescribeS3AccessPointAttachments yang memungkinkan prinsipal untuk mencantumkan semua titik akses S3 dalam file. Akun AWS Wilayah AWS	Juni 25, 2025
Amazon FSx ConsoleFu llAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, fsx:DetachAndDeleteS3AccessPoint yang memungkinkan prinsipal untuk menghapus titik akses S3.	Juni 25, 2025

Ubah	Deskripsi	Date
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>fsx:CreateAndAttachS3AccessPoint</code> yang memungkinkan prinsipal untuk membuat titik akses S3 dan melampirkannya ke volume. FSx	Juni 25, 2025
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>fsx:DescribeS3AccessPointAttachments</code> yang memungkinkan prinsipal untuk mencantumkan semua titik akses S3 dalam file. Akun AWS Wilayah AWS	Juni 25, 2025
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>fsx:DetachAndDeleteS3AccessPoint</code> yang memungkinkan prinsipal untuk menghapus titik akses S3.	Juni 25, 2025
Amazon FSx ConsoleReadOnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>ec2:DescribeNetworkInterfaces</code> yang memungkinkan prinsipal untuk melihat antarmuka jaringan elastis yang terkait dengan sistem file mereka.	Februari 25, 2025

Ubah	Deskripsi	Date
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>ec2:DescribeNetworkInterfaces</code> yang memungkinkan prinsipal untuk melihat antarmuka jaringan elastis yang terkait dengan sistem file mereka.	Februari 07, 2025
Amazon FSx ServiceRolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>ec2:GetSecurityGroupsForVpc</code> 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, <code>ec2:GetSecurityGroupsForVpc</code> yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024

Ubah	Deskripsi	Date
Amazon FSx ConsoleReadOnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>ec2:GetSecurityGroupsForVpc</code> 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, <code>ec2:GetSecurityGroupsForVpc</code> 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, <code>ec2:GetSecurityGroupsForVpc</code> yang memungkinkan prinsipal untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.	Januari 9, 2024

Ubah	Deskripsi	Date
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
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

Ubah	Deskripsi	Date
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
AWS kebijakan terkelola : Amazon FSx ServiceRolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx memodifikasi <code>cloudwatch:PutMetricData</code> izin yang ada sehingga Amazon FSx menerbitkan CloudWatch metrik ke namespace. <code>AWS/FSx</code>	Juli 24, 2023
Amazon FSx FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx memperbarui kebijakan untuk menghapus <code>fsx:*</code> izin dan menambahkan <code>fsx</code> tindakan tertentu.	13 Juli 2023
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx memperbarui kebijakan untuk menghapus <code>fsx:*</code> izin dan menambahkan <code>fsx</code> tindakan tertentu.	13 Juli 2023

Ubah	Deskripsi	Date
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
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

Ubah	Deskripsi	Date
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 rute EC2 untuk panggilan down cakupan.	2 September 2021
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon membuat Amazon 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 rute EC2 untuk panggilan down cakupan.	2 September 2021

Ubah	Deskripsi	Date
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

Ubah	Deskripsi	Date
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

Ubah	Deskripsi	Date
Amazon FSx ConsoleFu llAccess - 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 ConsoleFu llAccess - 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

Ubah	Deskripsi	Date
Amazon FSx ConsoleRe adOnlyAccess - 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 ConsoleRe adOnlyAccess - 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

Kontrol Akses Sistem File dengan Amazon VPC

Anda mengakses Amazon FSx untuk sistem file NetApp ONTAP dan SVMs menggunakan nama DNS atau alamat IP dari salah satu titik akhir mereka, tergantung pada jenis aksesnya. Nama

DNS memetakan ke alamat IP pribadi dari sistem file atau elastic network interface SVM di VPC Anda. Hanya sumber daya dalam VPC terkait, atau sumber daya yang terhubung dengan VPC terkait oleh Direct Connect atau VPN, yang dapat mengakses data dalam sistem file Anda melalui protokol NFS, SMB, atau iSCSI. 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.

Grup keamanan Amazon VPC

Grup keamanan bertindak sebagai firewall virtual untuk sistem file ONTAP Anda FSx untuk mengontrol lalu lintas masuk dan keluar. Aturan masuk mengontrol lalu lintas masuk ke sistem file Anda, dan aturan keluar mengontrol lalu lintas keluar dari sistem file Anda. Saat Anda membuat sistem file, Anda menentukan VPC tempat pembuatannya, dan grup keamanan default untuk VPC tersebut diterapkan. Anda dapat menambahkan aturan ke setiap grup keamanan yang memungkinkan lalu lintas ke atau dari sistem file terkait dan SVMs. Anda dapat melakukan modifikasi terhadap aturan-aturan untuk grup keamanan kapan saja. Aturan baru dan yang dimodifikasi secara otomatis diterapkan ke semua sumber daya yang terkait dengan grup keamanan. Ketika Amazon FSx memutuskan apakah akan mengizinkan lalu lintas untuk mencapai sumber daya, Amazon mengevaluasi semua aturan dari semua kelompok keamanan yang terkait dengan sumber daya.

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 ke sistem file Amazon Anda ke folder pada instance komputasi yang didukung.

Untuk informasi selengkapnya tentang aturan grup [keamanan](#), lihat [Aturan Grup Keamanan](#) di Panduan Pengguna Amazon EC2.

Membuat grup keamanan VPC

Untuk membuat grup keamanan untuk Amazon FSx

1. [Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2](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. Untuk aturan keluar, izinkan semua lalu lintas di semua port.
7. Tambahkan aturan berikut ke port masuk grup keamanan Anda. Untuk bidang sumber, Anda harus memilih Kustom dan masukkan grup keamanan atau rentang alamat IP yang terkait dengan instance yang perlu mengakses sistem file ONTAP Anda FSx , termasuk:
 - Linux, Windows, klien and/or macOS yang mengakses data dalam sistem file Anda melalui NFS, SMB, atau iSCSI.
 - File ONTAP apa pun systems/clusters yang akan Anda peer ke sistem file Anda (misalnya, untuk digunakan, SnapMirror SnapVault, atau FlexCache).
 - Setiap klien yang akan Anda gunakan untuk mengakses ONTAP REST API, CLI, ZAPIs atau (misalnya, instance, Harvest/Grafana Connector NetApp , NetApp atau Console).

Protokol	Port	Peran
Semua ICMP	Semua	Ping pada instance
SSH	22	Akses SSH ke alamat IP LIF manajemen cluster atau LIF manajemen node
TCP	111	Panggilan prosedur jarak jauh untuk NFS
TCP	135	Panggilan prosedur jarak jauh untuk CIFS
TCP	139	Sesi layanan NetBIOS untuk CIFS
TCP	161-162	Protokol manajemen jaringan sederhana (SNMP)

Protokol	Port	Peran
TCP	443	ONTAP REST API akses ke alamat IP LIF manajemen cluster atau LIF manajemen SVM
TCP	445	Microsoft SMB/CIFS melalui TCP dengan pembungkian NetBIOS
TCP	635	Dudukan NFS
TCP	749	Kerberos
TCP	2049	Daemon server NFS
TCP	3260	Akses iSCSI melalui LIF data iSCSI
TCP	4045	Daemon kunci NFS
TCP	4046	Monitor status jaringan untuk NFS
TCP	10000	Protokol manajemen data jaringan (NDMP) dan komunikasi intercluster NetApp SnapMirror
TCP	11104	Manajemen komunikasi NetApp SnapMirror antar kluster
TCP	11105	SnapMirror transfer data menggunakan intercluster LIFs
UDP	111	Panggilan prosedur jarak jauh untuk NFS
UDP	135	Panggilan prosedur jarak jauh untuk CIFS
UDP	137	Resolusi nama NetBIOS untuk CIFS
UDP	139	Sesi layanan NetBIOS untuk CIFS
UDP	161-162	Protokol manajemen jaringan sederhana (SNMP)
UDP	635	Dudukan NFS

Protokol	Port	Peran
UDP	2049	Daemon server NFS
UDP	4045	Daemon kunci NFS
UDP	4046	Monitor status jaringan untuk NFS
UDP	4049	Protokol kuota NFS

8. Tambahkan grup keamanan ke elastic network interface sistem file.

Larang akses ke sistem file

Untuk sementara melarang akses jaringan ke sistem file Anda dari semua klien, Anda dapat menghapus semua grup keamanan yang terkait dengan elastic network interface (s) sistem file Anda dan menggantinya dengan grup yang tidak memiliki inbound/outbound aturan.

Validasi Kepatuhan untuk Amazon FSx untuk NetApp ONTAP

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. Untuk informasi selengkapnya tentang tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS, lihat [Dokumentasi AWS Keamanan](#).

Amazon FSx untuk NetApp ONTAP dan antarmuka titik akhir VPC ()AWS PrivateLink

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. 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 ONTAP 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 dua Anda sendiri 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 VPC dipeer, sumber daya seperti Amazon Elastic Compute Cloud (Amazon EC2) instans di keduanya dapat VPCs 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 `AWSfsx.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 mengontrol akses ke Amazon FSx API, Anda dapat melampirkan kebijakan AWS Identity and Access Management (IAM) ke titik akhir VPC Anda. Kebijakan menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat [Mengontrol Akses ke Layanan dengan titik akhir VPC](#) dalam Panduan Pengguna Amazon VPC.

Ketahanan di Amazon FSx untuk ONTAP NetApp

Infrastruktur AWS global dibangun di sekitar Wilayah AWS dan Availability Zones. Wilayah AWS menyediakan beberapa Availability Zone yang terpisah secara fisik dan terisolasi, yang terhubung dengan latensi rendah, throughput tinggi, dan jaringan yang sangat redundan. Dengan Zona Ketersediaan, Anda dapat merancang serta mengoperasikan aplikasi dan basis data

yang secara otomatis melakukan fail over di antara zona tanpa gangguan. Zona Ketersediaan memiliki ketersediaan dan toleransi kesalahan yang lebih baik, dan dapat diskalakan dibandingkan infrastruktur pusat data tunggal atau multi tradisional.

Untuk informasi selengkapnya tentang Wilayah AWS dan Availability Zone, lihat [Infrastruktur AWS Global](#).

Selain infrastruktur AWS global, Amazon FSx menawarkan beberapa fitur untuk membantu mendukung ketahanan data dan kebutuhan cadangan Anda.

Pencadangan dan pemulihan

Amazon FSx membuat dan menyimpan cadangan otomatis volume di Amazon Anda FSx untuk sistem file NetApp ONTAP. Amazon FSx membuat cadangan otomatis volume Anda selama jendela cadangan Amazon Anda FSx untuk sistem file NetApp ONTAP. Amazon FSx menyimpan cadangan otomatis volume Anda sesuai dengan periode retensi cadangan yang Anda tentukan. Anda juga dapat mencadangkan volume Anda secara manual, dengan membuat cadangan yang diprakarsai pengguna. Anda mengembalikan cadangan volume kapan saja dengan membuat volume baru dengan cadangan yang ditentukan sebagai sumbernya.

Untuk informasi selengkapnya, lihat [Melindungi data Anda dengan backup volume](#).

Snapshot

Amazon FSx membuat salinan snapshot Amazon FSx untuk volume NetApp ONTAP. Salinan snapshot menawarkan perlindungan terhadap penghapusan atau modifikasi file yang tidak disengaja dalam volume Anda oleh pengguna akhir. Untuk informasi selengkapnya, lihat [Melindungi data Anda dengan snapshot](#).

Zona Ketersediaan

Amazon FSx untuk sistem file NetApp ONTAP dirancang untuk menyediakan ketersediaan data yang berkelanjutan bahkan jika server gagal. Setiap sistem file didukung oleh dua server file di setidaknya satu Availability Zone, masing-masing dengan penyimpanannya sendiri. Amazon FSx secara otomatis mereplikasi data Anda untuk melindunginya dari kegagalan komponen, terus memantau kegagalan perangkat keras, dan secara otomatis mengganti komponen infrastruktur jika terjadi kegagalan. Sistem file secara otomatis gagal berulang-ulang sesuai kebutuhan (biasanya dalam 60 detik), dan klien secara otomatis gagal berulang-ulang dengan sistem file.

Sistem file multi-AZ

Amazon FSx untuk sistem file NetApp ONTAP sangat tersedia dan tahan lama di seluruh AWS Availability Zone, dan dirancang untuk menyediakan ketersediaan data yang berkelanjutan bahkan jika Availability Zone tidak tersedia.

Untuk informasi selengkapnya, lihat [Opsional ketersediaan, daya tahan, dan penerapan](#).

Sistem file single-AZ

Amazon FSx untuk sistem file NetApp ONTAP sangat tersedia dan tahan lama dalam satu AWS Availability Zone, dan dirancang untuk menyediakan ketersediaan berkelanjutan dalam Availability Zone tersebut jika terjadi server file individual atau kegagalan disk.

Untuk informasi selengkapnya, lihat [Opsional ketersediaan, daya tahan, dan penerapan](#).

Keamanan infrastruktur di Amazon FSx untuk NetApp ONTAP

Sebagai layanan terkelola, Amazon FSx untuk NetApp ONTAP dilindungi oleh keamanan jaringan AWS global. Untuk informasi tentang layanan AWS keamanan dan cara AWS melindungi infrastruktur, lihat [Keamanan AWS Cloud](#). Untuk mendesain AWS lingkungan Anda menggunakan praktik terbaik untuk keamanan infrastruktur, lihat [Perlindungan Infrastruktur dalam Kerangka Kerja](#) yang AWS Diarsiteksikan dengan Baik Pilar Keamanan.

Anda menggunakan panggilan API yang AWS dipublikasikan untuk mengakses Amazon FSx melalui jaringan. Klien harus mendukung hal-hal berikut:

- Keamanan Lapisan Pengangkutan (TLS). Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Sandi cocok dengan sistem kerahasiaan maju sempurna (perfect forward secrecy, PFS) seperti DHE (Ephemeral Diffie-Hellman) atau ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini.

Gunakan NetApp ONTAP Vscan dengan FSx untuk ONTAP

Anda dapat menggunakan fitur NetApp ONTAP's Vscan untuk menjalankan perangkat lunak antivirus pihak ketiga yang didukung. Untuk informasi selengkapnya, lihat sumber daya berikut untuk setiap solusi yang didukung.

- Deep Instinct - [Solusi mitra Vscan](#) dan dokumentasi [Deep Instinct](#) 1

- SentinelOne — [Solusi mitra Vscan](#) dan [SentinelOne Singularity](#) Cloud Data Security
- [Symantec - Solusi mitra Vscan dan Mesin Perlindungan Symantec](#)
- [Trellix \(sebelumnya McAfee\) — Solusi mitra Vscan dan Dokumen Produk Trellix](#)
- Trend Micro - [solusi mitra Vscan](#)

Note

¹ Anda harus masuk ke portal Deep Instinct untuk melihat dokumentasi mereka.

ONTAPperan dan pengguna

NetApp ONTAP mencakup kemampuan kontrol akses berbasis peran (RBAC) yang kuat dan dapat diperluas. ONTAPperan menentukan kemampuan dan hak istimewa pengguna saat menggunakan ONTAP CLI dan REST API. Setiap peran mendefinisikan tingkat kemampuan administratif dan hak istimewa yang berbeda. Anda menetapkan peran kepada pengguna untuk tujuan mengontrol akses mereka ke FSx sumber daya ONTAP saat menggunakan ONTAP REST API dan CLI. Ada ONTAP peran yang tersedia secara terpisah FSx untuk pengguna sistem file ONTAP dan pengguna mesin virtual penyimpanan (SVM).

Saat Anda membuat sistem file FSx untuk ONTAP, ONTAP pengguna default dibuat di tingkat sistem file dan di tingkat SVM. Anda dapat membuat sistem file tambahan dan pengguna SVM, dan Anda dapat membuat peran SVM tambahan untuk memenuhi kebutuhan organisasi Anda. Bab ini menjelaskan ONTAP pengguna dan peran, dan menyediakan prosedur terperinci untuk membuat pengguna tambahan dan peran SVM.

Peran administrator sistem file dan pengguna

Pengguna sistem ONTAP file default adalah `fsxadmin`, yang memiliki `fsxadmin` peran yang ditetapkan untuk itu. Ada dua peran standar yang dapat Anda tetapkan untuk pengguna sistem file, yang tercantum sebagai berikut:

- **fsxadmin** Administrator dengan peran ini memiliki hak yang tidak terbatas dalam sistem. ONTAP Mereka dapat mengkonfigurasi semua sistem file dan sumber daya tingkat SVM yang tersedia FSx untuk sistem file ONTAP.
- **fsxadmin-readonly**—Administrator dengan peran ini dapat melihat semuanya di tingkat sistem file tetapi tidak dapat membuat perubahan apa pun.

Peran ini sangat cocok untuk digunakan dengan aplikasi pemantauan seperti NetApp Harvest karena memiliki akses hanya-baca ke semua sumber daya yang tersedia dan propertinya, tetapi tidak dapat membuat perubahan apa pun padanya.

Anda dapat membuat pengguna sistem file tambahan dan menetapkan mereka baik `fsxadmin-readonly` peran `fsxadmin` atau. Anda tidak dapat membuat peran baru atau memodifikasi peran yang ada. Untuk informasi selengkapnya, lihat [Membuat ONTAP pengguna baru untuk sistem file dan administrasi SVM](#).

Tabel berikut menjelaskan tingkat akses yang dimiliki peran administrator sistem file untuk perintah ONTAP CLI dan REST API dan direktori perintah.

Nama peran	Tingkat akses	Untuk perintah atau direktori perintah berikut
<code>fsxadmin</code>	<code>all</code>	Semua direktori perintah tersedia FSx untuk ONTAP
<code>fsxadmin-readonly</code>	<code>all</code>	<code>security login password</code> Untuk mengelola akun pengguna sendiri kata sandi lokal dan informasi kunci saja
	<code>none</code>	<code>security</code>
	<code>hanya-baca</code>	Semua direktori perintah lainnya tersedia FSx untuk ONTAP

Peran administrator SVM dan pengguna

Setiap SVM memiliki domain otentikasi terpisah dan dapat dikelola secara independen oleh administratornya sendiri. Untuk setiap SVM di sistem file Anda, pengguna default adalah `vsadmin`, yang memiliki `vsadmin` peran yang ditetapkan secara default. Selain `vsadmin` peran, ada peran SVM standar lainnya yang memberikan izin cakupan bawah yang dapat Anda tetapkan ke pengguna

SVM. Anda juga dapat membuat peran khusus yang menyediakan tingkat kontrol akses yang memenuhi kebutuhan organisasi Anda.

