



Panduan Pengguna Lustre

FSx for Lustre



FSx for Lustre: Panduan Pengguna Lustre

Copyright © 2024 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 menghina atau mendiskreditkan Amazon. Semua merek dagang lain yang tidak dimiliki oleh Amazon merupakan kekayaan masing-masing pemiliknya, yang mungkin atau mungkin tidak berafiliasi, terkait dengan, atau disponsori oleh Amazon.

Table of Contents

Apakah Amazon FSx for Lustre itu?	1
Beberapa opsi deployment	2
Beberapa opsi penyimpanan	2
FSx for Lustre dan repositori data	2
FSx for Lustre S3 integrasi repositori data	3
FSx for Lustre dan repositori data lokal	3
Mengakses sistem file	3
Integrasi dengan layanan AWS	4
Keamanan dan kepatuhan	5
Asumsi	5
Harga untuk Amazon FSx for Lustre	5
Forum Amazon FSx for Lustre	6
Apakah Anda baru pertama kali menggunakan Amazon FSx for Lustre?	6
Pengaturan	7
Mendaftar Amazon Web Services	7
Mendaftar untuk Akun AWS	7
Buat pengguna dengan akses administratif	8
Menambahkan izin untuk menggunakan repositori data di Amazon S3	9
Bagaimana FSx for Lustre memeriksa akses ke bucket S3	10
Langkah selanjutnya	12
Memulai	13
Prasyarat	13
Buat sistem file FSx for Lustre Anda	14
Instal klien Lustre	19
Pasang sistem berkas	20
Jalankan alur kerja Anda	22
Pembersihan sumber daya	22
Opsi deployment sistem file	24
Opsi deployment	24
Sistem file Scratch	25
Sistem file persisten	26
Jenis penerapan persistent_2	26
Jenis penerapan persistent_1	27
Wilayah yang tersedia	27

Menggunakan repositori data	30
Gambaran umum tentang repositori data	31
Dukungan metadata POSIX	32
Tautan keras dan mengekspor ke S3	34
Melampirkan izin POSIX ke bucket S3	35
Menautkan sistem file Anda ke bucket S3	38
Dukungan wilayah dan akun untuk bucket S3 yang ditautkan	40
Membuat tautan ke bucket S3	40
Bekerja dengan bucket Amazon S3 yang dienkripsi sisi server	50
Mengimpor perubahan dari repositori data	53
Secara otomatis mengimpor pembaruan dari bucket S3	54
Menggunakan tugas repositori data untuk mengimpor perubahan	59
Terlebih dulu memuat file ke dalam sistem file Anda	61
Mengekspor perubahan ke repositori data	62
Ekspor pembaruan ke bucket S3 Anda secara otomatis	64
Menggunakan tugas repositori data untuk mengekspor perubahan	66
Mengekspor file menggunakan perintah HSM	70
Tugas repositori data	71
Jenis-jenis tugas repositori data	71
Status dan detail tugas	72
Menggunakan tugas repositori data	73
Bekerja dengan laporan penyelesaian tugas	80
Memecahkan masalah kegagalan tugas	82
Melepaskan file	87
Menggunakan tugas repositori data untuk merilis file	88
Menggunakan Amazon FSx dengan data lokal	92
Log peristiwa repositori data	92
Bekerja dengan jenis penyebaran yang lebih lama	109
Tautkan sistem file Anda ke bucket Amazon S3	109
Secara otomatis mengimpor pembaruan dari bucket S3	117
Performa	122
Cara kerja sistem file FSx for Lustre	122
Performa kumpulan sistem file	123
Contoh: Agregat baseline dan burst throughput	128
Kinerja metadata sistem file	128
Layout penyimpanan sistem file	129

Sedang melakukan stripe data di sistem file Anda	130
Memodifikasi konfigurasi striping Anda	131
Layout file progresif	133
Memantau performa dan penggunaan	134
Tips performa	135
Mengakses sistem file	138
Sistem file Lustre dan kompatibilitas kernel klien	138
Menginstal klien Lustre	142
Amazon Linux	142
CentOS, Rocky Linux, dan Red Hat	144
Ubuntu	155
SUSE Linux	161
Pasang dari Amazon EC2	163
Memasang dari Amazon ECS	165
Pemasangan dari instans Amazon EC2 yang menghosting tugas Amazon ECS	166
Pemasangan dari wadah Docker	167
Memasang dari on-premise atau VPC lain	168
Memasang Amazon FSx secara otomatis	170
Pemasangan otomatis menggunakan /etc/fstab	170
Memasang fileset spesifik	173
Melepaskan sistem file	174
Menggunakan Instans Spot EC2	175
Menangani Interupsi Instans Spot Amazon EC2	176
Mengelola sistem file	179
Backup	179
Dukungan Backup di FSx for Lustre	181
Bekerja dengan backup harian otomatis	181
Bekerja dengan backup yang diinisiasi pengguna	182
Menggunakan AWS Backup dengan Amazon FSx	183
Menyalin cadangan	184
Menyalin cadangan dalam hal yang sama Akun AWS	186
Memulihkan cadangan	187
Menghapus cadangan	188
Kuota penyimpanan	189
Pemberlakuan kuota	189
Jenis kuota	190

Batas kuota dan masa tenggang	191
Mengatur dan melihat kuota	191
Kuota dan bucket terkait Amazon S3	195
Kuota dan memulihkan backup	196
Kapasitas penyimpanan	196
Pertimbangan saat meningkatkan kapasitas penyimpanan	197
Kapan harus meningkatkan kapasitas penyimpanan	198
Bagaimana penyekalaan penyimpanan dan permintaan backup secara bersamaan ditangani	198
Bagaimana meningkatkan kapasitas penyimpanan	199
Memantau peningkatan kapasitas penyimpanan	201
Kelola kinerja metadata	205
Konfigurasi kinerja metadata kilau	206
Pertimbangan saat meningkatkan kinerja metadata	207
Kapan harus meningkatkan kinerja metadata	207
Cara meningkatkan kinerja metadata	207
Mengubah mode konfigurasi metadata	209
Memantau pembaruan konfigurasi metadata	210
Kapasitas throughput	212
Pertimbangan saat memperbarui kapasitas throughput	213
Kapan harus mengubah kapasitas throughput	214
Bagaimana cara mengubah kapasitas throughput	214
Memantau perubahan kapasitas throughput pada konsol	216
Kompresi data	218
Mengelola kompresi data	219
Mengompresi file yang sebelumnya ditulis	222
Melihat ukuran file	222
Menggunakan CloudWatch metrik	223
Labu akar	223
Cara kerja root squash	224
Mengelola root squash	225
Status sistem file	230
Tandai sumber daya Anda	231
Dasar-dasar tag	231
Menandai Sumber Daya Anda	232
Pembatasan tanda	233

Izin dan tag	233
Maintenance	234
Menghapus sistem file	235
Bermigrasi ke FSx for Lustre dengan DataSync	236
Migrasi file dengan AWS DataSync	236
Prasyarat	236
DataSync langkah dasar migrasi	237
Memantau sistem file	238
Pemantauan CloudWatch dengan	238
Metrik sistem file	239
Metrik metadata sistem file	244
AutoImport dan AutoExport metrik	247
Dimensi Amazon FSx for Lustre	249
Cara menggunakan Amazon FSx for Lustre	249
Mengakses metrik CloudWatch	251
Membuat alarm	252
Logging dengan CloudWatch Log	253
Ikhtisar pencatatan	254
Log tujuan	255
Mengelola logging	255
Melihat log	257
Logging dengan AWS CloudTrail	258
Informasi Amazon FSx for Lustre di CloudTrail	258
Memahami entri file berkas log Amazon FSx for Lustre	259
Keamanan	262
Perlindungan data	263
Enkripsi data	264
Privasi lalu lintas antar jaringan	269
Pengelolaan identitas dan akses	269
Audiens	270
Mengautentikasi dengan identitas	271
Mengelola akses menggunakan kebijakan	274
FSx for Lustre dan IAM	277
Contoh kebijakan berbasis identitas	284
AWS kebijakan terkelola	287
Pemecahan Masalah	300