Peran yang telah ditentukan untuk administrator SVM dan kemampuannya adalah sebagai berikut:

Nama peran	Kemampuan
vsadmin	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Kelola volume, kecuali untuk pergerakan volume • Kelola kuota, qtrees, salinan Snapshot, dan file • Kelola LUNs • Lakukan SnapLock operasi, kecuali untuk penghapusan hak istimewa • Konfigurasi protokol: NFS, SMB, dan iSCSI • Konfigurasi layanan: DNS, LDAP, dan NIS • Pantau pekerjaan • Pantau koneksi jaringan dan antarmuka jaringan • Pantau kesehatan SVM
vsadmin-volume	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Kelola volume, termasuk pergerakan volume • Kelola kuota, qtrees, salinan Snapshot, dan file • Kelola LUNs • Konfigurasi protokol: NFS, SMB, dan iSCSI • Konfigurasi layanan: DNS, LDAP, dan NIS • Pantau antarmuka jaringan

Nama peran	Kemampuan
	• Pantau kesehatan SVM
<code>vsadmin-protocol</code>	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Kelola LUNs • Konfigurasi protokol: NFS, SMB, dan iSCSI • Konfigurasi layanan: DNS, LDAP, dan NIS • Monitor antarmuka jaringan • Pantau kesehatan SVM
<code>vsadmin-backup</code>	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Kelola operasi NDMP • Buat volume baca/tulis yang dipulihkan • Mengelola SnapMirror hubungan dan salinan Snapshot • Lihat volume dan informasi jaringan
<code>vsadmin-snaplock</code>	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Kelola volume, kecuali untuk pergerakan volume • Kelola kuota, qtrees, salinan Snapshot, dan file • Lakukan SnapLock operasi, termasuk penghapusan hak istimewa • Konfigurasi protokol: NFS dan SMB • Konfigurasi layanan: DNS, LDAP, dan NIS • Pantau pekerjaan • Pantau koneksi jaringan dan antarmuka jaringan

Nama peran	Kemampuan
vsadmin-readonly	• Mengelola akun pengguna Anda, kata sandi lokal, dan informasi kunci • Pantau kesehatan SVM • Pantau antarmuka jaringan • Lihat volume dan LUNs • Lihat layanan dan protokol

Untuk informasi selengkapnya tentang cara membuat peran SVM baru, lihat [Membuat peran SVM](#).

Menggunakan Active Directory untuk mengautentikasi pengguna ONTAP

Anda dapat mengautentikasi akses pengguna domain Windows Active Directory ke sistem file FSx untuk ONTAP dan SVM. Anda harus melakukan tugas-tugas berikut sebelum akun Active Directory dapat mengakses sistem file Anda:

- Anda perlu mengkonfigurasi akses pengontrol domain Active Directory ke SVM.

SVM yang Anda gunakan untuk mengonfigurasi sebagai gateway atau terowongan untuk akses pengontrol domain Active Directory harus mengaktifkan CIFS, digabungkan ke Active Directory, atau keduanya. Jika Anda tidak mengaktifkan CIFS dan hanya bergabung dengan terowongan SVM ke Active Directory, pastikan SVM bergabung dengan Active Directory Anda. Untuk informasi selengkapnya, lihat [Cara kerja bergabung SVMs ke Microsoft Active Directory](#).

- Anda perlu mengaktifkan akun pengguna domain Active Directory untuk mengakses sistem file.

Anda dapat menggunakan otentikasi kata sandi atau otentikasi kunci publik SSH untuk pengguna domain Windows yang mengakses ONTAP CLI atau REST API.

Untuk prosedur yang menjelaskan cara menggunakan untuk mengonfigurasi otentikasi Active Directory untuk sistem file dan administrator SVM, lihat [Mengkonfigurasi otentikasi Active Directory untuk pengguna ONTAP](#)

Membuat ONTAP pengguna baru untuk sistem file dan administrasi SVM

Setiap ONTAP pengguna dikaitkan dengan SVM atau sistem file. Pengguna sistem file dengan `fsxadmin` peran dapat membuat peran dan pengguna SVM baru dengan menggunakan perintah [security login create](#) ONTAP CLI.

`security login create` Perintah membuat metode login untuk utilitas manajemen. Metode login terdiri dari nama pengguna, aplikasi (metode akses), dan metode otentikasi. Nama pengguna dapat dikaitkan dengan beberapa aplikasi. Secara opsional dapat menyertakan nama peran kontrol akses. Jika nama grup Active Directory, LDAP, atau NIS digunakan, maka metode login memberikan akses ke pengguna yang termasuk dalam grup yang ditentukan. Jika pengguna adalah anggota dari beberapa grup yang disediakan dalam tabel login keamanan, maka pengguna akan mendapatkan akses ke daftar gabungan perintah yang diotorisasi untuk masing-masing grup.

Untuk informasi yang menjelaskan cara membuat ONTAP pengguna baru, lihat [Membuat ONTAP pengguna](#).

Topik

- [Membuat ONTAP pengguna](#)
- [Membuat peran SVM](#)
- [Mengkonfigurasi otentikasi Active Directory untuk pengguna ONTAP](#)
- [Mengkonfigurasi otentikasi kunci publik](#)
- [Memperbarui persyaratan kata sandi untuk sistem file dan peran SVM](#)
- [Gagal memperbarui kata sandi fsxadmin akun](#)

Membuat ONTAP pengguna

Untuk membuat SVM baru atau pengguna sistem file (ONTAP CLI)

Hanya pengguna sistem file dengan `fsxadmin` peran yang dapat membuat SVM baru dan pengguna sistem file.

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

- Gunakan perintah `security login create` ONTAP CLI untuk membuat akun pengguna baru di sistem file ONTAP atau SVM Anda FSx .

Masukkan data Anda untuk placeholder dalam contoh untuk menentukan properti wajib berikut:

- `-vserver`— Menentukan nama SVM di mana Anda ingin membuat peran SVM baru atau pengguna. Jika Anda membuat peran sistem file atau pengguna, jangan tentukan SVM.
- `-user-or-group-name`- Menentukan nama pengguna atau nama grup Active Directory dari metode login. Nama grup Active Directory hanya dapat ditentukan dengan metode domain otentikasi dan ssh aplikasi ontapi dan.
- `-application`- Menentukan penerapan metode login. Nilai yang mungkin termasuk http, ontapi, dan ssh.
- `-authentication-method`- Menentukan metode otentikasi untuk login. Kemungkinan nilainya mencakup berikut ini:
 - `domain` — Gunakan untuk otentikasi Active Directory
 - `kata sandi` - Gunakan untuk otentikasi kata sandi
 - `publickey` — Pengguna untuk otentikasi kunci publik
- `-role`- Menentukan nama peran akses-kontrol untuk metode login. Pada tingkat sistem file, satu-satunya peran yang dapat ditentukan adalah. `fsxadmin`

(Opsional) Anda juga dapat menggunakan satu atau lebih parameter berikut dengan perintah:

- `[-comment]`— Gunakan untuk menyertakan notasi atau komentar untuk akun pengguna. Misalnya, **Guest account**. Panjang maksimum adalah 128 karakter.
- `[-second-authentication-method {none|publickey|password|nsswitch}]`- Menentukan metode otentikasi faktor kedua. Anda dapat menentukan metode berikut:
 - `kata sandi` - Gunakan untuk otentikasi kata sandi
 - `publickey` — Gunakan untuk otentikasi Public-key
 - `nsswitch` - Gunakan untuk otentikasi NIS atau LDAP
 - `none` - Nilai default jika Anda tidak menentukan satu

```
Fsx0123456::> security login create -vserver vserver_name -user-or-group-name user_or_group_name -application login_application -authentication-method auth_method -role role_or_account_name
```

Perintah berikut membuat pengguna sistem file baru new_fsxadmin dengan fsxadmin-readonly peran yang ditetapkan, menggunakan SSH dengan kata sandi untuk masuk. Saat diminta, berikan kata sandi untuk pengguna.

```
Fsx0123456::> security login create -user-or-group-name new_fsxadmin -application ssh -authentication-method password -role fsxadmin-readonly
```

```
Please enter a password for user 'new_fsxadmin':  
Please enter it again:
```

```
Fsx0123456::>
```

- Perintah berikut membuat pengguna SVM baru new_vsadmin di fsx SVM dengan vsadmin_readonly peran, dikonfigurasi untuk menggunakan SSH dengan kata sandi untuk masuk. Saat diminta, berikan kata sandi untuk pengguna.

```
Fsx0123456::> security login create -vserver fsx -user-or-group-name new_vsadmin -application ssh -authentication-method password -role vsadmin-readonly
```

```
Please enter a password for user 'new_vsadmin':  
Please enter it again:
```

```
Fsx0123456::>
```

- Perintah berikut membuat pengguna sistem file read-only baru harvest2-user yang akan digunakan oleh aplikasi NetApp Harvest untuk mengumpulkan metrik kinerja dan kapasitas. Untuk informasi selengkapnya, lihat [Pemantauan FSx untuk sistem file ONTAP menggunakan Harvest dan Grafana](#).

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application ssh -role fsxadmin-readonly -authentication-method password
```

Untuk melihat informasi untuk semua sistem file dan pengguna SVM

- Gunakan perintah berikut untuk melihat semua informasi login untuk sistem file Anda dan SVMs.

```
Fsx0123456::> security login show
```

```
Vserver: Fsx0123456
```

User/Group Name	Application	Authentication Method	Role Name	Acct Locked	Second Authentication Method
autosupport	console	password	autosupport	no	none
fsxadmin	http	password	fsxadmin	no	none
fsxadmin	ontapi	password	fsxadmin	no	none
fsxadmin	ssh	password	fsxadmin	no	none
fsxadmin	ssh	publickey	fsxadmin	-	none
new_fsxadmin	ssh	password	fsxadmin-readonly	no	none

```
Vserver: fsx
```

User/Group Name	Application	Authentication Method	Role Name	Acct Locked	Second Authentication Method
new_vsadmin	ssh	password	vsadmin-readonly	no	none
vsadmin	http	password	vsadmin	yes	none
vsadmin	ontapi	password	vsadmin	yes	none
vsadmin	ssh	password	vsadmin	yes	none

```
10 entries were displayed.
```

```
Fsx0123456::>
```

Membuat peran SVM

Setiap SVM yang Anda buat memiliki administrator SVM default yang menetapkan peran yang telah ditentukan sebelumnya `vsadmin`. Selain set peran SVM yang [telah ditentukan, Anda dapat membuat peran SVM](#) baru. Jika Anda perlu membuat peran baru untuk SVM Anda, gunakan perintah `security login role create ONTAP CLI`. Perintah ini tersedia untuk administrator sistem file dengan `fsxadmin` peran.

Untuk membuat peran SVM baru (ONTAP CLI)

1. Anda dapat membuat peran SVM baru menggunakan [security login role create](#) ONTAP CLI perintah:

```
Fsx0123456::> security login role create -vserver vs1.example.com -role vol_role -
cmddirname volume
```

2. Tentukan parameter yang diperlukan berikut dalam perintah:
 - **-vserver**nama SVM
 - **-role**- Nama peran.
 - **-cmddirname**— Direktori perintah atau perintah tempat peran memberikan akses. Lampirkan nama subdirektori perintah dalam tanda kutip ganda. Misalnya, "volume snapshot". Masukkan DEFAULT untuk menentukan semua direktori perintah.
3. (Opsional) Anda juga dapat menambahkan salah satu parameter berikut ke perintah:
 - **-vserver**— Nama SVM yang terkait dengan peran tersebut.
 - **-access**— Tingkat akses untuk peran tersebut. Untuk direktori perintah, ini termasuk:
 - **none**— Menolak akses ke perintah di direktori perintah. Ini adalah nilai default untuk peran kustom.
 - **readonly**— Memberikan akses ke perintah show di direktori perintah dan subdirektornya.
 - **all**— Memberikan akses ke semua perintah di direktori perintah dan subdirektornya. Untuk memberikan atau menolak akses ke perintah intrinsik, Anda harus menentukan direktori perintah.

Untuk perintah non-intrinsik (perintah yang tidak berakhir dengan `create`, `modify`, `delete`, atau `show`):

- **none**— Menolak akses ke perintah di direktori perintah. Ini adalah nilai default untuk peran kustom.
- **readonly**- Tidak berlaku. Jangan gunakan.
- **all**— Memberikan akses ke perintah.
- **-query**— Objek query yang digunakan untuk memfilter tingkat akses, yang ditentukan dalam bentuk opsi yang valid untuk perintah, atau untuk perintah di direktori perintah. Lampirkan objek kueri dalam tanda kutip ganda.

4. Jalankan perintah `security login role create`.

Perintah berikut membuat peran kontrol akses bernama “admin” untuk vs1.example.com Vserver. Peran memiliki semua akses ke perintah “volume” tetapi hanya dalam agregat “aggr0”.

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-aggr aggr0" -access all -vserver vs1.example.com
```

Mengkonfigurasi otentikasi Active Directory untuk pengguna ONTAP

Gunakan ONTAP CLI untuk mengonfigurasi penggunaan otentikasi Active Directory untuk sistem ONTAP file dan pengguna SVM.

Anda harus menjadi administrator sistem file dengan fsxadmin peran untuk menggunakan perintah dalam prosedur ini.

Untuk mengatur otentikasi Active Directory untuk ONTAP pengguna (ONTAPCLI)

Perintah dalam prosedur ini tersedia untuk pengguna sistem file dengan fsxadmin peran tersebut.

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. Gunakan [security login domain-tunnel create](#) perintah seperti yang ditunjukkan untuk membuat terowongan domain untuk mengautentikasi pengguna Windows Active Directory. Ganti *svm_name* dengan nama SVM yang Anda gunakan untuk terowongan domain.

```
FsxId0123456::> security login domain-tunnel create -vserver svm_name
```

3. Gunakan [security login create](#) perintah untuk membuat akun pengguna domain Active Directory yang akan mengakses sistem file.

Tentukan parameter yang diperlukan berikut dalam perintah:

- **-vserver**— Nama SVM dikonfigurasi dengan CIFS dan bergabung dengan Active Directory Anda. Ini akan digunakan sebagai terowongan untuk mengautentikasi pengguna domain Active Directory ke sistem file. yang peran atau pengguna baru akan dibuat.
- **-user-or-group-name**— Nama pengguna atau nama grup Direktori Aktif dari metode login. Nama grup Active Directory hanya dapat ditentukan dengan metode domain otentikasi dan ontapi dan ssh aplikasi.
- **-application**— Penerapan metode login. Nilai yang mungkin termasuk http, ontapi, dan ssh.
- **-authentication-method**— Metode otentikasi yang digunakan untuk login. Kemungkinan nilainya mencakup berikut ini:
 - **domain** — untuk otentikasi Active Directory
 - **kata sandi** - untuk otentikasi kata sandi
 - **publickey** — untuk otentikasi kunci publik
- **-role**— Nama peran kontrol akses untuk metode login. Pada tingkat sistem file, satu-satunya peran yang dapat ditentukan adalah. **-role fsxadmin**

Contoh berikut membuat akun pengguna domain Active Directory CORP\Admin untuk sistem filesystem1 file.

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
application ssh -authmethod domain -role fsxadmin
```

Contoh berikut membuat akun CORP\Admin pengguna dengan otentikasi kunci publik.

```
FsxId0123456ab::> security login create -user-or-group-name "CORP\Admin" -
application ssh -authentication-method publickey -role fsxadmin
Warning: To use public-key authentication, you must create a public key for user
"CORP\Admin".
```

Buat kunci publik untuk CORP\Admin pengguna menggunakan perintah berikut:

```
FsxId0123456ab::> security login publickey create -username "CORP
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=
cwaltham@b0be837a91bf.ant.amazon.com"
```


Untuk masuk ke sistem file menggunakan SSH dengan kredensial Active Directory

- Contoh berikut menunjukkan bagaimana SSH ke dalam sistem file Anda dengan kredensial Active Directory Anda jika Anda memilih ssh untuk jenis. -application Ada username dalam format "domain-name\user-name", yang merupakan nama domain dan nama pengguna yang Anda berikan saat membuat akun, dipisahkan oleh garis miring terbalik dan dilampirkan dalam kutipan.

```
Fsx0123456: :> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
```

Saat diminta memasukkan kata sandi, gunakan kata sandi pengguna Active Directory.

Mengkonfigurasi otentikasi kunci publik

Untuk mengaktifkan otentikasi kunci publik SSH, Anda harus terlebih dahulu membuat kunci SSH dan mengaitkannya dengan akun administrator dengan menggunakan perintah. `security login publickey create` Ini memungkinkan akun untuk mengakses SVM. `security login publickey create` Perintah menerima parameter berikut.

Parameter	Deskripsi
<code>-vserver</code> (Opsional)	Nama SVM yang diakses akun. Jika Anda mengonfigurasi otentikasi kunci publik SSH untuk pengguna sistem file, jangan sertakan. <code>-versver</code>
<code>-username</code>	Nama pengguna akun. Nilai default, <code>admin</code> , adalah nama default administrator cluster.
<code>-index</code>	Nomor indeks kunci publik. Nilai default adalah 0 jika kunci adalah kunci pertama yang dibuat untuk akun. Jika tidak, nilai default adalah satu lebih dari nomor indeks tertinggi yang ada untuk akun.
<code>-publickey</code>	Kunci publik OpenSSH. Lampirkan kunci dalam tanda kutip ganda.

Parameter	Deskripsi
<code>-role</code>	Peran kontrol akses yang ditetapkan ke akun.
<code>-comment</code> (Opsional)	Teks deskriptif untuk kunci publik. Lampirkan teks dalam tanda kutip ganda.

Contoh berikut mengaitkan kunci publik dengan akun administrator SVM `svmadmin` untuk SVM `svm01`. Kunci publik diberi nomor indeks 5.

```
FSx0123456::> security login publickey create -vserver svm01 -username svmadmin
-index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAsPH64CYbUsDQCdW22JnK6J/
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5LUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMLPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

Important

Anda harus menjadi SVM atau administrator sistem file untuk melakukan tugas ini.

Memperbarui persyaratan kata sandi untuk sistem file dan peran SVM

Anda dapat memperbarui persyaratan kata sandi untuk sistem file atau peran SVM menggunakan perintah `security login role config modify` ONTAP CLI. Perintah ini hanya tersedia untuk akun administrator sistem file dengan `fsxadmin` peran. Saat memodifikasi persyaratan kata sandi, sistem akan memperingatkan jika ada pengguna yang ada dengan peran itu yang akan terpengaruh oleh perubahan tersebut.

Contoh berikut memodifikasi persyaratan kata sandi panjang minimum menjadi 12 karakter untuk pengguna dengan `vsadmin-readonly` peran pada `fsx` SVM. Dalam contoh ini, ada pengguna yang sudah ada dengan peran ini.

```
FSxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

Sistem menampilkan peringatan berikut karena pengguna yang ada:

```
Warning: User accounts with this role exist. Modifications to the username/password
restrictions on this role could result in non-compliant user
accounts.
```

```
Do you want to continue? {y|n}:
```

```
FsxId0123456::>
```

Gagal memperbarui kata sandi **fsxadmin** akun

Saat memperbarui kata sandi untuk **fsxadmin** pengguna, Anda mungkin menerima kesalahan jika tidak memenuhi persyaratan kata sandi yang ditetapkan pada sistem file. Anda dapat melihat persyaratan kata sandi dengan menggunakan perintah `security login role config show` ONTAP CLI atau REST API.

Untuk melihat persyaratan kata sandi untuk sistem file atau peran SVM

1. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

2. `security login role config show` Perintah mengembalikan persyaratan kata sandi untuk sistem file atau peran SVM.

```
FsxId0123456::> security login role config show -role fsxadmin -
fields password_requirement_fields
```

Untuk `-fields` parameter, tentukan salah satu atau semua hal berikut:

- `passwd-minlength`— Panjang minimum kata sandi.
- `passwd-min-special-chars`— Jumlah minimum karakter khusus dalam kata sandi.
- `passwd-min-lowercase-chars`— Jumlah minimum karakter huruf kecil dalam kata sandi.
- `passwd-min-uppercase-chars`— Jumlah minimum karakter huruf besar dalam kata sandi.
- `passwd-min-digits`— Jumlah minimum digit dalam kata sandi.

- `passwd-alphanum`— Informasi tentang penyertaan atau pengecualian karakter alfanumerik.
- `passwd-expiry-time`— Waktu kedaluwarsa kata sandi.
- `passwd-expiry-warn-time`— Waktu peringatan kedaluwarsa kata sandi.

3. Jalankan perintah berikut untuk melihat semua persyaratan kata sandi:

```
FsxId0123456::> security login role config show -role fsxadmin -fields passwd-minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-uppercase-chars
```

```
vserver          role      passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
-----
-----
-----
FsxId0123456      fsxadmin 3          enabled      0
unlimited          0          0            0
unlimited
```

Kuota

Berikut ini, Anda dapat mengetahui tentang kuota saat bekerja dengan Amazon FSx untuk NetApp ONTAP.

Topik

- [Kuota yang dapat Anda tingkatkan](#)
- [Kuota sumber daya untuk setiap sistem file](#)

Kuota yang dapat Anda tingkatkan

Berikut ini adalah kuota untuk Amazon FSx untuk NetApp ONTAP untuk masing-masing Akun AWS, per Wilayah AWS, yang dapat Anda tingkatkan.

Sumber daya	Default	Deskripsi
ONTAPsistem berkas	100	Jumlah maksimum Amazon FSx untuk sistem file NetApp ONTAP yang dapat Anda buat di akun ini.
ONTAPKapasitas penyimpanan SSD	524,288	Jumlah maksimum kapasitas penyimpanan SSD (dalam GiB) untuk semua Amazon FSx untuk sistem file NetApp ONTAP yang dapat Anda miliki di akun ini.
ONTAPkapasitas throughput	10,240	Jumlah maksimum kapasitas throughput (in MBps) untuk semua Amazon FSx untuk sistem file NetApp ONTAP yang dapat Anda miliki di akun ini.

Sumber daya	Default	Deskripsi
ONTAPSSD IOPS	1.000.000	Jumlah maksimum SSD IOPS untuk semua Amazon FSx untuk sistem file NetApp ONTAP yang dapat Anda miliki di akun ini.
Backup ONTAP	10.000	Jumlah maksimum pencadangan volume yang dimulai pengguna untuk semua FSx Amazon NetApp untuk sistem file ONTAP yang dapat Anda miliki di file. Akun AWS
Titik akses Amazon S3	10.000	Jumlah maksimum jalur akses Amazon S3 untuk semua jenis sumber data yang didukung (misalnya, FSx untuk NetApp ONTAP) yang dapat Anda buat per wilayah dalam file. Akun AWS Ini juga merupakan jumlah maksimum titik akses S3 yang dapat Anda lampirkan ke satu FSx untuk sistem file NetApp ONTAP atau volume. Kuota ini merupakan kuota layanan Amazon S3 dan dapat disesuaikan menggunakan Service Quotas.

Untuk meminta peningkatan kuota

1. Buka [AWS Dukungan](#) halaman, masuk jika perlu, lalu pilih Buat kasus.
2. Untuk Buat kasus, pilih Support akun dan penagihan.
3. Di panel Detail kasus buat entri berikut:

- Untuk Jenis, pilih Akun.
 - Untuk Kategori pilih Masalah Akun lainnya.
 - Untuk Subjek masukkan **Amazon FSx for NetApp ONTAP service limit increase request**.
 - Sediakan detail Deskripsi permintaan Anda, termasuk:
 - FSx Kuota yang Anda inginkan meningkat, dan nilai yang Anda inginkan meningkat menjadi, jika diketahui.
 - Alasan mengapa Anda mencari peningkatan kuota.
 - ID sistem file dan wilayah untuk setiap sistem file yang Anda minta peningkatan.
4. Berikan Opsi kontak pilihan Anda dan pilih Kirim.

Kuota sumber daya untuk setiap sistem file

Tabel berikut mencantumkan kuota di Amazon FSx untuk sumber daya NetApp ONTAP untuk setiap sistem file dalam file. Wilayah AWS

Sumber daya	Batas per sistem file
Kapasitas penyimpanan SSD minimum	1.024 GiB per pasangan ketersediaan tinggi (HA)
Kapasitas penyimpanan SSD minimum untuk memulai operasi penurunan	1.126 GiB per pasangan HA
Persentase penurunan SSD minimum	9% lebih kecil dari kapasitas saat ini
Kapasitas penyimpanan SSD maksimum	• Sistem file Single-AZ generasi kedua: 512 TiB per pasangan HA, hingga 1 PiB • Sistem file Multi-AZ generasi kedua: 512 TiB • Sistem file generasi pertama: 192 TiB

Sumber daya	Batas per sistem file
Pemanfaatan SSD maksimum yang disarankan	80% untuk kinerja optimal dan fungsionalitas tiering
Pemanfaatan SSD maksimum untuk mengurangi operasi	80% sebelum dan sesudah operasi penurunan
IOPS SSD maksimum	Sistem file generasi kedua: • 200.000 per pasangan HA (hingga 12 pasang) untuk Single-AZ • 200.000 total untuk Multi-AZ Sistem file generasi pertama: • 160.000 di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia) • 80.000 di semua Wilayah AWS tempat lain FSx untuk ONTAP tersedia
Kapasitas throughput minimum	• Sistem file generasi kedua (1 pasangan HA): 384 MBps • Sistem file generasi kedua (2 atau lebih pasangan HA): MBps 1.536 per pasangan HA • Sistem file generasi pertama: 128 MBps

Sumber daya	Batas per sistem file
Kapasitas throughput maksimum	Sistem file generasi kedua: • 73.728 MBps 1 untuk Single-AZ • 6.144 MBps untuk Multi-AZ Sistem file generasi pertama: • 4.096 MBps² di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia) • 2.048 MBps di semua Wilayah AWS tempat lain FSx untuk ONTAP tersedia
Jumlah volume maksimum	• Sistem file generasi kedua (1 pasangan HA): 500 • Sistem file generasi kedua (2 atau lebih pasangan HA): 1.000 • Sistem file generasi pertama: 500 Saat menggunakan titik akses S3 dengan sistem file Anda: • Sistem file generasi kedua (1 pasangan HA): 491 • Sistem file generasi kedua (2 atau lebih pasangan HA): 975 untuk 2 pasangan HA (903 untuk 12 pasangan HA) • Sistem file generasi pertama: 491
Jumlah snapshot maksimum	1.023 per volume 3

Sumber daya	Batas per sistem file
Jumlah maksimum backup	4.091 per volume 4

Sumber daya	Batas per sistem file
Jumlah maksimum SVMs	Sistem file generasi kedua dengan satu pasangan HA dan tipe jaringan IPv4 -only: • 6 (384 MBps kapasitas throughput) • 6 (768 MBps kapasitas throughput) • 14 (1.536 MBps kapasitas throughput) • 14 (3.072 MBps kapasitas throughput) • 24 (6.144 MBps kapasitas throughput) Sistem file generasi kedua dengan satu pasangan HA dan tipe jaringan dual-stack: • 6 (384 MBps kapasitas throughput) • 6 (768 MBps kapasitas throughput) • 11 (1.536 MBps kapasitas throughput) • 11 (3.072 MBps kapasitas throughput) • 11 (6.144 MBps kapasitas throughput) Sistem file generasi kedua dengan 2-12 pasangan HA dan tipe jaringan IPv4 -only atau dual-stack: • 11

Sumber daya	Batas per sistem file
	Sistem file generasi pertama dengan tipe jaringan IPv4 -only: • 6 (128 kapasitas MBps throughput) • 6 (256 kapasitas MBps throughput) • 14 (MBps kapasitas throughput 512) • 14 (MBps kapasitas throughput 1.024) • 24 (MBps kapasitas throughput 2.048) • 24 (MBps kapasitas throughput 4.096) Sistem file generasi pertama dengan tipe jaringan dual-stack: • 6 (128 kapasitas MBps throughput) • 6 (256 kapasitas MBps throughput) • 11 (MBps kapasitas throughput 512) • 11 (MBps kapasitas throughput 1.024) • 11 (MBps kapasitas throughput 2.048) • 11 (MBps kapasitas throughput 4.096)
Jumlah maksimum tag	50
Periode penyimpanan maksimum untuk cadangan otomatis	90 hari

Sumber daya	Batas per sistem file
Periode retensi maksimum untuk pencadangan yang dimulai pengguna	Tidak ada batas retensi
Jumlah maksimum rute yang didukung per sistem file	50 ⁵
Jumlah maksimum koneksi klien per server file ⁶	100.000

Note

¹ Pada sistem file single-AZ generasi kedua dengan 12 pasang HA (6.144 MBps per pasangan HA). Untuk informasi selengkapnya, lihat [Mengelola pasangan ketersediaan tinggi \(HA\)](#).

² Untuk menyediakan 4 GBps kapasitas throughput, FSx untuk sistem file generasi pertama ONTAP Anda memerlukan konfigurasi IOPS SSD maksimum (160.000) dan minimal 5.120 GiB kapasitas penyimpanan SSD yang didukung. Wilayah AWS Untuk informasi lebih lanjut tentang yang Wilayah AWS mendukung 4.096 MBps kapasitas throughput, lihat. [Dampak kapasitas throughput terhadap performa](#)

³ Anda dapat menyimpan hingga 1.023 snapshot per volume kapan saja. Setelah Anda mencapai batas ini, Anda harus menghapus snapshot yang ada sebelum snapshot baru volume Anda dapat dibuat.

⁴ Anda dapat menyimpan hingga 4.091 cadangan per volume kapan saja. Setelah Anda mencapai batas ini, Anda harus menghapus cadangan yang ada sebelum cadangan baru volume Anda dapat dibuat.

⁵ Anda dapat mengonfigurasi hingga 50 rute per sistem file kapan saja. Setelah Anda mencapai batas ini, Anda harus menghapus rute yang ada sebelum rute baru dapat dikonfigurasi. Jumlah rute yang dimiliki sistem file Anda ditentukan oleh jumlah yang SVMs dimilikinya dan jumlah tabel rute yang terkait dengannya. Anda dapat menentukan jumlah rute yang ada ke sistem file menggunakan persamaan berikut: $(1 + \text{jumlah SVMs dalam sistem file}) * (\text{tabel rute yang terkait dengan sistem file})$.

⁶ Koneksi klien didefinisikan sebagai koneksi TCP tunggal ke server file tertentu. Ada satu server file aktif per pasangan HA dalam sistem file. Klien dapat memiliki beberapa koneksi TCP ke server file. Misalnya, jika klien menggunakan multipathing.

Memecahkan masalah Amazon FSx untuk ONTAP NetApp

Gunakan bagian berikut untuk membantu memecahkan masalah sistem file FSx ONTAP.

Topik

- [Sistem file Anda dalam MISCONFIGURED keadaan](#)
- [Anda tidak dapat mengakses sistem file Anda](#)
- [Mesin virtual penyimpanan Anda \(SVM\) dalam keadaan MISCONFIGURED](#)
- [Pemecahan masalah SSD mengurangi masalah operasi](#)
- [Anda tidak dapat bergabung dengan mesin virtual penyimpanan \(SVM\) ke Active Directory](#)
- [Anda tidak dapat menghapus penyimpanan mesin virtual atau volume](#)
- [Volume Anda dalam MISCONFIGURED keadaan](#)
- [Volume Anda memiliki kapasitas penyimpanan yang tidak mencukupi](#)
- [Pencadangan Anda gagal karena kapasitas volume yang tidak mencukupi](#)
- [Memulihkan dihapus FSx untuk volume ONTAP](#)
- [Memecahkan masalah jaringan](#)
- [Memecahkan masalah I/O kesalahan dan kegagalan klaim kembali kunci NFS](#)

Sistem file Anda dalam **MISCONFIGURED** keadaan

Ada sejumlah penyebab potensial untuk sistem file berada dalam MISCONFIGURED keadaan, masing-masing dengan resolusi mereka sendiri, sebagai berikut.

Topik

- [Akun pemilik VPC telah menonaktifkan berbagi VPC multi-AZ](#)
- [Anda tidak dapat membuat SVM baru pada sistem file Multi-AZ](#)
- [Tingkat penyimpanan SSD sistem file Anda lebih dari 90% penuh](#)

Akun pemilik VPC telah menonaktifkan berbagi VPC multi-AZ

Sistem file multi-AZ yang dibuat oleh peserta Akun AWS dalam subnet VPC bersama akan masuk ke MISCONFIGURED status karena salah satu alasan berikut:

- Akun pemilik yang membagikan subnet VPC telah menonaktifkan dukungan berbagi VPC multi-AZ untuk sistem file ONTAP. FSx
- Akun pemilik telah berhenti membagikan subnet VPC.

Jika akun pemilik telah berhenti membagikan subnet VPC, Anda akan melihat pesan berikut di konsol untuk sistem file tersebut:

```
The vpc ID vpc-012345abcde does not exist
```

Untuk mengatasi masalah ini, Anda harus menghubungi akun pemilik yang membagikan subnet VPC dengan Anda. Untuk informasi lebih lanjut lihat [Membuat FSx untuk sistem file ONTAP di subnet bersama](#) untuk informasi lebih lanjut.

Anda tidak dapat membuat SVM baru pada sistem file Multi-AZ

Untuk sistem file multi-AZ yang dibuat oleh peserta Akun AWS dalam VPC bersama, Anda tidak akan dapat membuat SVM baru karena salah satu alasan berikut:

- Akun pemilik yang membagikan subnet VPC telah menonaktifkan dukungan berbagi VPC multi-AZ untuk sistem file ONTAP. FSx
- Akun pemilik telah berhenti membagikan subnet VPC.

Untuk mengatasi masalah ini, Anda harus menghubungi akun pemilik yang membagikan subnet VPC dengan Anda. Untuk informasi lebih lanjut lihat [Membuat FSx untuk sistem file ONTAP di subnet bersama](#) untuk informasi lebih lanjut.

Tingkat penyimpanan SSD sistem file Anda lebih dari 90% penuh

Tingkat penyimpanan SSD sistem file Single-AZ atau Multi-AZ Anda saat ini lebih dari 90% penuh. Kami menyarankan agar Anda tidak melebihi 80% pemanfaatan tingkat penyimpanan SSD Anda secara berkelanjutan. Jika Anda tidak mengosongkan ruang di tingkat penyimpanan SSD sebelum jendela pemeliharaan sistem file Anda berikutnya, FSx untuk ONTAP akan membatasi sementara throughput sistem file Anda selama operasi penambalan. Hal ini dilakukan untuk memastikan bahwa proses pemeliharaan latar belakang dapat selesai dalam jangka waktu yang wajar. Untuk menghindari hal ini, harap kurangi penggunaan tingkat penyimpanan SSD Anda hingga di bawah 90%. Anda dapat mengurangi pemanfaatan SSD dengan beberapa cara, termasuk:

- Meningkatkan kapasitas penyimpanan SSD sistem file Anda.
- Dengan menghapus data yang tidak dibutuhkan.
- Dengan menghapus snapshot volume yang tidak dibutuhkan.

Untuk informasi selengkapnya, lihat [Mengelola kapasitas penyimpanan](#).

Anda tidak dapat mengakses sistem file Anda

Bagian ini menjelaskan masalah dan resolusi yang terkait dengan tidak dapat mengakses sistem file Anda.

Topik

- [Sistem file Multi-AZ Anda memiliki tag tabel rute yang hilang](#)
- [Sistem file Anda memiliki lebih dari 50 rute](#)
- [Sistem file Anda tidak memiliki rute ke satu atau beberapa server file](#)
- [Elastic network interface sistem file telah dimodifikasi atau dihapus](#)
- [Alamat IP Elastis yang dilampirkan ke elastic network interface sistem file telah dihapus](#)
- [Grup keamanan VPC sistem file tidak memiliki aturan masuk yang diperlukan](#)
- [Grup keamanan VPC instans komputasi tidak memiliki aturan keluar yang diperlukan](#)
- [Subnet instance komputasi tidak menggunakan tabel rute apa pun yang terkait dengan sistem file Anda](#)
- [Amazon tidak FSx dapat memperbarui tabel rute untuk sistem file Multi-AZ yang dibuat menggunakan CloudFormation](#)
- [Tidak dapat mengakses sistem file melalui iSCSI dari klien di VPC lain](#)
- [Akun pemilik telah berhenti membagikan subnet VPC](#)
- [Tidak dapat mengakses sistem file melalui NFS, SMB, CLI ONTAP, atau ONTAP REST API dari klien di VPC lain atau lokal](#)

Sistem file Multi-AZ Anda memiliki tag tabel rute yang hilang

Amazon FSx mengelola tabel rute VPC untuk sistem file multi-AZ menggunakan otentikasi berbasis tag. Satu atau beberapa tabel rute yang terkait dengan sistem file Anda saat ini kehilangan tag tabel

rute ini. Tabel rute ini ditandai dengan `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Jika Anda tidak menambahkan tag ini secara manual sebelum jendela pemeliharaan berikutnya, setiap klien dalam subnet yang terkait dengan tabel rute yang kehilangan tag untuk sementara waktu akan kehilangan akses ke sistem file selama operasi penambalan. Untuk menghindari hal ini, silakan tambahkan tag tabel rute yang hilang secara manual.

Untuk informasi selengkapnya, lihat [Memperbarui sistem file](#).

Sistem file Anda memiliki lebih dari 50 rute

Sistem file Anda saat ini memiliki lebih dari 50 rute yang terkait dengannya. Jika Anda tidak menghapus beberapa rute ini sebelum jendela pemeliharaan terjadwal berikutnya sistem file Anda, proses failover mungkin memakan waktu lebih lama dari biasanya. Untuk menghindari hal ini, tolong kurangi jumlah rute menjadi kurang dari 50. Berikut ini adalah langkah-langkah yang dapat Anda ambil untuk mengurangi jumlah rute yang terkait dengan sistem file Anda:

- Menghapus rute berlebih
- Mengurangi jumlah SVMs yang terkait dengan sistem file
- Mengurangi jumlah tabel rute yang terkait dengan sistem file

Untuk informasi selengkapnya, lihat [Memperbarui sistem file](#) dan [Menghapus penyimpanan mesin virtual \(SVM\)](#).

Sistem file Anda tidak memiliki rute ke satu atau beberapa server file

Sistem file Anda saat ini kehilangan rute ke satu atau beberapa server file, dan tabel rute yang ada tidak memiliki cukup ruang untuk menambahkan entri tabel rute baru. Jika Anda tidak menambahkan rute yang hilang sebelum jendela pemeliharaan terjadwal berikutnya dari sistem file Anda, klien yang terhubung akan terputus selama operasi penambalan. Untuk menghindari hal ini, silakan tambahkan rute yang hilang.

Untuk informasi selengkapnya, lihat [Memperbarui sistem file](#) dan [Kuota](#).

Elastic network interface sistem file telah dimodifikasi atau dihapus

Anda tidak boleh memodifikasi atau menghapus salah satu antarmuka jaringan elastis sistem file. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan hilangnya koneksi

permanen antara virtual private cloud (VPC) dan sistem file Anda. Buat sistem file baru, dan jangan memodifikasi atau menghapus antarmuka FSx jaringan Amazon. Untuk informasi selengkapnya, lihat [Kontrol Akses Sistem File dengan Amazon VPC](#).

Alamat IP Elastis yang dilampirkan ke elastic network interface sistem file telah dihapus

Amazon FSx tidak mendukung akses sistem file dari Internet publik. Amazon FSx secara otomatis melepaskan alamat IP Elastis yang merupakan alamat IP publik yang dapat dijangkau dari Internet yang dilampirkan ke antarmuka network elastis sistem file. Untuk informasi selengkapnya, lihat [Klien yang didukung](#).

Grup keamanan VPC sistem file tidak memiliki aturan masuk 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 VPC instans komputasi 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.

Subnet instance komputasi tidak menggunakan tabel rute apa pun yang terkait dengan sistem file Anda

FSx untuk ONTAP membuat titik akhir untuk mengakses sistem file Anda dalam tabel rute VPC. Kami menyarankan Anda mengonfigurasi sistem file Anda untuk menggunakan semua tabel rute VPC yang terkait dengan subnet tempat klien Anda berada. Secara default, Amazon FSx menggunakan tabel rute utama VPC Anda. Anda dapat secara opsional menentukan satu atau beberapa tabel rute untuk Amazon FSx untuk digunakan saat Anda membuat sistem file.

Jika Anda dapat melakukan ping ke titik akhir Intercluster sistem file Anda tetapi tidak dapat melakukan ping ke titik akhir Manajemen sistem file Anda (lihat [Sumber daya sistem file](#) untuk informasi lebih lanjut), klien Anda kemungkinan tidak berada dalam subnet yang terkait dengan salah satu tabel rute sistem file Anda. Untuk mengakses sistem file Anda, kaitkan salah satu tabel rute

sistem file Anda dengan subnet klien Anda. Untuk informasi tentang memperbarui tabel rute Amazon VPC sistem file Anda, lihat. [Memperbarui sistem file](#)

Amazon tidak FSx dapat memperbarui tabel rute untuk sistem file Multi-AZ yang dibuat menggunakan CloudFormation

Amazon FSx mengelola tabel rute VPC untuk sistem file multi-AZ menggunakan otentikasi berbasis tag. Tabel rute ini ditandai dengan `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Saat membuat atau memperbarui FSx untuk sistem file ONTAP Multi-AZ menggunakan CloudFormation kami sarankan Anda menambahkan `Key: AmazonFSx; Value: ManagedByAmazonFSx` tag secara manual.

Jika Anda tidak dapat menjangkau sistem file Multi-AZ Anda, periksa untuk melihat apakah tabel rute VPC yang terkait dengan sistem file ditandai. `Key: AmazonFSx; Value: ManagedByAmazonFSx`. Jika tidak, maka Amazon tidak FSx dapat memperbarui tabel rute tersebut untuk merutekan alamat IP mengambang dari manajemen dan port data ke server file aktif ketika peristiwa failover terjadi. Untuk informasi tentang memperbarui tabel rute Amazon VPC sistem file Anda, lihat. [Memperbarui sistem file](#)

Tidak dapat mengakses sistem file melalui iSCSI dari klien di VPC lain

Untuk mengakses sistem file melalui protokol Internet Small Computer Systems Interface (iSCSI) dari klien di VPC lain, Anda dapat mengonfigurasi peering VPC Amazon atau AWS Transit Gateway antara VPC yang terkait dengan sistem file Anda dan VPC tempat klien Anda berada. Untuk informasi selengkapnya, lihat [Membuat dan menerima koneksi peering VPC](#) di panduan Amazon Virtual Private Cloud.

Akun pemilik telah berhenti membagikan subnet VPC

Jika Anda membuat sistem file Anda di subnet VPC yang telah dibagikan dengan Anda, akun pemilik mungkin telah berhenti berbagi subnet VPC.

Jika akun pemilik telah berhenti membagikan subnet VPC, Anda akan melihat pesan berikut di konsol untuk sistem file tersebut:

```
The vpc ID vpc-012345abcde does not exist
```

Anda harus menghubungi akun pemilik sehingga mereka dapat berbagi kembali subnet dengan Anda.

Tidak dapat mengakses sistem file melalui NFS, SMB, CLI ONTAP, atau ONTAP REST API dari klien di VPC lain atau lokal

Untuk mengakses sistem file melalui Network File System (NFS), Server Message Block (SMB), atau NetApp ONTAP CLI dan REST API dari klien di VPC lain atau di tempat, Anda harus mengonfigurasi perutean menggunakan AWS Transit Gateway antara VPC yang terkait dengan sistem file Anda dan jaringan tempat klien Anda berada. Untuk informasi selengkapnya, lihat [Mengakses data FSx ONTAP Anda](#).

Mesin virtual penyimpanan Anda (SVM) dalam keadaan **MISCONFIGURED**

Ada sejumlah penyebab potensial untuk Storage Virtual Machine untuk masuk ke MISCONFIGURED keadaan, masing-masing dengan resolusi mereka sendiri, sebagai berikut.

SVM Anda memiliki volume offline

Sistem file Anda berisi volume yang dalam keadaan offline. Kami menyarankan agar Anda menyimpan volume online secara berkelanjutan. Jika Anda tidak online volume ini sebelum jendela pemeliharaan sistem file Anda berikutnya, Amazon FSx akan online sementara volume ini selama durasi operasi penambalan. Untuk menghindari hal ini, silakan online atau hapus volume.

Untuk mengembalikan volume offline secara online, gunakan perintah [volume online](#) ONTAP CLI, seperti yang ditunjukkan pada contoh berikut. Jika hanya ada satu SVM (Vserver), Anda tidak perlu menentukan parameternya. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

SVM Anda memiliki volume offline dengan iSCSI LUN atau namespace NVMe/TCP

Sistem file Anda berisi volume yang dalam keadaan terbatas. Kami menyarankan agar Anda menyimpan volume online secara berkelanjutan. Jika Anda tidak online volume ini sebelum jendela pemeliharaan sistem file Anda berikutnya, Amazon FSx akan online sementara volume ini selama durasi operasi penambalan. Untuk menghindari hal ini, silakan online atau hapus volume.

Untuk mengembalikan volume offline secara online, gunakan perintah [volume online](#) ONTAPCLI, seperti yang ditunjukkan pada contoh berikut. Jika hanya ada satu SVM (Vserver), Anda tidak perlu menentukan parameternya. -vserver

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Kunci AWS Secrets Manager rahasia atau KMS tidak dikonfigurasi dengan benar

Amazon tidak FSx dapat membuat koneksi dengan pengontrol atau pengontrol domain Microsoft Active Directory Anda. Ini karena AWS Secrets Manager rahasia Anda atau tidak AWS KMS key dikonfigurasi dengan benar. Untuk informasi selengkapnya, lihat [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).

Untuk mengatasi kesalahan konfigurasi, lakukan hal berikut:

- Verifikasi bahwa ARN rahasia sudah benar dan ikuti format yang tepat:
`arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`
- Verifikasi bahwa rahasia berisi kedua bidang wajib dengan nilai yang tidak kosong:
 - CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME— Nama pengguna akun layanan AD Anda.
 - CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD— Kata sandi akun layanan AD Anda.
- Verifikasi bahwa rahasia dan kunci memiliki kebijakan berbasis sumber daya yang memberikan `fsx.amazonaws.com` izin kepada prinsipal FSx layanan Amazon untuk mengambil nilai rahasia.

Pemecahan masalah SSD mengurangi masalah operasi

Bagian ini menjelaskan masalah dan resolusi umum yang terkait dengan operasi penurunan kapasitas SSD.

Topik

- [Pengoperasian penurunan SSD Anda dihentikan sementara karena pemanfaatan SSD yang tinggi](#)
- [Pengoperasian penurunan SSD Anda dijeda karena hubungan FlexClone](#)
- [Mengarahkan akses klien untuk volume gagal selama penurunan SSD](#)

- [Pengoperasian penurunan SSD Anda membutuhkan waktu lebih lama dari yang diharapkan](#)

Pengoperasian penurunan SSD Anda dihentikan sementara karena pemanfaatan SSD yang tinggi

Jika tingkat penyimpanan SSD Anda melebihi 80% pemanfaatan selama operasi yang berkurang, Amazon FSx secara otomatis menghentikan operasi. Anda mungkin melihat pesan Tindakan Administratif yang mirip dengan:

```
Your file system has insufficient free space in aggr_1. Please free up space or increase your file system's storage capacity.
```

Operasi akan dilanjutkan setelah pemanfaatan turun di bawah 80%. Untuk mengatasi masalah ini, Anda dapat melakukan hal berikut:

- Hapus data yang tidak perlu dari volume yang telah dipindahkan ke disk baru.
- Tingkatkan lebih banyak data ke kumpulan kapasitas dengan memodifikasi kebijakan tingkatan volume.
- Kirim permintaan untuk meningkatkan kapasitas SSD dengan menelepon [update-file-system](#) dengan nilai target baru.

Anda harus memperbarui kapasitas penyimpanan SSD sistem file Anda sehingga kapasitas SSD yang dihasilkan sistem file Anda tidak melebihi 80% pemanfaatan setelah operasi berkurang. Untuk detail selengkapnya, lihat [Memperbarui penyimpanan SSD sistem file dan IOPS](#).

Anda dapat mengidentifikasi volume mana yang telah dipindahkan ke disk baru dengan memeriksa Message bidang dalam tindakan STORAGE_OPTIMIZATION administratif.

Anda juga dapat menelepon [describe-volumes](#) jika agregat adalah aggr1 atau aggr1_old.

Pengoperasian penurunan SSD Anda dijeda karena hubungan FlexClone

Jika FlexClone volume dibuat setelah memulai operasi penurunan SSD, Amazon FSx menghentikan operasi hingga klon dihapus. Ini karena ONTAP membagi hubungan klon saat memindahkan volume, yang akan menghasilkan penyimpanan duplikat pada disk baru. Untuk mengatasi masalah ini, Anda dapat mengidentifikasi dan menghapus FlexClone volume apa pun yang dibuat setelah operasi penurunan dimulai.

Setelah Anda menghapus semua FlexClone volume, operasi penurunan akan secara otomatis dilanjutkan.

Mengarahkan akses klien untuk volume gagal selama penurunan SSD

Selama operasi penurunan SSD, Amazon FSx perlu mengalihkan akses klien dari disk lama ke disk baru untuk setiap volume. Jika proses ini gagal, Anda mungkin melihat pesan Tindakan Administratif yang mirip dengan:

```
Redirecting client access for volume(s) fsvol-123 has failed due to insufficient SSD IOPS, throughput capacity, or because the volume is full.
```

Untuk mengatasi masalah ini, Anda dapat melakukan hal berikut:

- Periksa metrik pemanfaatan sumber daya sistem file Anda di Amazon CloudWatch untuk memastikan bahwa beban kerja Anda tidak memakan lebih dari 50% sumber daya berikut:
 - NetworkThroughputUtilization
 - FileServerDiskThroughputUtilization
 - FileServerDiskIopsUtilization
 - CPUUtilization
 - DiskIopsUtilization
- Jika volumenya penuh, tingkatkan kapasitas penyimpanan volume.
- Kurangi beban kerja pada sistem file Anda selama operasi penurunan.

Setelah mengatasi masalah ini, Amazon FSx akan secara otomatis mencoba mengalihkan akses klien satu jam sekali.

Pengoperasian penurunan SSD Anda membutuhkan waktu lebih lama dari yang diharapkan

Waktu yang diperlukan untuk menyelesaikan operasi penurunan SSD tergantung pada beberapa faktor, termasuk jumlah data yang disimpan pada sistem file, aktivitas beban kerja yang sedang berlangsung, dan sumber daya sistem yang tersedia. Jika operasi Anda memakan waktu lebih lama dari yang diharapkan, Anda dapat melakukan hal berikut:

- Verifikasi bahwa sistem file Anda memiliki sumber daya yang memadai yang tersedia (kurang dari 50% CPU, throughput disk, dan pemanfaatan SSD IOPS).

- Kurangi beban kerja berat tulis selama operasi untuk meminimalkan pertentangan sumber daya.

Anda dapat melacak kemajuan operasi dengan memeriksa ProgressPercent properti dalam tindakan STORAGE_OPTIMIZATION administratif.

Anda tidak dapat bergabung dengan mesin virtual penyimpanan (SVM) ke Active Directory

Jika Anda tidak dapat bergabung dengan SVM ke Active Directory (AD), tinjau [Cara kerja bergabung SVMs ke Microsoft Active Directory](#) terlebih dahulu. Masalah umum yang mencegah SVM bergabung ke Direktori Aktif Anda tercantum di bagian berikut, termasuk pesan kesalahan yang dihasilkan untuk setiap keadaan.

Topik

- [Nama SVM NetBIOS sama dengan nama NetBIOS untuk domain rumah.](#)
- [SVM sudah bergabung dengan Active Directory lain](#)
- [Amazon tidak FSx dapat terhubung ke pengontrol domain Direktori Aktif Anda karena nama NetBIOS SVM sudah digunakan](#)
- [Amazon tidak FSx dapat mengakses kredensial akun layanan Direktori Aktif Anda di AWS Secrets Manager](#)
- [Amazon tidak FSx dapat berkomunikasi dengan pengontrol domain Direktori Aktif Anda](#)
- [Amazon tidak FSx dapat terhubung ke Direktori Aktif Anda karena persyaratan port yang tidak terpenuhi atau izin akun layanan](#)
- [Amazon tidak FSx dapat terhubung ke pengontrol domain Direktori Aktif karena kredensial akun layanan tidak valid](#)
- [Amazon tidak FSx dapat terhubung ke pengontrol domain Direktori Aktif karena kredensial akun layanan tidak mencukupi](#)
- [Amazon tidak FSx dapat berkomunikasi dengan server DNS Active Directory atau pengontrol domain](#)
- [Amazon tidak FSx dapat berkomunikasi dengan Active Directory karena nama domain Active Directory tidak valid.](#)
- [Akun layanan tidak dapat mengakses grup administrator yang ditentukan dalam konfigurasi SVM Active Directory](#)

- [Amazon tidak FSx dapat terhubung ke pengontrol domain Direktori Aktif karena unit organisasi yang ditentukan tidak ada atau tidak dapat diakses](#)

Nama SVM NetBIOS sama dengan nama NetBIOS untuk domain rumah.

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi dengan Active Directory Anda. Ini karena nama server yang Anda tentukan adalah nama NetBIOS dari domain rumah. Untuk memperbaiki masalah ini, pilih nama NetBIOS untuk SVM Anda yang berbeda dari nama NetBIOS dari domain rumah. Kemudian coba kembali untuk bergabung dengan SVM Anda ke Active Directory Anda.

Untuk mengatasi masalah ini, ikuti prosedur yang dijelaskan [Bergabung SVMs ke Active Directory menggunakan Konsol Manajemen AWS, AWS CLI dan API](#) untuk mencoba kembali menggabungkan SVM Anda ke Direktori Aktif Anda. Pastikan Anda menggunakan nama NetBIOS untuk SVM Anda yang berbeda dari nama NetBIOS dari domain home Active Directory.

SVM sudah bergabung dengan Active Directory lain

Bergabung dengan SVM ke Active Directory gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi ke Direktori Aktif Anda. Ini karena SVM sudah bergabung ke domain. Untuk menggabungkan SVM ini ke domain lain, Anda dapat menggunakan ONTAP CLI atau REST API untuk memutuskan sambungan SVM ini dari Active Directory. Kemudian coba kembali untuk bergabung dengan SVM Anda ke Active Directory yang berbeda.

Untuk mengatasi masalah ini, lakukan hal berikut:

1. Gunakan CLI NetApp ONTAP untuk memutuskan sambungan SVM dari Active Directory saat ini. Untuk informasi selengkapnya, lihat [Berhenti bergabung dengan Active Directory dari SVM Anda menggunakan ONTAP NetApp CLI](#).
2. Ikuti prosedur yang dijelaskan [Bergabung SVMs ke Active Directory menggunakan Konsol Manajemen AWS, AWS CLI dan API](#) untuk mencoba kembali menggabungkan SVM Anda ke Active Directory yang baru.

Amazon tidak FSx dapat terhubung ke pengontrol domain Direktori Aktif Anda karena nama NetBIOS SVM sudah digunakan

Membuat SVM yang bergabung dengan Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi dengan Active Directory Anda. Ini karena nama NetBIOS (komputer) yang Anda tentukan sudah digunakan di Active Directory Anda. Untuk memperbaiki masalah ini, pilih nama NetBIOS untuk SVM Anda yang tidak digunakan di Direktori Aktif Anda., tentukan NetBIOS (komputer) Kemudian coba kembali untuk bergabung dengan SVM Anda ke Direktori Aktif Anda.

Untuk mengatasi masalah ini, ikuti prosedur yang dijelaskan [Bergabung SVMs ke Active Directory menggunakan Konsol Manajemen AWS, AWS CLI dan API](#) untuk mencoba kembali bergabung dengan SVM Anda ke AD Anda. Pastikan Anda menggunakan nama NetBIOS untuk SVM Anda yang unik dan belum digunakan di Direktori Aktif Anda.

Amazon tidak FSx dapat mengakses kredensial akun layanan Direktori Aktif Anda di AWS Secrets Manager

Bagian berikut menjelaskan masalah umum dan cara mengatasinya.

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