Menggunakan tanda dengan Amazon FSx	303
Menggunakan peran terkait layanan	309
Kontrol akses sistem file dengan Amazon VPC	316
Grup keamanan Amazon VPC	316
Lustre klien aturan grup keamanan VPC	320
ACL jaringan VPC Amazon	323
Validasi Kepatuhan	323
Titik akhir VPC antarmuka	324
Pertimbangan untuk titik akhir VPC antarmuka Amazon FSx	325
Membuat titik akhir VPC antarmuka untuk Amazon FSx API	325
Membuat kebijakan titik akhir VPC untuk Amazon FSx	326
Kuota	327
Kuota yang dapat Anda tingkatkan	327
Sumber daya kuota untuk setiap sistem file	329
Pertimbangan tambahan	329
Pemecahan Masalah	331
Membuat sistem file gagal	331
Tidak dapat membuat sistem file karena grup keamanan yang salah dikonfigurasi	331
Tidak dapat membuat sistem file yang tertaut ke bucket S3	332
Pemasangan sistem file gagal	332
Pemasangan sistem file gagal segera	332
Pemasangan sistem file hang dan kemudian gagal dengan kesalahan timeout	333
Pemasangan otomatis gagal dan instans tidak responsif	333
Pemasangan sistem file gagal selama boot sistem	334
Pemasangan sistem file menggunakan nama DNS gagal	334
Anda tidak dapat mengakses sistem file Anda	335
Alamat IP Elastis yang dilekatkan pada antarmuka jaringan elastis sistem file telah dihapus	335
Antarmuka jaringan elastis sistem file telah dimodifikasi atau dihapus	335
Membuat DRA gagal	336
Mengganti nama direktori membutuhkan waktu lama	337
Bucket S3 tertaut yang salah dikonfigurasi	338
Masalah penyimpanan	339
Kesalahan tulis karena tidak ada ruang pada target penyimpanan	339
Penyimpanan tidak seimbang pada OST	340
Masalah driver CSI	343

Informasi tambahan	344
Mengatur jadwal backup khusus	344
Gambaran umum arsitektur	345
AWS CloudFormation Templat	345
Otomatisasi deployment	346
Opsi tambahan	348
Riwayat dokumen	349
.....	ccclxviii

Apakah Amazon FSx for Lustre itu?

FSx for Lustre memudahkan dan hemat biaya untuk meluncurkan dan menjalankan sistem file Lustre yang populer dan berkinerja tinggi. Gunakan Lustre untuk beban kerja di mana kecepatan penting, seperti machine learning, komputasi performa tinggi (HPC), pemrosesan video, dan pemodelan keuangan.

Sistem file Lustre sumber terbuka dirancang untuk aplikasi yang memerlukan penyimpanan cepat —di mana Anda ingin penyimpanan Anda terus mengikuti komputasi Anda. Lustre dibangun untuk memecahkan masalah dengan cepat dan murah dengan memproses dataset dunia yang terus berkembang. Ini adalah sistem file yang banyak digunakan yang dirancang untuk komputer tercepat di dunia. Ini menyediakan latensi sub-milidetik, hingga ratusan GBps throughput, dan hingga jutaan IOPS. Untuk informasi lebih lanjut di Lustre, lihat [Situs web Lustre](#).

Sebagai layanan terkelola sepenuhnya, Amazon FSx memudahkan Anda untuk menggunakan Lustre untuk beban kerja di mana kecepatan penyimpanan penting. FSx for Lustre menghilangkan kompleksitas tradisional dalam menyiapkan dan mengelola sistem file Lustre, memungkinkan Anda untuk memutar dan menjalankan sistem file berkinerja tinggi yang telah teruji pertempuran dalam hitungan menit. Ini juga menyediakan beberapa opsi deployment sehingga Anda dapat mengoptimalkan biaya untuk kebutuhan Anda.

FSx for Lustre sesuai dengan POSIX, sehingga Anda dapat menggunakan aplikasi berbasis Linux Anda saat ini tanpa harus membuat perubahan apa pun. FSx for Lustre menyediakan antarmuka sistem file asli dan berfungsi seperti sistem file apa pun dengan sistem operasi Linux Anda. Ini juga memberikan read-after-write konsistensi dan mendukung penguncian file.

Topik

- [Beberapa opsi deployment](#)
- [Beberapa opsi penyimpanan](#)
- [FSx for Lustre dan repositori data](#)
- [Mengakses sistem file FSx for Lustre](#)
- [Integrasi dengan layanan AWS](#)
- [Keamanan dan kepatuhan](#)
- [Asumsi](#)
- [Harga untuk Amazon FSx for Lustre](#)
- [Forum Amazon FSx for Lustre](#)

- [Apakah Anda baru pertama kali menggunakan Amazon FSx for Lustre?](#)

Beberapa opsi deployment

Amazon FSx for Lustre menawarkan pilihan sistem file scratch dan persisten untuk mengakomodasi perlunya pengolahan data yang berbeda. Sistem file scratch yang ideal untuk penyimpanan sementara dan pengolahan jangka pendek data. Data tidak direplikasi dan tidak bertahan jika file server gagal. Sistem file persisten sangat ideal untuk penyimpanan jangka panjang dan beban kerja yang berfokus pada throughput. Dalam sistem file persisten, data direplikasi, dan server file diganti jika mereka gagal. Untuk informasi selengkapnya, lihat [Opsi penyebaran untuk sistem file FSx for Lustre](#).

Beberapa opsi penyimpanan

Amazon FSx for Lustre menawarkan pilihan jenis penyimpanan solid state drive (SSD) dan hard disk drive (HDD) yang dioptimalkan untuk berbagai persyaratan pemrosesan data:

- Opsi penyimpanan SSD - Untuk latensi rendah, beban kerja intensif IOPS yang biasanya memiliki operasi file acak yang kecil, pilih salah satu opsi penyimpanan SSD.
- Opsi penyimpanan HDD — Untuk beban kerja intensif throughput yang biasanya memiliki operasi file besar dan berurutan, pilih salah satu opsi penyimpanan HDD.

Jika Anda menyediakan sistem file dengan opsi penyimpanan HDD, Anda dapat secara opsional menyediakan cache SSD read-only yang berukuran hingga 20 persen dari kapasitas penyimpanan HDD Anda. Ini menyediakan latensi submilidetik dan IOPS yang lebih tinggi untuk file yang sering diakses. Baik sistem file berbasis SSD dan HDD disediakan dengan server metadata berbasis SSD. Akibatnya, semua operasi metadata, yang mewakili sebagian besar operasi sistem file, dikirimkan dengan latensi sub-milidetik.

Untuk informasi lebih lanjut tentang performa opsi penyimpanan ini, lihat [Performa Amazon FSx for Lustre](#).

FSx for Lustre dan repositori data

Anda dapat menautkan sistem file FSx for Lustre ke repositori data di Amazon S3 atau ke penyimpanan data lokal.

FSx for Lustre S3 integrasi repositori data

FSx for Lustre terintegrasi dengan Amazon S3, sehingga memudahkan Anda memproses kumpulan data cloud menggunakan sistem file kinerja tinggi Lustre. Saat ditautkan ke bucket Amazon S3, sistem file FSx for Lustre secara transparan menampilkan objek S3 sebagai file. Amazon FSx mengimpor daftar semua file yang ada di bucket S3 Anda pada pembuatan sistem file. Amazon FSx juga dapat mengimpor daftar file yang ditambahkan ke repositori data setelah sistem file dibuat. Anda dapat mengatur preferensi impor agar sesuai dengan kebutuhan alur kerja Anda. Sistem file juga memungkinkan Anda untuk menulis data sistem file kembali ke S3. Tugas repositori data menyederhanakan transfer data dan metadata antara sistem file FSx for Lustre Anda dan repositori data yang tahan lama di Amazon S3. Untuk informasi selengkapnya, lihat [Menggunakan repositori data dengan Amazon FSx for Lustre](#) dan [Tugas repositori data](#).

FSx for Lustre dan repositori data lokal

Dengan Amazon FSx for Lustre, Anda dapat mem-burst beban kerja pemrosesan data dari lokal ke lokasi AWS Cloud dengan mengimpor data menggunakan atau AWS Direct Connect atau AWS VPN. Untuk informasi selengkapnya, lihat [Menggunakan Amazon FSx dengan data lokal](#).

Mengakses sistem file FSx for Lustre

Anda dapat mencampur dan mencocokkan jenis instans komputasi dan Linux Amazon Machine Images (AMI) yang terhubung ke satu sistem file FSx for Lustre.