```
You can't provide both username/password and a domain join service account secret to connect to your Active Directory. Provide only one set of credentials.
```

Untuk mengatasi masalah ini

1. Pilih apakah Anda ingin memberikan kredensial yang disimpan dalam rahasia Secrets Manager, atau dalam teks biasa.
2. Saat bergabung dengan Active Directory, hanya berikan salah satu parameter tersebut dan bukan keduanya.

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

The domain join service account secret ARN format you entered isn't valid. Use the format: `arn:partition:secretsmanager:region:account-id:secret:secret-name-6chars`

Untuk mengatasi masalah ini

1. Ulasan [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).
2. Verifikasi bahwa format ARN yang Anda masukkan sudah benar.
Contoh format yang benar adalah `arn:aws:secretsmanager:us-east-1:123456789012:secret:MyDatabaseSecret-Ab3d5f`.

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx can't access the domain join service account secret [ARN]. Add a resource permission to the secret that grants the FSx service principal (`fsx.amazonaws.com`) permission to access it.

Untuk mengatasi masalah ini

1. Ulasan [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).
2. Verifikasi bahwa rahasia Secrets Manager yang Anda berikan memiliki kebijakan yang benar yang FSx memungkinkan Amazon menggunakan rahasia tersebut.

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

You don't have permission to access the domain join service account secret [ARN]. A resource permission needs to be added to the secret to grant you access.

Untuk mengatasi masalah ini

- Pemilik rahasia Secrets Manager atau administrator perlu memberikan akses akun Anda untuk menggunakan rahasia ini. Untuk informasi selengkapnya, lihat [Kebijakan berbasis identitas](#).

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

The domain join service account secret format or content isn't valid. Make sure the secret includes both `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`

and CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD fields with non-empty values.

Untuk mengatasi masalah ini

1. Ulas [Menyimpan kredensial Active Directory menggunakan AWS Secrets Manager](#).
2. Verifikasi bahwa rahasia Secrets Manager yang Anda berikan memiliki kedua bidang yang diperlukan.

Amazon tidak FSx dapat berkomunikasi dengan pengontrol domain Direktori Aktif Anda

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat berkomunikasi dengan Active Directory Anda. Untuk memperbaiki masalah ini, pastikan lalu lintas jaringan diizinkan antara Amazon FSx dan pengontrol domain Anda. Kemudian coba kembali untuk bergabung dengan SVM Anda ke Active Directory Anda.

Untuk mengatasi masalah ini, lakukan solusi berikut:

1. Tinjau persyaratan yang dijelaskan dalam [Persyaratan konfigurasi jaringan](#), dan buat perubahan yang diperlukan untuk mengaktifkan komunikasi jaringan antara Amazon FSx dan iklan Anda.
2. Setelah Amazon FSx dapat berkomunikasi dengan iklan Anda, ikuti prosedur yang dijelaskan [Bergabung SVMs ke Active Directory menggunakan Konsol Manajemen AWS, AWS CLI dan API](#) dan coba kembali menggabungkan SVM Anda ke AD Anda.

Amazon tidak FSx dapat terhubung ke Direktori Aktif Anda karena persyaratan port yang tidak terpenuhi atau izin akun layanan

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi dengan Active Directory Anda. Hal ini disebabkan oleh persyaratan port untuk Direktori Aktif Anda tidak terpenuhi, atau akun layanan yang diberikan tidak memiliki izin untuk bergabung dengan mesin virtual penyimpanan ke domain dengan unit organisasi yang ditentukan. Untuk memperbaiki masalah ini, perbarui konfigurasi Direktori Aktif mesin virtual penyimpanan Anda setelah menyelesaikan masalah izin apa pun dengan port dan akun layanan, seperti yang direkomendasikan dalam panduan FSx pengguna Amazon.

Untuk mengatasi masalah ini, lakukan solusi berikut:

1. Tinjau persyaratan yang dijelaskan dalam [Persyaratan konfigurasi jaringan](#), dan buat perubahan yang diperlukan untuk memenuhi persyaratan jaringan dan memastikan komunikasi diaktifkan pada port yang diperlukan
2. Tinjau persyaratan akun layanan yang dijelaskan dalam [Persyaratan akun layanan Direktori Aktif](#). Pastikan akun layanan memiliki izin yang didelegasikan yang diperlukan untuk menggabungkan SVM Anda ke domain Active Directory menggunakan unit organisasi yang ditentukan.
3. Setelah Anda membuat perubahan pada izin port atau akun layanan, ikuti prosedur yang dijelaskan [Bergabung SVMs ke Active Directory menggunakan Konsol Manajemen AWS, AWS CLI dan API](#) dan coba kembali bergabung dengan SVM Anda ke AD Anda.

Amazon tidak FSx dapat terhubung ke pengontrol domain Direktori Aktif karena kredensial akun layanan tidak valid

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat sambungan dengan pengontrol domain Direktori Aktif karena kredensial akun layanan yang diberikan tidak valid. Untuk memperbaiki masalah ini, perbarui konfigurasi Active Directory mesin virtual penyimpanan Anda dengan akun layanan yang valid.

Untuk mengatasi masalah ini, gunakan prosedur yang dijelaskan dalam [Memperbarui konfigurasi SVM Active Directory yang ada menggunakan Konsol Manajemen AWS, AWS CLI, dan API](#) untuk memperbarui kredensi akun layanan SVM. Saat memasukkan nama pengguna akun layanan, pastikan untuk hanya menyertakan nama pengguna (misalnya, ServiceAcct), dan jangan menyertakan awalan domain apa pun (misalnya, corp.com\ServiceAcct) atau akhiran domain (misalnya, ServiceAcct@corp.com). Jangan gunakan nama terhormat (DN) saat memasukkan nama pengguna akun layanan (misalnya, CN=ServiceAcct, OU=example, DC=corp, DC=com).

Amazon tidak FSx dapat terhubung ke pengontrol domain Direktori Aktif karena kredensial akun layanan tidak mencukupi

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi dengan pengontrol domain Direktori Aktif Anda. Hal ini disebabkan oleh persyaratan port yang belum terpenuhi untuk Direktori Aktif, atau akun layanan yang disediakan tidak memiliki izin untuk bergabung dengan mesin virtual penyimpanan ke domain dengan unit organisasi yang ditentukan.

Untuk mengatasi masalah ini, pastikan Anda telah mendelegasikan izin yang diperlukan ke 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
- Kemampuan untuk membuat dan menghapus objek komputer
- Kemampuan tervalidasi untuk membaca dan menulis Pembatasan Akun

Untuk informasi selengkapnya tentang membuat akun layanan dengan izin yang benar, lihat [Persyaratan akun layanan Direktori Aktif](#) dan [Mendelegasikan izin ke akun layanan Amazon FSx Anda](#).

Amazon tidak FSx dapat berkomunikasi dengan server DNS Active Directory atau pengontrol domain

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat berkomunikasi dengan Active Directory Anda. Ini karena Amazon tidak FSx dapat menjangkau server DNS yang disediakan atau pengontrol domain untuk domain Anda. Untuk memperbaiki masalah ini, perbarui konfigurasi Active Directory mesin virtual penyimpanan Anda dengan server DNS yang valid dan konfigurasi jaringan yang memungkinkan lalu lintas mengalir dari mesin virtual penyimpanan ke pengontrol domain.

Untuk mengatasi masalah ini, gunakan prosedur berikut:

1. Jika hanya beberapa pengontrol domain di Active Directory yang dapat dijangkau, misalnya karena keterbatasan geografis atau firewall, Anda dapat menambahkan pengontrol domain pilihan. Dengan menggunakan opsi ini, Amazon FSx mencoba menghubungi pengontrol domain pilihan. Tambahkan pengontrol domain pilihan menggunakan perintah [vserver cifs domain preferred-dc add](#) NetApp ONTAP CLI, sebagai berikut:

- a. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

- b. Masukkan perintah berikut, di mana:

- `-vserver vs1` menentukan nama mesin virtual penyimpanan (SVM).
- `-domain domain_name` menentukan nama Active Directory (FQDN) yang sepenuhnya memenuhi syarat dari domain yang menjadi milik pengontrol domain tertentu.
- `-preferred-dc IP_address,...` menentukan satu atau lebih alamat IP dari pengontrol domain pilihan, sebagai daftar yang dibatasi koma, dalam urutan preferensi.

```
FsxId123456789::> vs1 cifs domain preferred-dc add -vserver vs1 -domain domain_name -preferred-dc IP_address, ...+
```

Perintah berikut menambahkan pengontrol domain 172.17.102.25 dan 172.17.102.24 ke daftar pengontrol domain pilihan yang digunakan server SMB di SVM vs1 untuk mengelola akses eksternal ke domain cifs.lab.example.com.

```
FsxId123456789::> vs1 cifs domain preferred-dc add -vserver vs1 -domain cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. Periksa untuk melihat apakah Pengontrol Domain Anda dapat diselesaikan dengan DNS. Gunakan perintah CLI [vserver services access-check dns forward-lookup](#) NetApp ONTAP untuk mengembalikan alamat IP nama host berdasarkan pencarian di server DNS yang ditentukan atau konfigurasi DNS vs1.

- a. Untuk mengakses ONTAP CLI, buat sesi SSH pada port manajemen Amazon FSx untuk sistem file NetApp ONTAP atau SVM dengan menjalankan perintah berikut. Ganti *management_endpoint_ip* dengan alamat IP port manajemen sistem file.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Untuk informasi selengkapnya, lihat [Mengelola sistem file dengan ONTAP CLI](#).

- b. Masukkan mode lanjutan CLI ONTAP menggunakan perintah berikut.

```
FsxId123456789::> set adv
```

- c. Masukkan perintah berikut, di mana:

- `-vserver vservice_name` menentukan nama mesin virtual penyimpanan (SVM).
- `-hostname host_name` menentukan nama host untuk mencari di server DNS.
- `-node node_name` menentukan nama node di mana perintah dijalankan.
- `-lookup-type` menentukan jenis alamat IP yang akan dicari di server DNS, defaultnya adalah `all`.

```
FsxId123456789::> vservice services access-check dns forward-lookup \  
-vserver vservice_name -node node_name \  
-domains domain_name -name-servers dns_server_ip_address \  
-hostname host_name
```

3. Tinjau [informasi yang perlu Anda miliki](#) saat bergabung dengan SVM ke AD.
4. Tinjau [persyaratan jaringan](#) saat bergabung dengan SVM ke AD.
5. Gunakan prosedur yang dijelaskan [Persyaratan konfigurasi jaringan](#) untuk memperbarui konfigurasi Active Directory SVM Anda menggunakan alamat IP yang benar untuk server DNS Active Directory Anda.

Amazon tidak FSx dapat berkomunikasi dengan Active Directory karena nama domain Active Directory tidak valid.

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx telah mendeteksi FQDN yang disediakan tidak valid. Untuk memperbaiki masalah ini, perbarui konfigurasi Active Directory mesin virtual penyimpanan Anda dengan FQDN yang mematuhi persyaratan konfigurasi.

Untuk mengatasi masalah ini, gunakan prosedur berikut:

1. Tinjau persyaratan nama domain Active Directory lokal yang dijelaskan dalam [Informasi yang dibutuhkan saat bergabung dengan SVM ke Active Directory](#) Pastikan Direktori Aktif yang Anda coba gabungkan memenuhi persyaratan tersebut.
2. Gunakan prosedur yang dijelaskan dalam [Bergabung SVMs ke Active Directory menggunakan Konsol Manajemen AWS, AWS CLI dan API](#) dan coba kembali menggabungkan SVM Anda ke Active Directory. Pastikan untuk menggunakan format yang benar untuk FQDN domain Active Directory.

Akun layanan tidak dapat mengakses grup administrator yang ditentukan dalam konfigurasi SVM Active Directory

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat menerapkan konfigurasi Direktori Aktif Anda. Ini karena grup administrator yang Anda berikan tidak ada atau tidak dapat diakses ke akun layanan yang Anda berikan. Untuk memperbaiki masalah ini, pastikan bahwa konfigurasi jaringan Anda memungkinkan lalu lintas dari SVM ke pengontrol domain Active Directory dan server DNS Anda. Kemudian perbarui konfigurasi Direktori Aktif SVM Anda, berikan server DNS Active Directory Anda dan, tentukan grup administrator di domain yang dapat diakses ke akun layanan yang disediakan.

Untuk mengatasi masalah ini, lakukan solusi berikut:

1. Tinjau informasi tentang [penyediaan grup domain](#) untuk melakukan tindakan administratif pada SVM Anda. Pastikan Anda menggunakan nama yang benar dari grup administrator domain Active Directory.
2. Gunakan prosedur yang dijelaskan dalam [Bergabung SVMs ke Active Directory menggunakan Konsol Manajemen AWS, AWS CLI dan API](#) dan coba kembali menggabungkan SVM Anda ke AD.

Amazon tidak FSx dapat terhubung ke pengontrol domain Direktori Aktif karena unit organisasi yang ditentukan tidak ada atau tidak dapat diakses

Bergabung dengan SVM ke Active Directory yang dikelola sendiri gagal dengan pesan galat berikut:

Amazon FSx tidak dapat membuat koneksi dengan Active Directory Anda. Ini karena unit organisasi yang Anda tentukan tidak ada atau tidak dapat diakses oleh akun layanan yang disediakan. Untuk

memperbaiki masalah ini, perbarui konfigurasi Active Directory mesin virtual penyimpanan Anda, tentukan unit organisasi tempat akun layanan memiliki izin untuk bergabung.

Untuk mengatasi masalah ini, lakukan solusi berikut:

1. Tinjau [prasyarat untuk bergabung dengan SVM ke AD](#).
2. Tinjau [informasi yang perlu Anda miliki](#) saat bergabung dengan SVM ke AD.
3. Coba kembali menggabungkan SVM ke Active Directory menggunakan [prosedur ini dengan unit organisasi yang benar](#).

Anda tidak dapat menghapus penyimpanan mesin virtual atau volume

Masing-masing FSx untuk sistem file ONTAP dapat berisi satu atau lebih penyimpanan virtual machine (SVMs), dan setiap SVM dapat berisi satu atau lebih volume. Saat Anda menghapus sumber daya, Anda harus terlebih dahulu memastikan bahwa semua anak-anaknya telah dihapus. Misalnya, sebelum menghapus SVM, Anda harus terlebih dahulu menghapus semua volume non-root di SVM.

Important

Anda hanya dapat menghapus penyimpanan mesin virtual dengan menggunakan FSx konsol Amazon, API, dan CLI. Anda hanya dapat menghapus volume menggunakan FSx konsol Amazon, API, atau CLI jika volume memiliki FSx cadangan Amazon yang diaktifkan.

Untuk membantu melindungi data dan konfigurasi Anda, Amazon FSx mencegah penghapusan SVMs dan volume dalam keadaan tertentu. Jika Anda mencoba menghapus SVM atau volume, dan permintaan penghapusan Anda tidak berhasil, Amazon FSx memberi Anda informasi di AWS konsol, AWS Command Line Interface (AWS CLI), dan API mengenai alasan sumber daya tidak dihapus. Setelah Anda mengatasi penyebab kegagalan penghapusan, Anda dapat mencoba kembali permintaan penghapusan.

Topik

- [Mengidentifikasi penghapusan yang gagal](#)
- [Penghapusan SVM: Tabel rute tidak dapat diakses](#)

- [Penghapusan SVM: Hubungan teman sebaya](#)
- [SVM atau penghapusan volume: SnapMirror](#)
- [Penghapusan SVM: LIF berkemampuan Kerberos](#)
- [Penghapusan SVM: Alasan lain](#)
- [Penghapusan volume: hubungan FlexCache](#)

Mengidentifikasi penghapusan yang gagal

Saat menghapus FSx SVM atau volume Amazon, Anda biasanya melihat transisi Lifecycle status sumber daya hingga beberapa menit sebelum sumber daya menghilang dari FSx konsol Amazon, CLI, dan API. DELETING

Jika Anda mencoba menghapus sumber daya dan transisi Lifecycle statusnya dari ke DELETING dan kemudian kembali keCREATED, perilaku ini menunjukkan bahwa sumber daya tidak berhasil dihapus. Dalam hal ini, Amazon FSx melaporkan ikon peringatan di konsol di sebelah status CREATED Siklus Hidup. Memilih ikon peringatan menampilkan alasan penghapusan yang gagal.

Alasan paling umum mengapa Amazon FSx mencegah SVM dan penghapusan volume disediakan di bagian berikut, dengan step-by-step petunjuk tentang cara mengatasi masalah ini.

Penghapusan SVM: Tabel rute tidak dapat diakses

Masing-masing FSx untuk sistem file ONTAP membuat satu atau beberapa entri tabel rute untuk menyediakan failover otomatis dan gagal kembali di seluruh Availability Zones. Secara default, entri tabel rute ini dibuat di tabel rute default VPC Anda. Anda dapat secara opsional menentukan satu atau beberapa tabel rute non-default tempat FSx untuk antarmuka ONTAP dapat dibuat. Amazon FSx menandai setiap tabel rute yang dikaitkan dengan sistem file dengan AmazonFSx tag, dan jika tag ini dihapus, itu dapat mencegah Amazon FSx dari dapat menghapus sumber daya. Jika situasi ini terjadi, Anda melihat yang berikutLifecycleTransitionReason:

Amazon FSx is unable to complete the requested storage virtual machine operation because of an inability to access one or more of the route tables associated with your file system. Please contact Dukungan.

Anda dapat menemukan tabel rute sistem file Anda di FSx konsol Amazon dengan menavigasi ke halaman ringkasan sistem file, di bawah tab Jaringan & keamanan.

Memilih tautan tabel rute akan membawa Anda ke tabel rute Anda. Selanjutnya, verifikasi bahwa setiap tabel rute yang terkait dengan sistem file Anda ditandai dengan pasangan kunci-nilai ini:

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

Jika tag ini tidak ada, buat ulang, lalu coba hapus SVM lagi.

Penghapusan SVM: Hubungan teman sebaya

Jika Anda mencoba menghapus SVM atau volume yang merupakan bagian dari hubungan rekan, Anda harus terlebih dahulu menghapus hubungan rekan sebelum menghapus SVM atau volume. Persyaratan ini mencegah peered SVMs menjadi tidak sehat. Jika SVM Anda tidak dapat dihapus karena hubungan teman sebaya, Anda melihat yang berikut ini: LifecycleTransitionReason

Amazon FSx tidak dapat menghapus mesin virtual penyimpanan karena merupakan bagian dari hubungan rekan sejawat atau transisi SVM. Harap hapus hubungan dan coba lagi.

Anda dapat menghapus hubungan rekan SVM melalui CLI ONTAP. Untuk mengakses CLI ONTAP, ikuti langkah-langkahnya. [Mengelola sistem file dengan ONTAP CLI](#) Menggunakan CLI ONTAP, ambil langkah-langkah berikut.

1. Periksa hubungan rekan SVM dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789::> vserver peer show -vserver svm_name
```

Jika perintah ini berhasil, Anda akan melihat output yang mirip dengan berikut ini:

Vserver	Peer Vserver	Peer State	Peer Cluster	Peering Applications	Remote Vserver
<i>svm_name</i>	test2	peered	FsxId02d81fef0d84734b6	snapmirror	fsxDest
<i>svm_name</i>	test3	peered	FsxId02d81fef0d84734b6	snapmirror	fsxDest

2 entries were displayed.

2. Hapus setiap hubungan rekan SVM dengan menggunakan perintah berikut. Ganti *svm_name*, dan *remote_svm_name* dengan nilai aktual Anda.

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-  
vserver remote_svm_name
```

Jika perintah ini berhasil, Anda akan melihat output berikut:

```
Info: 'vserver peer delete' command is successful.
```

SVM atau penghapusan volume: SnapMirror

Sama seperti Anda tidak dapat menghapus SVM dengan hubungan rekan tanpa terlebih dahulu menghapus hubungan rekan (lihat [Penghapusan SVM: Hubungan teman sebaya](#)), Anda tidak dapat menghapus SVM yang memiliki SnapMirror hubungan tanpa terlebih dahulu menghapus hubungan tersebut. SnapMirror Untuk menghapus SnapMirror hubungan, gunakan ONTAP CLI untuk mengambil langkah-langkah berikut pada sistem file yang menjadi tujuan hubungan. SnapMirror Untuk mengakses CLI ONTAP, ikuti langkah-langkahnya. [Mengelola sistem file dengan ONTAP CLI](#)

Note

FSx Cadangan Amazon digunakan SnapMirror untuk membuat point-in-time, backup tambahan dari volume sistem file Anda. Anda tidak dapat menghapus SnapMirror hubungan ini untuk cadangan Anda di CLI ONTAP. Namun, hubungan ini secara otomatis dihapus ketika Anda menghapus volume melalui AWS CLI, API, atau konsol.

1. Buat daftar SnapMirror hubungan Anda pada sistem file tujuan dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

Jika perintah ini berhasil, Anda akan melihat output yang mirip dengan berikut ini:

Source Path	Destination Type	Path	Mirror State	Relationship Status	Total Progress	Last Healthy	Last Updated
sourceSvm:sourceVol	XDP	destSvm:destVol	Snapmirrored				

Idle	-	true	-

2. Hapus SnapMirror hubungan Anda dengan menjalankan perintah berikut pada sistem file tujuan.

```
FsxId123456789abcdef:> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

Penghapusan SVM: LIF berkemampuan Kerberos

Jika Anda mencoba menghapus SVM yang memiliki antarmuka logis (LIF) dengan Kerberos diaktifkan, Anda harus menonaktifkan Kerberos terlebih dahulu pada LIF itu sebelum menghapus SVM.

Anda dapat menonaktifkan Kerberos pada LIF melalui CLI ONTAP. Untuk mengakses CLI ONTAP, ikuti langkah-langkahnya. [Mengelola sistem file dengan ONTAP CLI](#)

1. Masuk ke mode diagnostik di CLI ONTAP dengan menggunakan perintah berikut.

```
FsxId123456789abcdef:> set diag
```

Saat diminta untuk melanjutkan, masukkan **y**.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

2. Periksa antarmuka mana yang mengaktifkan Kerberos. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef:> kerberos interface show -vserver svm_name
```

Jika perintah ini berhasil, Anda akan melihat output yang mirip dengan berikut ini:

```
(vserver nfs kerberos interface show)
      Logical
Vserver  Interface      Address      Kerberos SPN
-----  -
svm_name  nfs_smb_management_1
                               10.19.153.48  enabled
5 entries were displayed.
```

- Nonaktifkan LIF Kerberos dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda. Anda harus memberikan nama pengguna dan kata sandi Direktori Aktif yang Anda gunakan untuk menggabungkan SVM ini ke Direktori Aktif Anda.

```
FsxId123456789abcdef:> kerberos interface disable -vserver svm_name -lif
nfs_smb_management_1
```

Jika perintah ini berhasil, Anda akan melihat output berikut. Berikan nama pengguna dan kata sandi Direktori Aktif yang Anda gunakan untuk menggabungkan SVM ini ke Direktori Aktif Anda. Saat diminta untuk melanjutkan, masukkan **y**.

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *****

Warning: This command deletes the service principal name from the machine account
on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

- Verifikasi bahwa Kerberos dinonaktifkan pada SVM dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef:> kerberos interface show -vserver svm_name
```

Jika perintah ini berhasil, Anda akan melihat output yang mirip dengan berikut ini:

```
(vserver nfs kerberos interface show)

      Logical
Vserver  Interface      Address      Kerberos SPN
-----  -
svm_name  nfs_smb_management_1
                               10.19.153.48  disabled

5 entries were displayed.
```

- Jika antarmuka ditampilkan sebagai *disabled*, coba hapus SVM lagi melalui AWS CLI, API, atau konsol.

Jika Anda tidak dapat menghapus LIF dengan menggunakan perintah sebelumnya, Anda dapat menghapus paksa LIF Kerberos dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

 Important

Perintah berikut dapat untai objek komputer SVM Anda di Active Directory Anda.

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif  
nfs_smb_management_1 -force true
```

Jika perintah ini berhasil, Anda akan melihat output yang mirip dengan berikut ini. Saat diminta untuk melanjutkan, masukkan **y**.

```
(vserver nfs kerberos interface disable)
```

```
Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver  
"svm_name" will be deleted.
```

```
The corresponding account on the KDC will not be deleted. Do you want to continue?  
{y|n}: y
```

Penghapusan SVM: Alasan lain

FSx untuk ONTAP SVMs membuat objek komputer di Active Directory Anda ketika mereka bergabung dengan Active Directory Anda. Dalam beberapa kasus, Anda mungkin ingin secara manual memutuskan sambungan SVM dari Active Directory Anda dengan menggunakan ONTAP CLI. Untuk mengakses CLI ONTAP, ikuti langkah-langkahnya, [Mengelola sistem file dengan ONTAP CLI](#) masuk ke CLI ONTAP di tingkat sistem file dengan kredensial. fsxadmin Menggunakan CLI ONTAP, ambil langkah-langkah berikut untuk memutuskan sambungan SVM dari Active Directory Anda.

 Important

Prosedur ini dapat untai objek komputer SVM Anda di Active Directory Anda.

1. Masuk ke mode lanjutan di CLI ONTAP dengan menggunakan perintah berikut.

```
FsxId123456789abcdef:> set adv
```

Setelah menjalankan perintah ini, Anda akan melihat output ini. Masuk **y** untuk melanjutkan.

```
Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y
```

2. Hapus DNS untuk Active Directory Anda dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef:> vserver services name-service dns dynamic-update record
delete -vserver svm_name -lif nfs_smb_management_1
```

Note

Jika catatan DNS telah dihapus atau jika server DNS tidak dapat dijangkau, perintah ini gagal. Jika itu terjadi, lanjutkan dengan langkah berikutnya.

3. Nonaktifkan DNS dengan menggunakan perintah berikut. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef:> vserver services name-service dns dynamic-update modify -
vserver svm_name -is-enabled false -use-secure false
```

Jika perintah ini berhasil, Anda akan melihat output berikut:

```
Warning: DNS updates for Vserver "svm_name" are now disabled.
        Any LIFs that are subsequently modified or deleted
        can result in a stale DNS entry on the DNS server,
        even when DNS updates are enabled again.
```

4. Putuskan sambungan perangkat dari Active Directory. Ganti *svm_name* dengan nama SVM Anda.

```
FsxId123456789abcdef:> vserver cifs delete -vserver svm_name
```

Setelah menjalankan perintah ini, Anda akan melihat output berikut, di **CORP.EXAMPLE.COM** mana diganti dengan nama domain Anda. Saat diminta, masukkan nama pengguna dan kata sandi Anda. Ketika ditanya apakah Anda ingin menghapus server, masukkan **y**.

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
server.
Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

Penghapusan volume: hubungan FlexCache

Anda tidak dapat menghapus volume yang merupakan volume asal untuk suatu FlexCache hubungan kecuali Anda menghapus hubungan cache terlebih dahulu. Untuk menentukan volume mana yang memiliki FlexCache hubungan, Anda dapat menggunakan CLI ONTAP. Untuk mengakses CLI ONTAP, ikuti langkah-langkahnya. [Mengelola sistem file dengan ONTAP CLI](#)

1. Periksa FlexCache hubungan dengan menggunakan perintah berikut.

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. Hapus setiap hubungan cache dengan menggunakan perintah berikut. Ganti **dest_svm_name**, dan **dest_vol_name** dengan nilai aktual Anda.

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. Setelah Anda menghapus hubungan cache, coba hapus SVM Anda melalui AWS CLI, API, atau konsol lagi.

Volume Anda dalam **MISCONFIGURED** keadaan

Ada sejumlah penyebab potensial untuk volume ONTAP untuk masuk ke MISCONFIGURED keadaan, dijelaskan dalam topik berikut.

Volume Anda lebih dari 98% penuh

Sistem file Anda saat ini berisi volume yang lebih dari 98% penuh. Kami menyarankan agar Anda tidak melebihi 95% pemanfaatan volume Anda secara berkelanjutan. Jika Anda tidak mengosongkan ruang dalam volume sebelum jendela pemeliharaan sistem file Anda berikutnya, Amazon FSx akan menonaktifkan penguncian oportunistik pada volume, merusak “oplocks” yang ada. Amazon FSx akan mengaktifkan kembali oplocks pada volume setelah proses patching selesai. Untuk menghindari hal ini, harap kurangi pemanfaatan kapasitas penyimpanan volume hingga di bawah 98%. Beberapa cara untuk mencapai ini termasuk:

- Meningkatkan ukuran volume.
- Menghapus data yang tidak dibutuhkan.
- Menghapus snapshot yang tidak dibutuhkan.

Untuk informasi selengkapnya, lihat [Memperbarui kapasitas penyimpanan](#), dan [Menghapus snapshot](#).

Volume offline Anda memiliki iSCSI LUN atau namespace NVMe/TCP

Sistem file Anda saat ini meng-host volume yang dalam keadaan offline, dan volume itu berisi iSCSI LUN, atau namespace, atau keduanya NVMe/TCP . Kami menyarankan agar Anda menyimpan volume online secara berkelanjutan. Jika Anda tidak online volume ini sebelum jendela pemeliharaan sistem file Anda berikutnya, Amazon FSx akan online sementara volume ini selama durasi operasi penambalan. Untuk menghindari hal ini, silakan online atau hapus volume.

Untuk mengembalikan volume offline secara online, gunakan perintah [volume online](#)ONTAPCLI, seperti yang ditunjukkan pada contoh berikut. Jika hanya ada satu SVM (Vserver), Anda tidak perlu menentukan parameternya. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Volume offline Anda adalah FlexCache asal

Sistem file Anda berisi volume FlexCache asal yang dalam keadaan offline. Kami menyarankan agar Anda menyimpan volume online secara berkelanjutan. Jika Anda tidak online volume ini sebelum jendela pemeliharaan sistem file Anda berikutnya, Amazon FSx akan online sementara volume ini selama durasi operasi penambalan. Selama waktu ini, ada kemungkinan bahwa data akan ditulis kembali ke volume FlexCache asal dengan data dari volume cache. Untuk menghindari hal ini, silakan online atau hapus volume.

Untuk mengembalikan volume offline secara online, gunakan perintah [volume online](#)ONTAPCLI, seperti yang ditunjukkan pada contoh berikut. Jika hanya ada satu SVM (Vserver), Anda tidak perlu menentukan parameternya. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Volume offline Anda adalah bagian dari suatu SnapMirror hubungan

Sistem file Anda saat ini meng-host volume yang dalam keadaan offline, dan volume itu adalah SnapMirror sumber atau tujuan. Kami menyarankan agar Anda menyimpan volume online secara berkelanjutan. Jika Anda tidak online volume ini sebelum jendela pemeliharaan sistem file Anda berikutnya, Amazon FSx akan online sementara volume ini selama durasi operasi penambalan dan menjeda hubungan. SnapMirror Selama waktu ini, ada kemungkinan bahwa data akan ditulis ke volume SnapMirror tujuan dengan data dari volume SnapMirror sumber. Untuk menghindari hal ini, silakan online atau hapus volume.

Untuk mengembalikan volume offline secara online, gunakan perintah [volume online](#)ONTAPCLI, seperti yang ditunjukkan pada contoh berikut. Jika hanya ada satu SVM (Vserver), Anda tidak perlu menentukan parameternya. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Volume terbatas Anda berisi iSCSI LUN atau namespace NVMe/TCP

Sistem file Anda saat ini meng-host volume yang berada dalam keadaan terbatas, dan volume tersebut berisi iSCSI LUN, namespace, NVMe/TCP atau keduanya. Kami menyarankan agar Anda

menyimpan volume online secara berkelanjutan. Jika Anda tidak online volume ini sebelum jendela pemeliharaan sistem file Anda berikutnya, Amazon FSx akan online sementara volume ini selama durasi operasi penambalan. Untuk menghindari hal ini, silakan online atau hapus volume.

Untuk mengembalikan volume offline secara online, gunakan perintah [volume online](#) ONTAPCLI, seperti yang ditunjukkan pada contoh berikut. Jika hanya ada satu SVM (Vserver), Anda tidak perlu menentukan parameternya. `-vserver`

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Volume terbatas Anda adalah FlexCache asal

Sistem file Anda berisi volume FlexCache asal yang dalam keadaan terbatas. Kami menyarankan agar Anda menyimpan volume online secara berkelanjutan. Jika Anda tidak online volume ini sebelum jendela pemeliharaan sistem file Anda berikutnya, Amazon FSx akan online sementara volume ini selama durasi operasi penambalan. Selama waktu ini, ada kemungkinan bahwa data akan ditulis kembali ke volume FlexCache asal dengan data dari volume cache. Untuk menghindari hal ini, silakan online atau hapus volume.

Untuk mengembalikan volume offline secara online, gunakan perintah [volume online](#) ONTAPCLI, seperti yang ditunjukkan pada contoh berikut. Jika hanya ada satu SVM (Vserver), Anda tidak perlu menentukan parameternya. `-vserver`

```
FsxID-abcdef123456:> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Volume terbatas Anda adalah bagian dari suatu SnapMirror hubungan

Sistem file Anda saat ini meng-host volume yang dalam keadaan terbatas, dan volume itu adalah SnapMirror sumber atau tujuan. Kami menyarankan agar Anda menyimpan volume online secara berkelanjutan. Jika Anda tidak online volume ini sebelum jendela pemeliharaan sistem file Anda berikutnya, Amazon FSx akan online sementara volume ini selama durasi operasi penambalan dan menjeda hubungan. SnapMirror Selama waktu ini, ada kemungkinan bahwa data akan ditulis ke volume SnapMirror tujuan dengan data dari volume SnapMirror sumber. Untuk menghindari hal ini, silakan online atau hapus volume.

Untuk mengembalikan volume offline secara online, gunakan perintah [volume online](#) ONTAP CLI, seperti yang ditunjukkan pada contoh berikut. Jika hanya ada satu SVM (Vserver), Anda tidak perlu menentukan parameternya. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name
```

```
Volume 'vs1:vol1' is now online.
```

Volume Anda memiliki kapasitas penyimpanan yang tidak mencukupi

Jika Anda kehabisan ruang pada volume Anda, Anda dapat menggunakan prosedur yang ditunjukkan di sini untuk mendiagnosis dan menyelesaikan situasi.

Topik

- [Tentukan bagaimana kapasitas penyimpanan volume Anda digunakan](#)
- [Meningkatkan kapasitas penyimpanan volume](#)
- [Menggunakan autosizing volume](#)
- [Penyimpanan utama sistem file Anda penuh](#)
- [Menghapus snapshot](#)
- [Meningkatkan kapasitas file maksimum volume](#)

Tentukan bagaimana kapasitas penyimpanan volume Anda digunakan

Anda dapat melihat bagaimana kapasitas penyimpanan volume Anda dikonsumsi dengan menggunakan perintah `volume show-space` NetApp ONTAP CLI. Informasi ini dapat membantu Anda membuat keputusan tentang cara merebut kembali atau menghemat kapasitas penyimpanan volume. Untuk informasi selengkapnya, lihat [Untuk memantau kapasitas penyimpanan volume \(konsol\)](#).

Meningkatkan kapasitas penyimpanan volume

Anda dapat meningkatkan kapasitas penyimpanan volume dengan menggunakan FSx konsol Amazon, AWS CLI, dan Amazon FSx API. Untuk informasi lebih lanjut tentang memperbarui volume dengan kapasitas yang meningkat, lihat [Memperbarui volume](#).

Atau, Anda dapat meningkatkan kapasitas penyimpanan volume menggunakan perintah [volume modify](#) NetApp ONTAP CLI. Untuk informasi selengkapnya, lihat [Untuk mengubah kapasitas penyimpanan volume \(konsol\)](#).

Menggunakan autosizing volume

Anda dapat menggunakan autosizing volume sehingga volume secara otomatis tumbuh dengan jumlah tertentu, atau ke ukuran tertentu ketika mencapai ambang ruang yang digunakan. Anda dapat melakukan ini untuk tipe FlexVol volume, yang merupakan tipe volume default FSx untuk ONTAP, menggunakan perintah ONTAP [volume autosize](#) NetApp CLI. Untuk informasi selengkapnya, lihat [Mengaktifkan autosizing](#).

Penyimpanan utama sistem file Anda penuh

Jika penyimpanan utama sistem file ONTAP Anda FSx penuh, Anda tidak dapat menambahkan data lagi ke volume dalam sistem file Anda, bahkan jika volume menunjukkan bahwa ia memiliki kapasitas penyimpanan yang cukup tersedia. Anda dapat melihat jumlah kapasitas penyimpanan utama yang tersedia di tab Pemantauan & kinerja pada halaman detail sistem file di FSx konsol Amazon. Untuk informasi selengkapnya, lihat [Memantau pemanfaatan penyimpanan SSD](#)

Untuk mengatasi masalah ini, Anda dapat meningkatkan ukuran tingkat penyimpanan utama sistem file Anda. Untuk informasi selengkapnya, lihat [Memperbarui penyimpanan SSD sistem file dan IOPS](#).

Menghapus snapshot

Snapshot diaktifkan secara default pada volume Anda, menggunakan kebijakan snapshot default. Snapshot disimpan di `.snapshot` direktori di root volume. Anda dapat mengelola kapasitas penyimpanan volume sehubungan dengan snapshot dengan cara berikut:

- [Hapus snapshot secara manual](#) — merebut kembali kapasitas penyimpanan dengan menghapus snapshot secara manual.
- [Buat kebijakan penghapusan otomatis snapshot — buat kebijakan](#) yang menghapus snapshot lebih agresif daripada kebijakan snapshot default.
- [Matikan snapshot otomatis](#) — hemat kapasitas penyimpanan dengan mematikan snapshot otomatis.