Sistem file Amazon FSx for Lustre dapat diakses dari beban kerja komputasi yang berjalan di instans Amazon Elastic Compute Cloud (Amazon EC2), di Amazon Elastic Container Service (Amazon ECS) container Docker, dan container yang berjalan di Amazon Elastic Kubernetes Service (Amazon EKS).

- Amazon EC2 — Anda mengakses sistem file dari instans komputasi Amazon EC2 menggunakan klien Lustre sumber terbuka. Instans Amazon EC2 dapat mengakses sistem file Anda dari Availability Zone di Amazon Virtual Private Cloud (Amazon VPC) yang sama, asalkan konfigurasi jaringan Anda menyediakan akses di seluruh subnet dalam VPC. Setelah sistem file Amazon FSx for Lustre terpasang, Anda dapat bekerja dengan file dan direktorinya seperti yang Anda lakukan menggunakan sistem file lokal.
- Amazon EKS — Anda mengakses Amazon FSx for Lustre dari kontainer yang berjalan di Amazon EKS menggunakan driver open-source [FSx for Lustre CSI, seperti yang dijelaskan dalam Panduan Pengguna Amazon EKS](#). kontainer Anda yang berjalan di Amazon EKS dapat menggunakan volume persisten performa tinggi (PVs) yang didukung oleh Amazon FSx for Lustre.

- Amazon ECS - Anda mengakses Amazon FSx for Lustre dari wadah Amazon ECS Docker di instans Amazon EC2. Untuk informasi selengkapnya, lihat [Pemasangan dari Amazon Elastic Container Service](#).

Amazon FSx for Lustre kompatibel dengan AMI berbasis Linux paling populer, termasuk Amazon Linux 2 dan Amazon Linux, Red Hat Enterprise Linux (RHEL), CentOS, Ubuntu, dan SUSE Linux. Klien Lustre disertakan dengan Amazon Linux 2 dan Amazon Linux. Untuk RHEL, CentOS, dan Ubuntu, AWS repositori klien Lustre menyediakan klien yang kompatibel dengan sistem operasi ini.

Menggunakan FSx for Lustre, Anda dapat membobol beban kerja intensif komputasi Anda dari lokal ke lokasi dengan mengimpor data melalui atau. AWS Cloud AWS Direct Connect AWS Virtual Private Network Anda dapat mengakses sistem file Amazon FSx dari on-premise, menyalin data ke sistem file sesuai kebutuhan, dan menjalankan beban kerja komputasi intensif pada instans di cloud.

Untuk informasi selengkapnya tentang klien, instance komputasi, dan lingkungan tempat Anda dapat mengakses sistem file FSx for Lustre, lihat. [Mengakses sistem file](#)

Integrasi dengan layanan AWS

Amazon FSx for Lustre terintegrasi SageMaker dengan Amazon sebagai sumber data input. Saat menggunakan SageMaker dengan FSx for Lustre, pekerjaan pelatihan pembelajaran mesin Anda dipercepat dengan menghilangkan langkah pengunduhan awal dari Amazon S3. Selain itu, total biaya kepemilikan (TCO) dikurangi dengan menghindari mengunduh berulang objek umum untuk tugas berulang pada dataset yang sama seperti yang Anda hemat dengan biaya permintaan S3. Untuk informasi lebih lanjut, lihat [Apa itu SageMaker?](#) di Panduan SageMaker Pengembang Amazon. Untuk panduan tentang cara menggunakan Amazon FSx for Lustre sebagai SageMaker sumber data, [lihat Mempercepat pelatihan di Amazon menggunakan sistem file Amazon SageMaker FSx for Lustre dan Amazon EFS](#) di Blog Machine Learning.AWS

FSx for Lustre AWS Batch terintegrasi dengan menggunakan EC2 Launch Templates. AWS Batch memungkinkan Anda menjalankan beban kerja komputasi batch pada AWS Cloud, termasuk komputasi kinerja tinggi (HPC), pembelajaran mesin (ML), dan beban kerja asinkron lainnya. AWS Batch secara otomatis dan dinamis mengukur instance berdasarkan persyaratan sumber daya pekerjaan. Untuk informasi lebih lanjut, lihat [Apa itu AWS Batch?](#) dalam AWS Batch User Guide.

FSx for Lustre terintegrasi dengan. AWS ParallelCluster AWS ParallelCluster adalah alat manajemen cluster sumber terbuka yang AWS didukung yang digunakan untuk menyebarkan dan mengelola

cluster HPC. Secara otomatis dapat membuat FSx for Lustre sistem file atau menggunakan sistem file yang ada selama proses pembuatan cluster.

Keamanan dan kepatuhan

Sistem file FSx for Lustre mendukung enkripsi saat istirahat dan dalam perjalanan. Amazon FSx secara otomatis mengenkripsi data sistem file saat istirahat menggunakan kunci yang dikelola di (). AWS Key Management Service AWS KMS Data dalam perjalanan juga secara otomatis dienkripsi pada sistem file tertentu Wilayah AWS ketika diakses dari instans Amazon EC2 yang didukung. Untuk informasi selengkapnya tentang enkripsi data di FSx for Lustre Wilayah AWS , termasuk di mana enkripsi data dalam perjalanan didukung, lihat [Enkripsi data di Amazon FSx for Lustre](#) Amazon FSx telah dinilai mematuhi sertifikasi ISO, PCI-DSS, dan SOC, dan HIPAA memenuhi syarat. Untuk informasi selengkapnya, lihat [Keamanan di FSx for Lustre](#).

Asumsi

Dalam panduan ini, kami membuat asumsi berikut:

- Jika Anda menggunakan Amazon Elastic Compute Cloud (Amazon EC2), kita asumsikan bahwa Anda sudah familiar dengan layanan tersebut. Untuk informasi lebih lanjut tentang cara menggunakan Amazon EC2, lihat [Dokumentasi Amazon EC2](#).
- Kami berasumsi bahwa Anda sudah familiar dengan menggunakan Amazon Virtual Private Cloud (Amazon VPC). Untuk informasi lebih lanjut tentang cara menggunakan Amazon VPC, lihat [Panduan Pengguna Amazon VPC](#).
- Kami berasumsi bahwa Anda belum mengubah aturan pada grup keamanan default untuk VPC Anda berdasarkan layanan Amazon VPC. Jika Anda telah mengubahnya, pastikan bahwa Anda menambahkan aturan yang diperlukan untuk mengizinkan lalu lintas jaringan dari instans Amazon EC2 Anda ke sistem file Amazon FSx for Lustre. Untuk rincian lebih lanjut, lihat [Kontrol akses sistem file dengan Amazon VPC](#).

Harga untuk Amazon FSx for Lustre

Dengan Amazon FSx for Lustre, tidak ada biaya perangkat keras atau perangkat lunak dimuka. Anda hanya membayar sumber daya yang digunakan, tanpa komitmen minimum, biaya penyiapan, atau biaya tambahan. Untuk informasi tentang harga dan biaya yang terkait dengan layanan, lihat [Harga Amazon FSx for Lustre](#).

Forum Amazon FSx for Lustre

Jika Anda mengalami masalah saat menggunakan Amazon FSx for Lustre, periksa [Forum](#).

Apakah Anda baru pertama kali menggunakan Amazon FSx for Lustre?

Jika pengguna Amazon FSx for Lustre pertama kali, kami merekomendasikan agar Anda membaca bagian-bagian berikut secara berurutan:

1. Jika Anda siap untuk membuat sistem file Amazon FSx for Lustre pertama Anda, cobalah [Memulai dengan Amazon FSx for Lustre](#).
2. Untuk informasi tentang performa, lihat [Performa Amazon FSx for Lustre](#).
3. Untuk informasi tentang menghubungkan sistem file Anda ke repositori data bucket Amazon S3, lihat [Menggunakan repositori data dengan Amazon FSx for Lustre](#).
4. Untuk detail keamanan Amazon FSx for Lustre, lihat [Keamanan di FSx for Lustre](#).
5. Untuk informasi tentang batas skalabilitas Amazon FSx for Lustre, termasuk throughput dan ukuran sistem file, lihat [Kuota](#).
6. Untuk informasi mengenai API Amazon FSx for Lustre, lihat [Referensi Amazon FSx for Lustre](#).

Menyiapkan Amazon FSx for Lustre

Sebelum Anda menggunakan Amazon FSx for Lustre untuk pertama kalinya, selesaikan tugas di bagian ini. [Mendaftar Amazon Web Services](#) Untuk menyelesaikan [tutorial Memulai](#), pastikan bucket Amazon S3 yang akan Anda tautkan ke sistem file Anda memiliki izin yang tercantum. [Menambahkan izin untuk menggunakan repositori data di Amazon S3](#)

Topik

- [Mendaftar Amazon Web Services](#)
- [Menambahkan izin untuk menggunakan repositori data di Amazon S3](#)
- [Bagaimana FSx for Lustre memeriksa akses ke bucket S3 yang ditautkan](#)
- [Langkah selanjutnya](#)

Mendaftar Amazon Web Services

Untuk mengatur AWS, selesaikan tugas-tugas berikut:

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

Mendaftar untuk Akun AWS

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

Untuk mendaftar untuk Akun AWS

1. Buka <https://portal.aws.amazon.com/billing/signup>.
2. Ikuti petunjuk online.

Bagian dari prosedur pendaftaran melibatkan tindakan menerima panggilan telepon dan memasukkan kode verifikasi di 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 mengirimkan Anda email konfirmasi setelah proses pendaftaran selesai. Anda dapat melihat aktivitas akun Anda saat ini dan mengelola akun Anda dengan mengunjungi <https://aws.amazon.com/> dan memilih Akun Saya.

Buat pengguna dengan akses administratif

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

Amankan Anda Pengguna root akun AWS

1. Masuk ke [AWS Management Console](#) 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.

Menambahkan izin untuk menggunakan repositori data di Amazon S3

Amazon FSx for Lustre sangat terintegrasi dengan Amazon S3. Integrasi ini berarti bahwa aplikasi yang mengakses sistem file FSx for Lustre Anda juga dapat mengakses objek yang disimpan di bucket Amazon S3 Anda yang ditautkan dengan mulus. Untuk informasi selengkapnya, lihat [Menggunakan repositori data dengan Amazon FSx for Lustre](#).

Untuk menggunakan repositori data, Anda harus terlebih dahulu mengizinkan izin IAM tertentu Amazon FSx for Lustre dalam peran yang terkait dengan akun untuk pengguna administrator Anda.

Untuk menanamkan kebijakan yang selaras untuk peran yang menggunakan konsol

1. Masuk ke AWS Management Console dan buka konsol IAM di <https://console.aws.amazon.com/iam/>.
2. Di panel navigasi, pilih Peran.
3. Dari daftar, pilih nama peran untuk menanamkan kebijakan ke dalamnya.
4. Pilih tab Izin.
5. Gulir ke bagian bawah laman dan pilih Tambah kebijakan selaras.

Note

Anda tidak dapat menanam kebijakan yang selaras pada peran terkait-layanan di IAM. Karena layanan terkait menentukan apakah Anda bisa mengubah izin peran tersebut, Anda mungkin bisa menambah kebijakan tambahan dari konsol layanan, API, atau AWS CLI. Untuk melihat dokumentasi peran terkait-layanan untuk layanan, lihat Layanan yang Bekerja dengan IAM AWS dan pilih Ya pada kolom Peran Terkait-Layanan untuk layanan Anda.