Saat Anda menghapus snapshot, Anda tidak merebut kembali jumlah penyimpanan yang sama dengan ukuran snapshot yang Anda hapus. Anda dapat melihat jumlah penyimpanan yang dapat

Anda reklamasi saat menghapus snapshot dengan menggunakan perintah [volume snapshot compute-reclaimable ONTAP -vserver](#) CLI, menggunakan data Anda untuk mengganti,, dan.

svm_name vol_name snapshot_name

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name  
-snapshot snapshot_name  
A total of 667648 bytes can be reclaimed.
```

Untuk informasi selengkapnya tentang menghapus snapshot dan mengelola kebijakan snapshot untuk menghemat kapasitas penyimpanan, lihat. [Menghapus snapshot](#)

Meningkatkan kapasitas file maksimum volume

Volume FSx untuk ONTAP dapat kehabisan kapasitas file ketika jumlah inode yang tersedia, atau pointer file, habis. Secara default, jumlah inode yang tersedia pada volume adalah 1 untuk setiap 32KiB ukuran volume. Untuk informasi selengkapnya, lihat [Kapasitas file volume](#).

Jumlah inode dalam volume meningkat sepadan dengan kapasitas penyimpanan volume, hingga ambang batas 648 GiB. Secara default, volume yang memiliki kapasitas penyimpanan 648 GiB atau lebih semuanya memiliki jumlah inode yang sama, 21.251.126. Untuk melihat kapasitas file maksimum volume, lihat [Memantau kapasitas file volume](#).

Jika Anda membuat volume lebih besar dari 648 GiB, dan Anda ingin memiliki lebih dari 21.251.126 inode, Anda harus meningkatkan jumlah maksimum file pada volume secara manual. Jika volume Anda kehabisan kapasitas penyimpanan, Anda dapat memeriksa kapasitas file maksimumnya. Jika mendekati kapasitas filenya, Anda dapat meningkatkannya secara manual. Untuk informasi selengkapnya, lihat [Untuk meningkatkan jumlah maksimum file pada volume \(ONTAPCLI\)](#).

Pencadangan Anda gagal karena kapasitas volume yang tidak mencukupi

Pencadangan harian otomatis volume Anda gagal dengan pesan berikut:

```
Amazon FSx could not create a backup of your volume because the backup snapshot was  
deleted.
```

Pencadangan harian otomatis gagal karena kapasitas penyimpanan gratis tidak mencukupi pada volume. Untuk mengurangi kondisi ini, Anda perlu mengosongkan kapasitas penyimpanan pada

volume. Anda dapat melakukannya dengan menggunakan satu atau lebih opsi berikut, tergantung pada situasi Anda:

- [Meningkatkan kapasitas penyimpanan volume](#)
- [Tingkatkan cadangan snapshot volume](#)
- [Nonaktifkan penghapusan otomatis snapshot](#)
- [Jangan hapus snapshot cadangan menggunakan ONTAP CLI](#)

Memulihkan dihapus FSx untuk volume ONTAP

Ketika volume FSx untuk ONTAP dihapus, itu ditempatkan dalam antrian ONTAP's pemulihan. Meskipun Anda dapat memulihkan volume langsung dari antrian ini menggunakan ONTAP CLI, volume yang dipulihkan tidak akan muncul kembali di AWS konsol atau FSx Amazon API dan tag AWS apa pun yang sebelumnya diterapkan ke volume akan hilang secara permanen. Untuk memulihkan volume ONTAP dengan benar sambil mempertahankan AWS integrasi dan kebijakan keamanan berbasis tag, Anda dapat [memulihkan cadangan ke volume baru](#) atau [mereplikasi data volume ke volume baru menggunakan](#) FSx SnapMirror Untuk informasi selengkapnya tentang antrian ONTAP's pemulihan, lihat [NetApp's dokumentasi](#).

Memecahkan masalah jaringan

Jika Anda mengalami masalah jaringan, Anda dapat menggunakan prosedur yang ditampilkan di sini untuk mendiagnosis masalah.

Anda ingin menangkap jejak paket

Packet tracing adalah proses memverifikasi jalur paket melalui lapisan ke tujuannya. Anda mengontrol proses pelacakan paket dengan perintah CLI berikut NetApp ONTAP:

- `network tcpdump start`— Memulai penelusuran paket
- `network tcpdump show`— Menunjukkan jejak paket yang sedang berjalan
- `network tcpdump stop`— Menghentikan jejak paket yang sedang berjalan

Perintah ini tersedia untuk pengguna yang memiliki `fsxadmin` peran pada sistem file Anda.

Untuk menangkap jejak paket dari sistem file Anda

1. Untuk SSH ke dalam NetApp ONTAP CLI sistem file Anda, ikuti langkah-langkah yang didokumentasikan di bagian [Menggunakan CLI NetApp ONTAP](#) Panduan Pengguna FSx Amazon NetApp untuk ONTAP.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Masukkan tingkat hak istimewa diagnostik di CLI ONTAP dengan menggunakan perintah berikut.

```
::> set diag
```

Saat diminta untuk melanjutkan, masukkan.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

3. Identifikasi lokasi pada sistem file Anda di mana Anda ingin menyimpan jejak paket Anda. Volume harus online dan harus dipasang di namespace dengan jalur persimpangan yang valid. Gunakan perintah berikut untuk memeriksa volume yang memenuhi kriteria tersebut:

```
::*> volume show -junction-path !- -fields junction-path
vserver volume    junction-path
-----
fsx      test_vol1 /test_vol1
fsx      test_vol2 /test_vol2
fsx      test_vol2 /test_vol3
```

4. Mulai jejak dengan argumen minimum yang diperlukan. Ganti yang berikut ini:
 - Ganti *node_name* dengan nama node (misalnya, FsxId01234567890abcdef-01).
 - Ganti *svm_name* dengan nama mesin virtual penyimpanan Anda (misalnya, fsx).
 - Ganti *junction_path_name* dengan nama volume (misalnya, test-vol1).

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
packet traces are occurring. Use the
```

```
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
disable Snapshots on the
tcpdump destination volume.
```

Important

Jejak paket hanya dapat ditangkap pada e0e antarmuka dan di ruang Default IP. FSx Untuk ONTAP, semua lalu lintas jaringan menggunakan e0e antarmuka.

Saat menggunakan packet tracing, ingatlah hal berikut:

- Saat memulai jejak paket, Anda harus menyertakan jalur ke tempat Anda ingin menyimpan file jejak, dalam format ini: *svm_name /clus//junction-path-name*
- Secara opsional, berikan nama file untuk jejak paket. Jika filter_name tidak ditentukan, maka secara otomatis dihasilkan dalam bentuk: *node-name __.trc port-name yyyymmdd_hhmmss*
- Jika jejak bergulir ditentukan, filter_name diakhiran dengan angka yang menunjukkan posisi dalam urutan rotasi.
- CLI ONTAP juga menerima argumen opsional berikut: -pass-through

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
<filter-expression>
```

- Untuk informasi tentang ekspresi filter, lihat halaman manual [pcap-filter \(7\)](#).

5. Lihat jejak yang sedang berlangsung:

```
::*> debug network tcpdump show
```

Node	IPspace	Port	Filename
-----	-----	-----	-----

```
FsxId123456789abcdef-01 Default e0e /clus/fsx/test_vol1/  
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. Hentikan jejaknya:

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -  
port e0e  
Info: Stopped network trace on interface "e0e"
```

7. Kembali ke tingkat hak istimewa admin:

```
::*> set -priv admin  
::>
```

8. Akses jejak paket.

Jejak paket Anda disimpan dalam volume yang Anda tentukan menggunakan debug network tcpdump start perintah, dan dapat diakses melalui ekspor NFS atau berbagi SMB yang sesuai dengan volume itu.

Untuk informasi selengkapnya tentang menangkap jejak paket, lihat [Cara menggunakan dump jaringan debug di ONTAP 9.10+ di](#) NetApp Knowledge Base

Memecahkan masalah I/O kesalahan dan kegagalan klaim kembali kunci NFS

Bagian ini menjelaskan masalah yang terkait dengan I/O kesalahan dan kegagalan reklamasi kunci NFS selama peristiwa failover aktif untuk sistem file ONTAP dan resolusi FSx untuk masing-masingnya.

Anda mengalami I/O kesalahan selama peristiwa failover

Selama failovers aktif FSx untuk sistem file ONTAP Single-AZ, klien NFS mungkin mengalami kesalahan sementara I/O atau jeda yang diperpanjang. Untuk klien NFSv4 +, Anda mungkin melihat pesan log kernel seperti:

```
NFS: __nfs4_reclaim_open_state: Lock reclaim failed!
```

Pesan-pesan ini menunjukkan bahwa klien tidak dapat berhasil merebut kembali kunci NFS selama jendela failover.

Untuk mengurangi I/O kesalahan selama peristiwa failover

Di Linux, Anda dapat mengonfigurasi pengaturan jaringan pada klien Anda untuk mengurangi waktu deteksi failover dari 55-60 detik menjadi 15-20 detik.

⚠ Important

Selalu uji konfigurasi ini di lingkungan non-produksi terlebih dahulu. Pengaturan ini meningkatkan lalu lintas Address Resolution Protocol (ARP), yang digunakan untuk memetakan alamat IP ke alamat fisik (MAC) di jaringan lokal, dan mungkin tidak cocok untuk lingkungan yang dibatasi jaringan.

Untuk mengkonfigurasi pengaturan jaringan yang dioptimalkan untuk klien NFS

1. Buat file konfigurasi sysctl pada setiap klien NFS. Contoh berikut digunakan default untuk menerapkan pengaturan ke semua antarmuka jaringan. Jika instans Anda memiliki beberapa antarmuka jaringan, Anda dapat mengganti default dengan nama antarmuka tertentu (misalnya, eth0 atau ens5) yang digunakan untuk menyambung ke sistem file ONTAP Single-AZ Anda FSx :

```
$ sudo tee /etc/sysctl.d/99-fsx-failover.conf > /dev/null << 'EOF'
# NFS client optimizations for faster failover detection
# Replace 'default' with your interface name (e.g., eth0, ens5) to target a
specific interface
net.ipv4.neigh.default.base_reachable_time_ms=5000
net.ipv4.neigh.default.delay_first_probe_time=1
net.ipv4.neigh.default.ucast_solicit=0
net.ipv4.tcp_syn_retries=3
EOF
```

2. Terapkan pengaturan segera:

```
$ sudo sysctl -p /etc/sysctl.d/99-fsx-failover.conf
```

3. Verifikasi konfigurasi aktif. Jika Anda menggunakan default, Anda dapat memverifikasi dengan perintah berikut. Jika Anda menentukan antarmuka tertentu, ganti default dengan nama antarmuka Anda (misalnya, eth0 atau ens5):

```
$ sysctl net.ipv4.neigh.default.base_reachable_time_ms
$ sysctl net.ipv4.neigh.default.delay_first_probe_time
$ sysctl net.ipv4.neigh.default.ucast_solicit
$ sysctl net.ipv4.tcp_syn_retries
```

Pastikan pengaturan ini diterapkan secara konsisten di semua klien NFS yang terhubung ke sistem file ONTAP Anda FSx dalam Availability Zone yang sama. Saat menggunakan pengoptimalan jaringan ini, ingatlah hal berikut:

- `base_reachable_time_ms=5000` - Mengurangi validitas entri cache ARP dari 30 detik menjadi 5 detik, memungkinkan klien mendeteksi perubahan kepemilikan IP lebih cepat selama peristiwa failover.
- `delay_first_probe_time=1` - Mengurangi penundaan sebelum memeriksa entri jaringan basi dari 5 detik menjadi 1 detik.
- `ucast_solicit=0` - Melewatkan probe tetangga unicast dan segera mengeluarkan permintaan ARP siaran, mempercepat penemuan kembali server file aktif.
- `tcp_syn_retries=3` - Mengurangi durasi coba lagi koneksi TCP dari 127 detik menjadi 15 detik.

Setelah pengaturan jaringan di tempat, Anda harus memantau lingkungan Anda untuk memvalidasi perubahan. Anda dapat menguji peristiwa failover dengan memodifikasi kapasitas throughput sistem file Anda. Untuk informasi selengkapnya, lihat [Menguji failover pada sebuah sistem file](#).

Memantau lingkungan Anda setelah menerapkan perubahan

- Pantau log sistem untuk kesalahan NFS untuk melihat pesan log kernel terkait NFS.