6. Pilih Membuat kebijakan dengan Editor Visual
7. Tambahkan pernyataan kebijakan izin berikut.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": [
      "iam:CreateServiceLinkedRole",
      "iam:AttachRolePolicy",
      "iam:PutRolePolicy"
    ],
    "Resource": "arn:aws:iam::*:role/aws-service-role/s3.data-source.lustre.fsx.amazonaws.com/*"
  }
}
```

Setelah Anda membuat kebijakan yang selaras, ini akan secara otomatis tertanam di peran Anda. Untuk informasi lebih lanjut tentang peran terkait layanan, lihat [Menggunakan peran terkait layanan untuk Amazon FSx](#).

Bagaimana FSx for Lustre memeriksa akses ke bucket S3 yang ditautkan

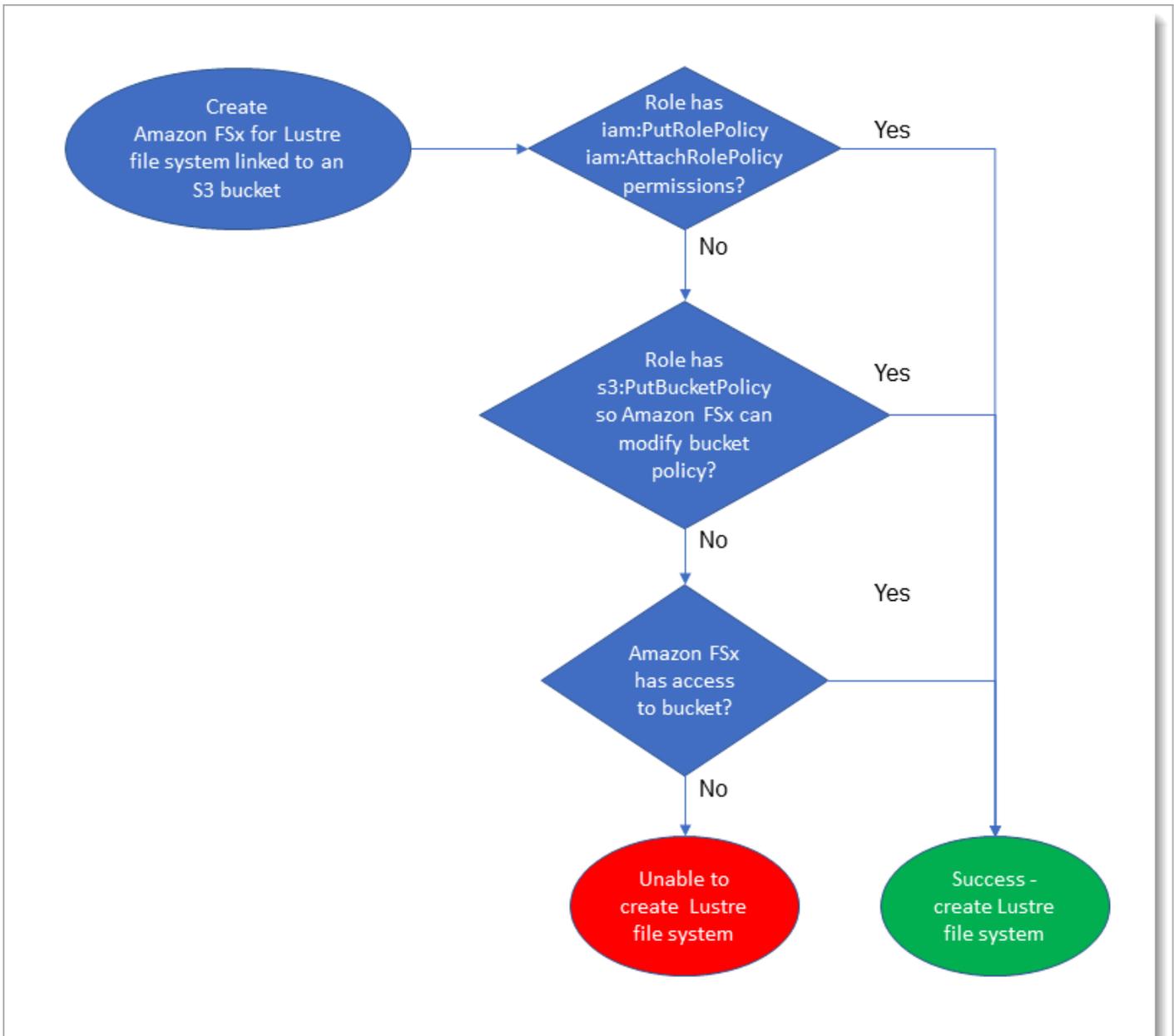
Jika peran IAM yang Anda gunakan untuk membuat sistem file FSx for Lustre tidak memiliki `iam:PutRolePolicy` izin dan, Amazon FSx akan memeriksa apakah peran `iam:AttachRolePolicy` tersebut dapat memperbarui kebijakan bucket S3 Anda. Amazon FSx dapat memperbarui kebijakan bucket Anda jika `s3:PutBucketPolicy` izin disertakan dalam peran

IAM Anda untuk mengizinkan sistem file Amazon FSx mengimpor atau mengekspor data ke bucket S3 Anda. Jika diizinkan untuk mengubah kebijakan bucket, Amazon FSx menambahkan izin berikut ke kebijakan bucket:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:PutObject`
- `s3:Get*`
- `s3:List*`
- `s3:PutBucketNotification`
- `s3:PutBucketPolicy`
- `s3>DeleteBucketPolicy`

Jika Amazon FSx tidak dapat mengubah kebijakan bucket, Amazon FSx akan memeriksa apakah kebijakan bucket yang ada memberi Amazon FSx akses ke bucket.

Jika semua opsi ini gagal, maka permintaan untuk membuat sistem file gagal. Diagram berikut mengilustrasikan pemeriksaan yang diikuti Amazon FSx saat menentukan apakah sistem file dapat mengakses bucket S3 yang akan ditautkan.



Langkah selanjutnya

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

Memulai dengan Amazon FSx for Lustre

Berikut ini, Anda dapat mempelajari cara untuk mulai menggunakan Amazon FSx for Lustre. Langkah-langkah ini memandu Anda membuat sistem file Amazon FSx for Lustre dan mengaksesnya dari instans-instans komputasi Anda. Secara opsional, langkah-langkah tersebut menunjukkan cara menggunakan sistem file Amazon FSx for Lustre Anda untuk memproses data di bucket Amazon S3 Anda dengan aplikasi berbasis file Anda.

Latihan memulai ini terdiri dari langkah-langkah sebagai berikut.

Topik

- [Prasyarat](#)
- [Buat sistem file FSx for Lustre Anda](#)
- [Instal dan konfigurasi klien Lustre](#)
- [Pasang sistem berkas](#)
- [Jalankan alur kerja Anda](#)
- [Pembersihan sumber daya](#)

Prasyarat

Untuk melaksanakan latihan memulai ini, Anda memerlukan hal-hal berikut ini:

- AWS Akun dengan izin yang diperlukan untuk membuat sistem file Amazon FSx for Lustre dan instans Amazon EC2. Untuk informasi selengkapnya, lihat [Menyiapkan Amazon FSx for Lustre](#).
- Buat grup keamanan Amazon VPC untuk dikaitkan dengan sistem file FSx for Lustre Anda, dan jangan mengubahnya setelah pembuatan sistem file. Untuk informasi selengkapnya, lihat [Untuk membuat grup keamanan untuk sistem file Amazon FSx Anda](#).
- Instans Amazon EC2 menjalankan rilis yang di-support Linux di virtual private cloud (VPC) Anda berdasarkan layanan Amazon VPC. Untuk memulai latihan ini, kami sarankan menggunakan Amazon Linux 2023. Anda akan menginstal klien Lustre pada instance EC2 ini, dan kemudian memasang sistem file FSx for Lustre Anda pada instance EC2. Untuk informasi selengkapnya tentang membuat instans EC2, lihat [Memulai: Meluncurkan instans](#) atau [Meluncurkan instans Anda](#) di Panduan Pengguna Amazon EC2.

Klien Lustre mendukung Amazon Linux; Amazon Linux 2; Amazon Linux 2023; CentOS dan Red Hat Enterprise Linux 7.7 hingga 7.9, 8.2 hingga 8.9, 9.0, 9.3, dan 9.4; Rocky Linux 8.4 hingga 8.9, 9.0, 9.3, dan 9.4; SUSE Linux Enterprise Server 12 SP3, SP4, dan SP5; dan Ubuntu 18.04, 20.04, dan 22.04. Untuk informasi selengkapnya, lihat [Sistem file Lustre dan kompatibilitas kernel klien](#).

Saat membuat instans Amazon EC2 Anda untuk mulai latihan, selalu ingat hal berikut:

- Kami merekomendasikan Anda membuat instans Anda di VPC default Anda.
- Kami merekomendasikan Anda menggunakan grup keamanan default saat membuat instans EC2 Anda.
- Setiap sistem file FSx for Lustre memerlukan satu alamat IP untuk setiap server metadata (MDS) dan satu alamat IP untuk setiap server penyimpanan (OSS).
 - Untuk sistem file Persistent_2 dengan konfigurasi metadata, setiap nilai IOPS Metadata 12000 juga memerlukan satu alamat IP dalam subnet tempat sistem file Anda berada.
 - Sistem file SSD persisten disediakan dengan penyimpanan 2,4 TiB per OSS.
 - Sistem file HDD persisten dengan kapasitas throughput 12 MB/s/Tib disediakan dengan penyimpanan 6 TiB per OSS.
 - Sistem file HDD persisten dengan kapasitas throughput 40 MB/s/Tib disediakan dengan penyimpanan 1,8 TiB per OSS.
 - Sistem file Scratch_2 disediakan dengan penyimpanan 2,4 TiB per OSS.
 - Sistem file Scratch_1 disediakan dengan penyimpanan 3,6 TiB per OSS.
- Bucket Amazon S3 untuk menyimpan data agar beban kerja Anda diproses. Bucket S3 akan menjadi repositori data tahan lama yang ditautkan untuk sistem file FSx for Lustre Anda.
- Tentukan jenis sistem file Amazon FSx for Lustre yang ingin Anda buat, scratch atau persisten. Untuk informasi selengkapnya, lihat [Opsi penyebaran sistem file untuk FSx for Lustre](#).

Buat sistem file FSx for Lustre Anda

Selanjutnya, buatlah sistem file Anda di konsol.

Untuk membuat sistem file Anda

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Dari dasbor, pilih Buat sistem file untuk memulai wizard pembuatan sistem file.
3. Pilih FSx for Lustre lalu pilih Selanjutnya untuk menampilkan halaman Buat Sistem File.

4. Berikan informasi di bagian Detail sistem file:

- Untuk nama sistem file-opsional, berikan nama untuk sistem file Anda. Anda dapat menggunakan hingga 256 huruf, spasi, dan angka Unicode, ditambah karakter khusus + - = . _ : /.
- Untuk jenis Deployment dan storage, pilih salah satu opsi:

Penyimpanan SSD menyediakan beban kerja dengan latensi rendah, IOPS-intensif yang biasanya memiliki operasi file yang kecil dan acak. Penyimpanan HDD menyediakan beban kerja throughput-intensif yang biasanya memiliki operasi file berurutan dan Large.

Untuk informasi selengkapnya tentang jenis penyimpanan, lihat [Beberapa opsi penyimpanan](#).

Untuk informasi selengkapnya tentang jenis penerapan, lihat [Opsi penyebaran untuk sistem file FSx for Lustre](#).

Untuk informasi selengkapnya tentang Wilayah AWS tempat mengenkripsi data dalam perjalanan tersedia, lihat [Mengkripsi data dalam perjalanan](#)

- Pilih jenis penyebaran SSD yang Persisten untuk penyimpanan jangka panjang dan untuk beban kerja yang sensitif terhadap latensi yang membutuhkan tingkat IOP/throughput tertinggi. Server file sangat tersedia, data secara otomatis direplikasi dalam Availability Zone sistem file, dan mendukung enkripsi data dalam perjalanan. Persistent, SSD menggunakan Persistent 2, generasi terbaru dari sistem file persisten.
- Pilih jenis penyebaran HDD Persisten untuk penyimpanan jangka panjang dan untuk beban kerja yang berfokus pada throughput yang tidak sensitif terhadap latensi. Server file tersedia melimpah, data secara otomatis direplikasi dalam sistem file milik Availability Zone, dan jenis ini mendukung enkripsi data dalam transit. Persistent, HDD menggunakan tipe penerapan Persistent 1.