```
$ sudo journalctl -f | grep -i nfs
```

Verifikasi bahwa ada lebih sedikit kemunculan pesan seperti `Lock reclaim failed`.

- Pantau log aplikasi untuk mengonfirmasi lebih sedikit I/O waktu tunggu, kesalahan koneksi, dan kegagalan terkait coba ulang selama peristiwa failover.
- Validasi dampak jaringan untuk memastikan bahwa peningkatan lalu lintas ARP tidak mempengaruhi kinerja jaringan di lingkungan Anda.

Pendekatan alternatif untuk NFSv4 lingkungan

Di NFSv4 lingkungan di mana memodifikasi konfigurasi sisi klien tidak layak, pertimbangkan alternatif berikut:

- Perpanjang batas waktu NFSv4 sewa. Bekerja dengan administrator penyimpanan Anda untuk meningkatkan batas waktu NFSv4 sewa. Memperpanjang batas waktu ini memberi klien waktu tambahan untuk merebut kembali kunci selama peristiwa failover. Untuk informasi selengkapnya, lihat [Menentukan masa tenggang NFSv4 penguncian](#) dalam NetApp ONTAP dokumentasi.

Riwayat Dokumen untuk Amazon FSx untuk NetApp ONTAP

- Versi API: 2018-03-01
- Pembaruan dokumentasi terbaru: 16 Oktober 2025

Tabel berikut menjelaskan perubahan penting pada Panduan Pengguna Amazon FSx NetApp ONTAP. Untuk notifikasi tentang pembaruan dokumentasi, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Support ditambahkan untuk jalur akses Amazon S3 untuk Amazon FSx untuk ONTAP NetApp	Jalur akses Amazon S3 FSx untuk Amazon untuk NetApp ONTAP menyediakan cara baru untuk mengakses data yang disimpan untuk sistem file ONTAP menggunakan API Amazon S3. FSx Dengan jalur akses Amazon S3, Anda dapat menyederhanakan akses data untuk aplikasi berkemampuan Amazon S3 tanpa memerlukan perubahan pada konfigurasi sistem file yang ada. Untuk informasi selengkapnya, lihat Menggunakan jalur akses Amazon S3 FSx untuk Amazon untuk NetApp ONTAP .	Desember 2, 2025
Support ditambahkan untuk AWS Secrets Manager integrasi	Amazon FSx sekarang terintegrasi dengan AWS Secrets Manager pengelola kredensial Active Directory yang ditingkatkan. Untuk informasi selengkapnya, lihat Menyimpan kredensial Direktori	November 5, 2025

	Aktif menggunakan. AWS Secrets Manager	
Amazon FSx ConsoleFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru, <code>secretsmanager:ListSecrets</code> , yang memungkinkan kepala sekolah untuk membuat daftar rahasia AWS Secrets Manager untuk memilih kredensi akun layanan bergabung dengan domain. Untuk informasi selengkapnya, lihat kebijakan AWS terkelola: Amazon FSx FullAccess .	November 5, 2025
NetApp BlueXPberganti nama menjadi NetApp Console	NetApp BlueXP sekarang dikenal sebagai NetApp Console. Untuk informasi selengkapnya, lihat Menggunakan NetApp Konsol .	Oktober 16, 2025
Support ditambahkan untuk Internet Protocol versi 6 (IPv6)	FSx untuk sistem file ONTAP sekarang mendukung dua opsi jenis jaringan: IPv4 - only dan dual-stack (untuk keduanya dan). IPv4 IPv6 Anda harus menentukan salah satu opsi tersebut saat membuat sistem file Anda. Anda dapat mengubah jenis jaringan yang ada FSx untuk sistem file ONTAP kapan saja. Untuk informasi selengkapnya, lihat Mengelola jenis jaringan .	September 30, 2025

[Wilayah AWS Dukungan
tambahan ditambahkan](#)

Generasi kedua (Multi-AZ 2 dan Single-AZ 2) FSx untuk sistem file ONTAP sekarang tersedia di Asia Pasifik (Seoul), Kanada (Tengah), Eropa (Spanyol), dan Eropa (Zurich). Untuk informasi selengkapnya, lihat [Ketersediaan oleh Wilayah AWS](#).

September 30, 2025

[Wilayah AWS Dukungan
tambahan ditambahkan](#)

FSx untuk sistem file ONTAP sekarang tersedia di Wilayah Asia Pasifik (Taipei). Untuk informasi selengkapnya, lihat [Ketersediaan oleh Wilayah AWS](#).

Agustus 18, 2025

[Support ditambahkan untuk
mengurangi kapasitas
penyimpanan SSD](#)

FSx untuk ONTAP sekarang memungkinkan Anda untuk mengurangi kapasitas penyimpanan solid-state drive (SSD) sistem file Anda pada sistem file generasi kedua, memungkinkan Anda untuk mengoptimalkan biaya penyimpanan untuk beban kerja dengan berbagai kebutuhan penyimpanan kinerja tinggi. Untuk informasi selengkapnya, lihat [Kapan mengurangi kapasitas penyimpanan SSD](#).

Agustus 14, 2025

[Amazon FSx memperbarui kebijakan FSx ServiceRolePolicy AWS terkelola Amazon](#)

Amazon FSx menambahkan `ec2:AssignIpv6Addresses` dan `ec2:UnassignIpv6Addresses` izin ke Amazon FSxServiceRolePolicy. Untuk informasi selengkapnya, lihat [Amazon FSx memperbarui kebijakan AWS terkelola](#).

Juli 22, 2025

[Amazon FSx memperbarui kebijakan FSx FullAccess AWS terkelola Amazon](#)

Kebijakan FSx FullAccess terkelola [Amazon](#) telah diperbarui untuk menambahkan `fsx:CreateAndAttachS3AccessPoint`, `fsx:DescribeS3AccessPointAttachments`, dan `fsx:DetachAndDeleteS3AccessPoint` izin.

Juni 25, 2025

[Amazon FSx memperbarui kebijakan FSx ConsoleFullAccess AWS terkelola Amazon](#)

Kebijakan FSx ConsoleFullAccess terkelola [Amazon](#) telah diperbarui untuk menambahkan `fsx:CreateAndAttachS3AccessPoint`, `fsx:DescribeS3AccessPointAttachments`, dan `fsx:DetachAndDeleteS3AccessPoint` izin.

Juni 25, 2025

FSx untuk ONTAP mendukung Amazon Elastic Service VMware	FSx untuk ONTAP sekarang dapat digunakan sebagai datastore eksternal untuk Amazon EVS. Untuk informasi selengkapnya, lihat Menggunakan Amazon Elastic VMware Service with FSx for ONTAP .	Juni 9, 2025
Wilayah AWS Dukungan tambahan ditambahkan	Generasi kedua (Multi-AZ 2 dan Single-AZ 2) FSx untuk sistem file ONTAP sekarang tersedia di Asia Pasifik (Tokyo) dan Asia Pasifik (Mumbai). Untuk informasi selengkapnya, lihat Ketersediaan oleh Wilayah AWS .	Juni 2, 2025
Support ditambahkan untuk modus FlexCache write-back	FSx untuk volume ONTAP sekarang mendukung mode FlexCache tulis kembali. Untuk informasi selengkapnya, lihat Mereplikasi data Anda dengan FlexCache .	28 Mei 2025
Wilayah AWS Dukungan tambahan ditambahkan	FSx untuk sistem file ONTAP sekarang tersedia di Asia Pasifik (Thailand) dan Meksiko (Tengah). Untuk informasi selengkapnya, lihat Ketersediaan oleh Wilayah AWS .	8 Mei 2025

[Autonomous Ransomware Protection \(ARP\) sekarang didukung](#)

ARP, fitur NetApp berbasis AI yang memantau dan melindungi terhadap serangan ransomware dan malware, sekarang didukung oleh untuk ONTAP. FSx Untuk informasi selengkapnya, lihat [Melindungi data Anda dengan Autonomous Ransomware Protection](#)

April 7, 2025

[Topik baru di Panduan Pengguna FSx untuk ONTAP menjelaskan cara menyiapkan server SMB di grup kerja](#)

[Menyiapkan server SMB di workgroup](#) menjelaskan cara mengatur server SMB di workgroup pada SVM sebagai alternatif untuk bergabung dengan SVM ke Microsoft Active Directory.

Maret 4, 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

[HarvestDasbor tambahan sekarang didukung](#)

HarvestDasbor tambahan sekarang didukung oleh FSx untuk ONTAP, termasuk dasbor yang tidak diaktifkan secara default. Daftar dasbor yang FSx tidak didukung ONTAP juga telah ditambahkan. Untuk informasi selengkapnya, lihat [FSx Memantau sistem file ONTAP menggunakan Harvest dan Grafana](#).

Februari 18, 2025

[Baru FSx untuk ONTAP Penagihan dan topik pelaporan penggunaan ditambahkan ke Panduan Pengguna FSx ONTAP](#)

[Pelaporan AWS penagihan dan penggunaan FSx untuk topik ONTAP](#) menjelaskan cara mengakses penagihan laporan penggunaan FSx untuk sistem file ONTAP di konsol. AWS Manajemen Penagihan dan Biaya Ini juga menyediakan semua jenis penggunaan di kedua laporan yang khusus FSx untuk ONTAP.

Februari 13, 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 ONTAP 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

[Topik baru diterbitkan, Mereplikasi data dengan FlexCache](#)

Menerbitkan topik baru yang menjelaskan cara mereplikasi data dalam sistem file ONTAP lokal ke sistem file ONTAP FSx untuk menggunakan sistem file ONTAP telah diterbitkan. FlexCache Untuk informasi selengkapnya, lihat [Mereplikasi data dengan FlexCache](#).

Desember 19, 2024

[Support ditambahkan untuk sistem file generasi kedua](#)

Anda sekarang dapat membuat sistem file Single-AZ dan Multi-AZ generasi kedua. Satu pasangan ketersediaan tinggi (HA) sekarang memberikan hingga 6 GBps kapasitas throughput dan 200.000 IOPS SSD. Untuk informasi lebih lanjut, lihat [Pasangan ketersediaan tinggi \(HA\)](#).

9 Juli 2024

[Support ditambahkan untuk membaca data dari volume saat sedang dipulihkan dari cadangan](#)

Anda sekarang dapat mem-mount volume dengan akses read-only ke data file saat sedang dipulihkan dari cadangan pada sistem file generasi kedua. Untuk informasi selengkapnya, lihat [Memulihkan cadangan ke volume baru](#).

9 Juli 2024

[Support ditambahkan untuk menyesuaikan kapasitas throughput pada sistem file generasi kedua](#)

Anda sekarang dapat menyesuaikan kapasitas throughput sistem file generasi kedua Anda setelah pembuatan. Untuk informasi selengkapnya, lihat [Mengelola kapasitas throughput](#).

9 Juli 2024

[Support ditambahkan untuk menambahkan pasangan HA ke sistem file single-AZ generasi kedua](#)

Anda sekarang dapat menambahkan pasangan HA ke sistem file single-AZ generasi kedua setelah pembuatan. Anda dapat memiliki total 12 pasangan HA pada sistem file Single-AZ generasi kedua. Untuk informasi selengkapnya, lihat [Menambahkan pasangan ketersediaan tinggi \(HA\)](#).

9 Juli 2024

[Support ditambahkan untuk protokol Non-Volatile Memory Express melalui TCP \(/TCP\) NVMe](#)

Anda sekarang dapat menggunakan NVMe/TCP protokol untuk transportasi data di Amazon FSx untuk sistem file NetApp ONTAP. Untuk informasi selengkapnya, lihat [Menggunakan protokol penyimpanan blok](#)

9 Juli 2024

[Support ditambahkan untuk fsxadmin-readonly peran bagi pengguna administrasi sistem file](#)

fsxadmin-readonly Peran ini sekarang tersedia untuk pengguna administrasi sistem ONTAP file, dan dapat digunakan untuk aplikasi pemantauan sistem file seperti NetApp Harvest. Untuk informasi selengkapnya, lihat [Peran dan pengguna administrator sistem berkas](#).

April 30, 2024

[Support ditambahkan untuk otentikasi kunci publik SSH untuk pengguna administratif domain Windows](#)

Anda sekarang dapat menggunakan otentikasi kunci publik SSH dengan sistem file domain Active Directory dan pengguna SVM. Untuk informasi selengkapnya, lihat [Mengonfigurasi autentikasi Direktori Aktif untuk ONTAP pengguna.](#)

April 30, 2024

[Support ditambahkan untuk 12 pasangan HA dalam sistem file scale-out](#)

Amazon FSx untuk NetApp ONTAP menambahkan dukungan untuk 12 pasangan HA dalam sistem file scale-out. Sistem file dengan 12 pasang HA dapat menghasilkan hingga 72 GBps kapasitas throughput dan 2.400.000 IOPS SSD di 12 pasangan ketersediaan tinggi (HA). Untuk informasi selengkapnya, lihat [Pasangan ketersediaan tinggi \(HA\)](#) dan [Amazon FSx untuk performa NetApp ONTAP.](#)

Maret 4, 2024

[Support ditambahkan untuk mode tulis cloud](#)

Amazon FSx untuk NetApp ONTAP menambahkan dukungan untuk mode tulis cloud untuk volume. Untuk informasi selengkapnya, lihat [Mengaktifkan mode tulis cloud pada volume.](#)

Februari 6, 2024

[Support ditambahkan untuk membuat cadangan FlexGroup volume dengan AWS Backup](#)

Anda sekarang dapat menggunakan AWS Backup untuk mencadangkan dan memulihkan FlexGroup volume pada sistem file ONTAP Anda FSx . Untuk informasi selengkapnya, lihat [Menggunakan AWS Backup dengan Amazon FSx](#).

Januari 11, 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

[Support ditambahkan untuk metrik scale-out](#)

FSx untuk ONTAP sekarang menyediakan CloudWatch metrik Amazon untuk sistem file dengan beberapa pasangan HA. Untuk informasi selengkapnya, lihat [Metrik sistem file Scale-out](#).

26 November 2023

[Support ditambahkan untuk sistem file scale-out](#)

Amazon FSx untuk NetApp ONTAP menambahkan dukungan untuk sistem file scale-out yang dapat memberikan hingga 36 GBps kapasitas throughput dan 1.200.000 IOPS SSD di enam pasangan ketersediaan tinggi (HA). Untuk informasi selengkapnya, lihat [Pasangan ketersediaan tinggi \(HA\)](#) dan [Amazon FSx untuk performa NetApp ONTAP](#).

26 November 2023

[Support ditambahkan untuk FlexGroup volume](#)

Amazon FSx untuk NetApp ONTAP menambahkan dukungan untuk FlexGroup volume. Untuk informasi selengkapnya, lihat [Gaya volume](#).

26 November 2023

[Dukungan VPC bersama
ditambahkan untuk sistem file
Multi-AZ](#)

Akun peserta sekarang dapat membuat sistem file multi-AZ dalam VPC yang telah dibagikan dengan mereka. Akun pemilik dapat mengelola fitur ini di FSx konsol Amazon, CLI, dan API. Untuk informasi selengkapnya, lihat [Membuat FSx untuk sistem file ONTAP di subnet bersama](#)

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: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 membuat peran dan pengguna ONTAP tambahan](#)

Amazon FSx untuk NetApp ONTAP sekarang mendukung pembuatan peran ONTAP tambahan dan pengguna untuk menentukan kemampuan dan hak istimewa pengguna saat menggunakan ONTAP CLI dan REST API. Untuk informasi selengkapnya, lihat [Peran dan pengguna di Amazon FSx untuk NetApp ONTAP](#).

September 6, 2023

[Support ditambahkan untuk CloudWatch metrik tambahan dan dasbor pemantauan yang disempurnakan](#)

FSx untuk ONTAP sekarang menyediakan metrik kinerja tambahan dan dasbor pemantauan yang disempurnakan untuk meningkatkan visibilitas ke dalam aktivitas sistem file. Untuk informasi selengkapnya, lihat [Memantau dengan CloudWatch](#).

17 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 memperbarui kebijakan AWS terkelola](#).

Juli 24, 2023

[Support ditambahkan untuk menggunakan NetApp System Manager secara langsung](#)

Anda dapat mengelola sistem file ONTAP Anda FSx menggunakan System Manager langsung dari NetApp BlueXP. Untuk informasi selengkapnya, lihat [Menggunakan Manajer NetApp Sistem dengan BlueXP](#).

13 Juli 2023

[Support ditambahkan untuk memantau acara EMS](#)

Anda dapat memantau FSx peristiwa sistem file ONTAP menggunakan asli NetApp ONTAP. Events Management System (EMS) Anda dapat melihat acara EMS menggunakan CLI NetApp ONTAP. Untuk informasi selengkapnya, lihat [FSx Memantau peristiwa ONTAP EMS](#).

13 Juli 2023

Support ditambahkan untuk SnapLock

FSx untuk ONTAP sekarang mendukung SnapLock volume. SnapLock memungkinkan Anda untuk melindungi file Anda dengan mentransi sisinya ke status tulis sekali, baca banyak (WORM), yang mencegah modifikasi atau penghapusan untuk periode retensi tertentu. FSx untuk ONTAP mendukung mode Kepatuhan dan retensi Perusahaan dengan SnapLock. Untuk informasi selengkapnya, lihat [Bekerja dengan SnapLock](#).

13 Juli 2023

Support ditambahkan untuk IPsec enkripsi data dalam perjalanan

FSx untuk ONTAP sekarang mendukung penggunaan IPsec enkripsi untuk mengenkripsi data dalam perjalanan antara sistem file dan klien yang terhubung. Untuk informasi selengkapnya, lihat [Mengkonfigurasi IPsec menggunakan otentikasi PSK dan Mengkonfigurasi IPsec menggunakan otentikasi sertifikat](#).

13 Juli 2023

Ukuran volume maksimum telah meningkat

FSx untuk ONTAP memperbarui ukuran maksimum volume dari 100 TB menjadi 300 TB. Untuk informasi selengkapnya, lihat [Mengaktifkan autosizing volume](#).

13 Juli 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 menggabungkan mesin virtual penyimpanan yang ada ke Active Directory](#)

Anda dapat menggabungkan mesin virtual penyimpanan yang ada ke Active Directory menggunakan Konsol Manajemen AWS, AWS CLI dan API. Untuk informasi selengkapnya, lihat [Menggabungkan SVM ke Direktori Aktif](#).

13 Juni 2023

[Support untuk cache NVMe
baca ditambahkan untuk
sistem file Single-AZ](#)

NVMe cache baca sekarang didukung untuk sistem file AZ tunggal yang dibuat setelah 28 November 2022 dengan setidaknya 2 GBps kapasitas throughput di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia). Untuk informasi selengkapnya, lihat [Dampak jenis penerapan pada performa](#).

28 November 2022

[Support ditambahkan untuk
menggunakan rentang alamat
IP in-vPC untuk membuat
sistem file multi-AZ](#)

Anda sekarang dapat membuat Multi-AZ FSx untuk sistem file ONTAP dengan menentukan titik akhir yang berada dalam rentang alamat IP VPC Anda. Untuk informasi selengkapnya, lihat [Membuat FSx untuk sistem file ONTAP](#).

28 November 2022

[Support ditambahkan untuk
memperbarui tabel rute VPC
pada sistem file Multi-AZ](#)

Anda sekarang dapat mengaitkan (menambahkan) tabel rute VPC baru ke sistem file Multi-AZ FSx untuk ONTAP yang ada atau memisahkan (menghapus) tabel rute VPC yang ada dari sistem file Multi-AZ untuk ONTAP yang ada. FSx Untuk informasi selengkapnya, lihat [Memperbarui sistem file](#).

28 November 2022

[Support ditambahkan untuk enkripsi data dalam perjalanan dengan AWS Nitro System](#)

Data dalam perjalanan dienkripsi secara otomatis ketika diakses dari EC2 instans Amazon yang didukung di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia). Untuk informasi selengkapnya, lihat [Mengenkripsi data dalam perjalanan dengan Sistem AWS Nitro](#).

28 November 2022

[Support ditambahkan untuk membuat volume DP](#)

Anda sekarang dapat membuat volume DP (perlindungan data) dengan menggunakan FSx konsol Amazon,, AWS CLI atau Amazon API. FSx Anda dapat menggunakan volume DP sebagai tujuan SnapVault hubungan NetApp SnapMirror atau, saat Anda ingin memigrasi atau melindungi data satu volume. Untuk informasi selengkapnya, lihat [Jenis volume](#).

28 November 2022

[Support ditambahkan untuk menyalin tag volume ke backup](#)

Anda sekarang dapat mengaktifkan CopyTagsToBackups di AWS CLI atau Amazon FSx API untuk secara otomatis menyalin tag dari volume Anda ke cadangan. Untuk informasi selengkapnya, lihat [Menyalin tag ke cadangan](#).

28 November 2022

[Support ditambahkan untuk memilih kebijakan snapshot](#)

Sekarang Anda dapat memilih dari tiga kebijakan snapshot bawaan saat membuat atau memperbarui volume menggunakan FSx konsol Amazon, AWS CLI, atau Amazon FSx API. Anda juga dapat memilih kebijakan snapshot khusus yang dibuat di ONTAP CLI atau REST API. Untuk informasi selengkapnya, lihat [Kebijakan snapshot](#).

28 November 2022

[Support ditambahkan untuk opsi kapasitas throughput sistem file tambahan](#)

FSx untuk ONTAP sekarang mendukung 4.096 MBps kapasitas throughput untuk sistem file yang dibuat setelah 28 November 2022 di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia). Untuk informasi selengkapnya, lihat [Dampak kapasitas throughput terhadap kinerja](#).

28 November 2022

[Support ditambahkan untuk IOPS SSD tambahan](#)

FSx untuk ONTAP sekarang mendukung 160.000 IOPS SSD untuk sistem file yang dibuat setelah 28 November 2022 di Wilayah AS Timur (Ohio), Wilayah AS Timur (Virginia N.), Wilayah AS Barat (Oregon), dan Eropa (Irlandia). Untuk informasi selengkapnya, lihat [Dampak kapasitas throughput terhadap kinerja](#).

28 November 2022

[Support ditambahkan FSx untuk menggunakan ONTAP sebagai datastore eksternal untuk Cloud on VMware AWS](#)

Anda dapat menggunakan FSx ONTAP sebagai datastore eksternal untuk VMware Cloud pada Pusat Data yang Ditetapkan AWS Perangkat Lunak (). SDDCs Dukungan tambahan ini memberikan fleksibilitas untuk meningkatkan atau menurunkan penyimpanan secara independen dari sumber daya komputasi untuk VMware Cloud pada beban AWS kerja. Untuk informasi selengkapnya, lihat [Menggunakan VMware Cloud with FSx for ONTAP](#).

30 Agustus 2022

[Secara otomatis meningkatkan kapasitas penyimpanan sistem file](#)

Gunakan CloudFormation template AWS yang dapat disesuaikan yang dikembangkan untuk secara otomatis meningkatkan kapasitas penyimpanan sistem file Anda ketika jumlah kapasitas penyimpanan SSD yang digunakan melebihi ambang batas yang Anda tentukan. Untuk informasi selengkapnya, lihat [Meningkatkan kapasitas penyimpanan SSD secara dinamis](#).

Juni 3, 2022

[Amazon FSx kini terintegrasi dengan AWS Backup](#)

Anda sekarang dapat menggunakan AWS Backup untuk mencadangkan dan memulihkan sistem FSx file Anda selain menggunakan FSx cadangan Amazon asli. Untuk informasi selengkapnya, lihat [Menggunakan AWS Backup dengan Amazon FSx](#).

Mei 18, 2022

[Support ditambahkan untuk penyebaran sistem file ONTAP Zona Ketersediaan tunggal](#)

Anda dapat membuat Single-AZ FSx untuk sistem file ONTAP, yang dirancang untuk memberikan ketersediaan dan daya tahan tinggi dalam satu Availability Zone (AZ). Untuk informasi selengkapnya, lihat [Memilih penerapan sistem file](#).

13 April 2022

[Support ditambahkan untuk titik AWS PrivateLink 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 memodifikasi kapasitas throughput untuk sistem file ONTAP yang ada](#)

Anda sekarang dapat memodifikasi kapasitas throughput yang tersedia untuk sistem file ONTAP yang ada. Untuk informasi selengkapnya, lihat [Mengelola kapasitas throughput](#).

Maret 30, 2022

[Support ditambahkan untuk kapasitas penyimpanan SSD dan penskalaan IOPS yang disediakan](#)

Anda sekarang dapat meningkatkan kapasitas penyimpanan SSD dan IOPS yang disediakan untuk sistem file ONTAP yang ada FSx saat penyimpanan dan persyaratan IOPS Anda berkembang. Untuk informasi selengkapnya, lihat [Mengelola kapasitas penyimpanan dan IOPS yang disediakan](#).

Januari 25, 2022

[Support ditambahkan untuk CloudWatch metrik Amazon](#)

Anda dapat memantau sistem file Anda menggunakan Amazon CloudWatch, yang mengumpulkan dan memproses data mentah dari FSx ONTAP menjadi metrik hampir real-time yang dapat dibaca. Untuk informasi selengkapnya, lihat [Memantau dengan Amazon CloudWatch](#).

Januari 19, 2022

[Support ditambahkan untuk opsi throughput sistem file tambahan](#)

FSx untuk ONTAP sekarang mendukung 128 MBps dan 256 MBps opsi untuk throughput sistem file. Untuk informasi selengkapnya, lihat [Dampak kapasitas throughput terhadap kinerja](#).

30 November 2021

[Amazon FSx untuk NetApp ONTAP sekarang tersedia secara umum](#)

FSx untuk ONTAP adalah layanan yang dikelola sepenuhnya yang menyediakan penyimpanan file yang sangat andal, terukur, berkinerja, dan kaya fitur yang dibangun di atas NetApp sistem file ONTAP. Ini menyediakan fitur, kinerja, kemampuan, dan sistem NetApp file APIs yang sudah dikenal dengan kelincahan, skalabilitas, dan kesederhanaan layanan yang dikelola AWS sepenuhnya.

2 September 2021

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