Pilih dengan cache SSD untuk membuat cache SSD yang berukuran hingga 20 persen dari kapasitas penyimpanan HDD Anda untuk menyediakan latensi sub-milidetik dan IOPS yang lebih tinggi untuk file yang sering diakses.

- Pilih Scratch, tipe penyebaran SSD untuk penyimpanan sementara dan pemrosesan data jangka pendek. Scratch, SSD menggunakan sistem file Scratch 2, dan menawarkan enkripsi data dalam transit.
- Pilih jumlah Throughput per unit penyimpanan yang Anda inginkan untuk sistem file Anda. Opsi ini hanya berlaku untuk jenis deployment Persisten.

Throughput per unit penyimpanan adalah jumlah Baca dan Tulis throughput untuk setiap 1 tebibita (TiB) penyimpanan yang telah disediakan, dalam MB/s/TiB. Anda membayar untuk jumlah throughput yang Anda berikan:

- Untuk penyimpanan SSD Persistent, pilih nilai 125, 250, 500, atau 1.000 MB/s/Tib.
- Untuk penyimpanan HDD Persistent, pilih nilai 12 atau 40 MB/s/Tib.

Anda dapat menambah atau mengurangi jumlah throughput per unit penyimpanan sesuai kebutuhan setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat [Mengelola kapasitas throughput](#).

- Untuk kapasitas Penyimpanan, atur jumlah kapasitas penyimpanan untuk sistem file Anda, di TiB:
 - Untuk jenis penyebaran SSD yang Persisten, atur ini ke nilai 1,2 TiB, 2,4 TiB, atau kenaikan 2,4 TiB.
 - Untuk jenis penyebaran HDD yang Persisten, nilai ini dapat berupa peningkatan 6,0 TiB untuk sistem file 12 MB/s/Tib dan peningkatan 1,8 TiB untuk sistem file 40 MB/s/Tib.

Anda dapat meningkatkan jumlah kapasitas penyimpanan sebagaimana diperlukan setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat [Mengelola kapasitas penyimpanan](#).

- Untuk Konfigurasi Metadata, Anda memiliki dua opsi untuk menyediakan jumlah Metadata IOPS untuk sistem file Anda:
 - Pilih Otomatis (default) jika Anda ingin Amazon FSx secara otomatis menyediakan dan menskalakan Metadata IOPS pada sistem file Anda berdasarkan kapasitas penyimpanan sistem file Anda.
 - Pilih User-provisioned jika Anda ingin menentukan jumlah Metadata IOPS yang akan disediakan untuk sistem file Anda. Nilai yang valid adalah 1500 3000 6000, 12000,, dan kelipatan 12000, hingga maksimum. 192000

Untuk informasi selengkapnya tentang Metadata IOPS, lihat. [Konfigurasi kinerja metadata kilau](#)

- Untuk Jenis kompresi data, pilih TIDAK ADA untuk menonaktifkan kompresi data atau pilih LZ4 untuk mengaktifkan kompresi data dengan algoritma LZ4. Untuk informasi selengkapnya, lihat [Kompresi data Lustre](#).

Semua sistem file FSx for Lustre dibangun di atas Lustre versi 2.15 saat dibuat menggunakan konsol Amazon FSx.

5. Di bagian Jaringan & keamanan, berikan informasi jaringan dan grup keamanan berikut:

- Untuk Virtual Private Cloud (VPC), pilih VPC yang ingin Anda kaitkan dengan sistem file Anda. Untuk mulai latihan ini, pilih VPC yang sama yang Anda pilih untuk instans Amazon EC2 Anda.
- Untuk Grup keamanan VPC, ID untuk grup keamanan default untuk VPC Anda harus sudah ditambahkan. Jika Anda tidak menggunakan grup keamanan default, pastikan bahwa aturan jalur masuk berikut ditambahkan ke grup keamanan yang Anda gunakan untuk mulai latihan ini.

Type	Protokol	Rentang port	Sumber	Deskripsi
Semua TCP	TCP	0-65535	<i>the_ID_of _this_sec urity_gro up</i> kustom	Aturan lalu lintas jalur masuk Lustre

Tangkapan layar berikut menunjukkan contoh mengedit aturan jalur masuk.

Edit inbound rules

Type: All traffic | Protocol: All | Port Range: 0 - 65535 | Source: Custom | Description: Inbound TCP Lustre con...

Add Rule

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

Cancel Save

⚠ Important

Pastikan bahwa grup keamanan yang Anda gunakan mengikuti instruksi konfigurasi yang disediakan [Kontrol akses sistem file dengan Amazon VPC](#). Anda harus mengatur grup keamanan untuk memungkinkan lalu lintas masuk pada port 988 dan 1018-1023

dari grup keamanan itu sendiri atau CIDR subnet penuh, yang diperlukan untuk memungkinkan host sistem file berkomunikasi satu sama lain.

- Untuk Subnet, pilih nilai apa pun dari daftar subnet yang tersedia.
6. Untuk bagian Enkripsi, pilihan yang tersedia bervariasi tergantung pada jenis sistem file mana yang Anda buat:
- Untuk sistem file persisten, Anda dapat memilih kunci enkripsi AWS Key Management Service (AWS KMS) untuk mengenkripsi data pada sistem file Anda saat istirahat.
 - Untuk sistem file scratch, data saat istirahat dienkripsi menggunakan kunci yang dikelola oleh AWS
 - Untuk scratch 2 dan sistem file persisten, data pada transit dienkripsi secara otomatis ketika sistem file diakses dari jenis instans Amazon EC2 yang di-support. Untuk informasi selengkapnya, lihat [Mengkripsi data dalam perjalanan](#).
7. Untuk Impor/Ekspor Repositori Data - bagian opsional, menautkan sistem file Anda ke repositori data Amazon S3 dinonaktifkan secara default. Untuk informasi tentang mengaktifkan opsi ini dan membuat asosiasi repositori data ke bucket S3 yang ada, lihat. [Untuk menautkan bucket S3 saat membuat sistem file \(konsol\)](#)

 Important

- Memilih opsi ini juga menonaktifkan cadangan dan Anda tidak akan dapat mengaktifkan cadangan saat membuat sistem file.
 - Jika Anda menautkan satu atau lebih sistem file Amazon FSx for Lustre ke bucket Amazon S3, jangan hapus bucket Amazon S3 sampai semua sistem file tertaut telah dihapus.
8. Untuk Logging - opsional, logging diaktifkan secara default. Saat diaktifkan, kegagalan dan peringatan untuk aktivitas repositori data pada sistem file Anda akan dicatat ke Amazon Logs. CloudWatch Untuk informasi tentang mengonfigurasi logging, lihat [Mengelola logging](#).
9. Pada Backup dan pemeliharaan - opsional, Anda dapat melakukan hal berikut.

Untuk backup otomatis harian:

- Nonaktifkan cadangan otomatis harian. Opsi ini diaktifkan secara default, kecuali jika Anda mengaktifkan Impor/Ekspor Repositori Data,.

- Atur waktu mulai untuk Jendela backup otomatis harian.
- Atur periode retensi cadangan otomatis, dari 1 - 35 hari.

Untuk informasi selengkapnya, lihat [Bekerja dengan backup](#).

10. Atur waktu mulai Jendela pemeliharaan mingguan, atau biarkan saja pengaturan default Tidak Ada preferensi.
11. Untuk Root Squash - opsional, root squash dinonaktifkan secara default. Untuk informasi tentang mengaktifkan dan mengonfigurasi root squash, lihat. [Untuk mengaktifkan root squash saat membuat sistem file \(konsol\)](#)
12. Buat tag apa pun yang ingin Anda terapkan ke sistem file Anda.
13. Pilih Selanjutnya untuk menampilkan halaman Buat ringkasan sistem file.
14. Tinjau pengaturan untuk sistem file Amazon FSx for Lustre Anda, dan pilih Buat sistem file.

Sekarang setelah Anda membuat sistem file Anda, perhatikan nama domain dan nama pemasangan sistem file yang memenuhi syarat untuk langkah selanjutnya. Anda dapat menemukan nama domain yang memenuhi syarat dan nama mount untuk sistem file dengan memilih nama sistem file di dasbor Cache, dan kemudian memilih Lampirkan.

Instal dan konfigurasi klien Lustre

Sebelum Anda dapat mengakses sistem file Amazon FSx for Lustre dari instans Amazon EC2 Anda, Anda harus melakukan hal berikut:

- Verifikasi instans EC2 Anda memenuhi persyaratan kernel minimum.
- Perbarui kernel jika diperlukan.
- Unduh dan instal klien Lustre.

Untuk memeriksa versi kernel dan mengunduh klien Lustre

1. Buka jendela terminal pada instans EC2 Anda.
2. Tentukan kernel mana yang sedang berjalan pada instans komputasi Anda dengan menjalankan perintah berikut.

```
uname -r
```

3. Lakukan salah satu hal berikut ini:

- Jika perintah kembali `6.1.79-99.167.amzn2023.x86_64` untuk instans-instans EC2 berbasis x86, atau `6.1.79-99.167.amzn2023.aarch64` atau lebih tinggi untuk instans-instans EC2 berbasis Graviton2, unduh dan instal Lustre client dengan perintah berikut ini.

```
sudo dnf install -y lustre-client
```

- Jika perintah memberikan hasil kurang dari `6.1.79-99.167.amzn2023.x86_64` untuk instans-instans EC2 berbasis x86, atau kurang dari `6.1.79-99.167.amzn2023.aarch64` untuk instans-instans EC2 berbasis Graviton2, perbarui kernel dan reboot instans-instans Amazon EC2 Anda dengan menjalankan perintah berikut.

```
sudo dnf -y update kernel && sudo reboot
```

Konfirmasikan bahwa kernel telah diperbarui menggunakan perintah `uname -r`. Kemudian unduh dan instal Lustre client seperti yang dideskripsikan di atas.

Untuk informasi tentang menginstal Lustre client pada distribusi Linux lainnya, lihat [Menginstal klien Lustre](#).

Pasang sistem berkas

Untuk me-mount sistem file Anda, Anda akan membuat direktori pemasangan, atau mount point, dan kemudian me-mount sistem file ke klien Anda, dan memverifikasi bahwa klien Anda dapat mengakses sistem file.

Untuk memasang sistem file Anda

1. Buatlah sebuah direktori untuk titik pemasangan dengan perintah berikut ini.

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

2. Pasang sistem file Amazon FSx for Lustre ke direktori yang Anda buat. Gunakan perintah berikut dan ganti item berikut:

- Ganti *file_system_dns_name* dengan nama Sistem Nama Domain (DNS) dari sistem file sebenarnya.

- Ganti *mountname* dengan nama mount sistem file, yang bisa Anda dapatkan dengan menjalankan `describe-file-systems` AWS CLI perintah atau operasi API [DescribeFileSistem](#).

```
sudo mount -t lustre -o relatime,flock file_system_dns_name@tcp:/mountname /mnt/fsx
```

Perintah ini memasang sistem file Anda dengan dua pilihan, `-o relatime` dan `flock`:

- `relatime`— Sementara `atime` opsi mempertahankan `atime` (waktu akses inode) data untuk setiap kali file diakses, `relatime` opsi ini juga mempertahankan `atime` data, tetapi tidak untuk setiap kali file diakses. Dengan `relatime` opsi diaktifkan, `atime` data ditulis ke disk hanya jika file telah dimodifikasi sejak `atime` data terakhir diperbarui (`mtime`), atau jika file terakhir diakses lebih dari jumlah waktu tertentu yang lalu (6 jam secara default). Menggunakan salah satu `atime` opsi `relatime` or akan mengoptimalkan proses [rilis file](#).

Note

Jika beban kerja Anda memerlukan akurasi waktu akses yang tepat, Anda dapat memasang dengan opsi `atime` pemasangan. Namun, hal itu dapat memengaruhi kinerja beban kerja dengan meningkatkan lalu lintas jaringan yang diperlukan untuk mempertahankan nilai waktu akses yang tepat.

Jika beban kerja Anda tidak memerlukan waktu akses metadata, menggunakan opsi `noatime` pemasangan untuk menonaktifkan pembaruan untuk mengakses waktu dapat memberikan peningkatan kinerja. Ketahuilah bahwa proses `atime` terfokus seperti rilis file atau rilis validitas data akan menjadi tidak akurat dalam rilisnya.

- `flock` — Memungkinkan penguncian file untuk sistem file Anda. Jika Anda tidak ingin penguncian file diaktifkan, gunakan perintah `mount` tanpa `flock`.
3. Verifikasi bahwa perintah pemasangan berhasil dengan mencantumkan isi direktori tempat Anda memasang sistem file `/mnt/fsx`, dengan menggunakan perintah berikut ini.

```
ls /mnt/fsx
import-path lustre
$
```

Anda juga dapat menggunakan perintah `df`, berikut.

```
df
```

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
devtmpfs	1001808	0	1001808	0%	/dev
tmpfs	1019760	0	1019760	0%	/dev/shm
tmpfs	1019760	392	1019368	1%	/run
tmpfs	1019760	0	1019760	0%	/sys/fs/cgroup
/dev/xvda1	8376300	1263180	7113120	16%	/
123.456.789.0@tcp:/ <i>mountname</i>	3547698816	13824	3547678848	1%	/mnt/fsx
tmpfs	203956	0	203956	0%	/run/user/1000

Hasilnya menunjukkan sistem file Amazon FSx terpasang pada /mnt/fsx.

Jalankan alur kerja Anda

Kini setelah sistem file Anda dibuat dan dipasang ke instans komputasi, Anda dapat menggunakannya untuk menjalankan beban kerja komputasi Anda yang ber-performa tinggi.

Anda dapat membuat asosiasi repositori data untuk menautkan sistem file Anda ke repositori data Amazon S3, Untuk informasi selengkapnya, lihat. [Menautkan sistem file Anda ke bucket S3](#)

Setelah menautkan sistem file ke repositori data Amazon S3, Anda dapat mengekspor data yang telah Anda tulis ke sistem file kembali ke bucket Amazon S3 kapan saja. Dari sebuah terminal pada salah satu instans komputasi Anda, jalankan perintah berikut untuk mengekspor file ke bucket Amazon S3 Anda.

```
sudo lfs hsm_archive file_name
```

Untuk informasi lebih lanjut tentang cara menjalankan perintah ini pada sebuah folder atau koleksi besar file dengan cepat, lihat [Mengekspor file menggunakan perintah HSM](#).

Pembersihan sumber daya

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

Untuk membersihkan sumber daya

1. Jika Anda ingin melakukan ekspor akhir, jalankan perintah berikut.

```
nohup find /mnt/fsx -type f -print0 | xargs -0 -n 1 sudo lfs hsm_archive &
```

2. Pada konsol Amazon EC2, akhiri instans Anda. Untuk informasi selengkapnya, lihat [Menghentikan Instans Anda](#) di Panduan Pengguna Amazon EC2.
3. Pada konsol Amazon FSx for Lustre, hapus sistem file Anda dengan prosedur berikut:
 - a. Di panel navigasi, pilih Sistem file.
 - b. Pilih sistem file yang ingin Anda hapus dari daftar sistem berkas di dasbor.
 - c. Pilih Tindakan, pilih Hapus sistem file.
 - d. Di kotak dialog yang muncul, pilih apakah Anda ingin mengambil cadangan akhir dari sistem file. Kemudian berikan ID sistem file untuk mengonfirmasi penghapusan. Pilih Hapus sistem file.
4. Jika Anda membuat bucket Amazon S3 untuk latihan ini, dan jika Anda tidak ingin menyimpan data yang Anda ekspor, sekarang Anda dapat menghapusnya. Untuk informasi selengkapnya, lihat [Menghapus bucket](#) di Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Opsi penyebaran untuk sistem file FSx for Lustre

FSx for Lustre menyediakan sistem file paralel berkinerja tinggi yang menyimpan data di beberapa server file jaringan untuk memaksimalkan kinerja dan mengurangi kemacetan. Server ini memiliki beberapa disk. Untuk menyebarkan beban, Amazon FSx membagi data sistem file menjadi potongan yang lebih kecil dan menyebarkannya ke disk dan server menggunakan proses yang disebut striping. Untuk informasi lebih lanjut tentang FSx for Lustre data striping, lihat [Sedang melakukan stripe data di sistem file Anda](#)

Merupakan praktik terbaik untuk menautkan repositori data jangka panjang yang sangat tahan lama yang berada di Amazon S3 dengan sistem file berkinerja tinggi FSx for Lustre Anda.

Dalam skenario ini, Anda menyimpan kumpulan data di repositori data Amazon S3 yang ditautkan. Saat Anda membuat sistem file FSx for Lustre, Anda menautkannya ke repositori data S3 Anda. Pada titik ini, objek dalam bucket S3 Anda terdaftar sebagai file dan direktori pada sistem file FSx Anda. Amazon FSx kemudian secara otomatis akan menyalin isi file dari S3 ke sistem file Lustre Anda ketika sebuah file diakses untuk pertama kalinya pada sistem file Amazon FSx. Setelah beban kerja komputasi Anda berjalan, atau kapan saja, Anda dapat menggunakan tugas repositori data untuk mengekspor perubahan kembali ke S3. Untuk informasi selengkapnya, lihat [Menggunakan repositori data dengan Amazon FSx for Lustre](#) dan [Menggunakan tugas repositori data untuk mengekspor perubahan](#).

Opsi penyebaran sistem file untuk FSx for Lustre

Amazon FSx for Lustre menyediakan dua opsi sistem deployment file: scratch dan persisten.

Note

Kedua opsi deployment mensupport penyimpanan solid state drive (SSD). Namun, penyimpanan hard disk drive (HDD) hanya didukung di salah satu jenis penyebaran persisten.

Anda memilih jenis penerapan sistem file saat membuat sistem file baru, menggunakan, AWS Command Line Interface (AWS CLI) AWS Management Console, atau Amazon fsX for Lustre API. Untuk informasi selengkapnya, lihat [Buat sistem file FSx for Lustre Anda](#) dan [CreateFileSistem](#) di Referensi API Amazon FSx.

Enkripsi data saat istirahat diaktifkan secara otomatis saat Anda membuat sistem file Amazon FSx for Lustre, terlepas dari jenis penerapan yang Anda gunakan. Scratch 2 dan sistem file persisten secara otomatis mengenkripsi data dalam transit ketika mereka diakses dari Instans Amazon EC2 yang mensupport enkripsi dalam transit. Untuk informasi lebih lanjut tentang enkripsi, lihat [Enkripsi data di Amazon FSx for Lustre](#).

Sistem file Scratch

Sistem file Scratch dirancang untuk penyimpanan sementara dan pemrosesan data jangka pendek. Data tidak direplikasi dan tidak bertahan jika server file gagal. Sistem file scratch menyediakan keluaran throughput yang tinggi hingga enam kali throughput dasar yaitu 200 MBps per TiB kapasitas penyimpanan. Untuk informasi selengkapnya, lihat [Performa kumpulan sistem file](#).

Gunakan sistem file scratch ketika Anda membutuhkan penyimpanan yang mengoptimalkan biaya untuk beban kerja jangka pendek, proses berat.

Pada sistem file scratch, server file tidak diganti jika gagal dan data tidak direplikasi. Jika server file atau disk penyimpanan menjadi tidak tersedia pada sistem file scratch, file yang disimpan di server lain masih dapat diakses. Jika klien mencoba untuk mengakses data yang ada di server atau disk tidak tersedia, klien akan mengalami kesalahan I/O langsung.

Tabel berikut menggambarkan ketersediaan atau daya tahan yang sistem file scratch dengan contoh ukuran yang dirancang selama satu hari dan seminggu. Karena sistem file yang lebih besar memiliki lebih banyak server file dan lebih banyak disk, kemungkinan kegagalan meningkat.

Ukuran sistem file (TiB)	Jumlah server file	Ketersediaan/daya tahan lebih dari satu hari	Ketersediaan/daya tahan lebih dari satu minggu
1.2	2	99,9%	99,4%
2.4	2	99,9%	99,4%
4.8	3	99,8%	99,2%
9.6	5	99,8%	98,6%
50,4	22	99,1%	93,9%

Sistem file persisten

Sistem file persisten dirancang untuk penyimpanan jangka panjang dan beban kerja. Server file sangat tersedia, dan data secara otomatis direplikasi dalam Availability Zone yang sama di mana sistem file berada. Volume data yang dilampirkan pada server file direplikasi secara independen dari server file ke file yang dilampirkan.

Amazon FSx terus memantau sistem file persisten untuk kegagalan perangkat keras, dan secara otomatis menggantikan komponen infrastruktur jika terjadi kegagalan. Pada sistem file persisten, jika server file menjadi tidak tersedia, itu diganti secara otomatis dalam beberapa menit setelah kegagalan. Selama jangka waktu tersebut, klien meminta data pada server yang secara transparan coba lagi dan akhirnya berhasil setelah server file diganti. Data pada sistem file persisten direplikasi pada disk, dan setiap disk yang gagal secara otomatis diganti secara transparan.

Gunakan sistem file persisten untuk penyimpanan jangka panjang dan untuk beban kerja yang berfokus pada throughput yang berjalan untuk waktu yang lama atau tanpa batas waktu, dan itu mungkin sensitif terhadap gangguan ketersediaan.

Jenis penerapan persisten secara otomatis mengenkripsi data saat transit saat diakses dari instans Amazon EC2 yang mendukung enkripsi saat transit.

Amazon FSx for Lustre mendukung dua jenis penerapan persisten: Persistent_1 dan Persistent_2.

Jenis penerapan persistent_2

Persistent_2 adalah generasi terbaru dari tipe penerapan Persistent, dan paling cocok untuk kasus penggunaan yang memerlukan penyimpanan jangka panjang, dan memiliki beban kerja yang sensitif terhadap latensi yang memerlukan tingkat IOPS dan throughput tertinggi. Jenis penyebaran persistent_2 mendukung tingkat throughput per unit penyimpanan yang lebih tinggi dibandingkan dengan sistem file Persistent_1, dan menawarkan empat tingkat throughput per unit penyimpanan: 125, 250, 500, dan 1000 MB/s/Tib.

Jika Anda menentukan konfigurasi metadata saat membuat sistem file Persistent_2, Anda dapat memilih untuk meningkatkan kinerja metadata dari waktu ke waktu—terlepas dari kapasitas penyimpanan sistem file Anda—untuk memenuhi persyaratan kinerja yang terus meningkat dan untuk mendukung beban kerja yang lebih besar.

Anda dapat membuat sistem file Persistent_2 dengan mode konfigurasi metadata menggunakan konsol Amazon FSx,, dan API. AWS Command Line Interface

Jenis penerapan persistent_1

Jenis penyebaran persistent_1 dapat dibangun di atas Lustre 2.10 atau 2.12, dan mendukung jenis penyimpanan SSD (solid state drive) dan HDD (hard disk drive). Jenis penerapan Persistent_1 sangat cocok untuk kasus penggunaan yang memerlukan penyimpanan jangka panjang, dan memiliki beban kerja yang berfokus pada throughput yang tidak sensitif terhadap latensi.

Untuk sistem file Persistent_1 dengan penyimpanan SSD, throughput per unit penyimpanan adalah 50, 100, atau 200 MB/s per tebibyte (TiB). Untuk penyimpanan HDD, throughput Persistent_1 per unit penyimpanan adalah 12 atau 40 MB/s per TiB.

Anda dapat membuat jenis penerapan Persistent_1 hanya dengan menggunakan API Amazon FSx dan AWS CLI Amazon.

Wilayah yang tersedia

Jenis penerapan persisten tersedia sebagai berikut: Wilayah AWS

Wilayah AWS	Persistent_1	Persistent_2
AS Timur (Ohio)	✓	✓
AS Timur (Virginia Utara)	✓	✓
Zona Lokal AS Timur (Atlanta)		✓ (Hanya 125 dan 250 persisten)
AS Barat (California Utara)	✓	
Zona Lokal AS Barat (Los Angeles)	✓	
AS Barat (Oregon)	✓	✓
Afrika (Cape Town)	✓	
Asia Pasifik (Hong Kong)	✓	✓
Asia Pasifik (Hyderabad)	✓	

Wilayah AWS	Persistent_1	Persistent_2
Asia Pasifik (Jakarta)	✓	
Asia Pasifik (Melbourne)	✓	
Asia Pasifik (Mumbai)	✓	✓
Asia Pasifik (Osaka)	✓	
Asia Pasifik (Seoul)	✓	✓
Asia Pasifik (Singapura)	✓	✓
Asia Pasifik (Sydney)	✓	✓
Asia Pasifik (Tokyo)	✓	✓
(Canada (Central)	✓	✓
Kanada Barat (Calgary)		✓ (Hanya 125 dan 250 persisten)
Eropa (Frankfurt)	✓	✓
Eropa (Irlandia)	✓	✓
Eropa (London)	✓	✓
Eropa (Milan)	✓	
Eropa (Paris)	✓	
Eropa (Spanyol)	✓	
Eropa (Stockholm)	✓	✓
Eropa (Zürich)	✓	

Wilayah AWS	Persistent_1	Persistent_2
Israel (Tel Aviv)		✓ (Hanya 125 dan 250 persisten)
Timur Tengah (Bahrain)	✓	
Timur Tengah (UEA)	✓	
Amerika Selatan (Sao Paulo)	✓	
AWS GovCloud (AS-Timur)	✓	
AWS GovCloud (AS-Barat)	✓	

Untuk informasi lebih lanjut tentang kinerja FSx for Lustre, lihat [Performa kumpulan sistem file](#)

Menggunakan repositori data dengan Amazon FSx for Lustre

Amazon FSx for Lustre menyediakan sistem file berkinerja tinggi yang dioptimalkan untuk pemrosesan beban kerja yang cepat. Amazon FSx for Lustre dapat mendukung beban kerja seperti machine learning, komputasi performa tinggi (HPC), pemrosesan video, pemodelan keuangan, dan electronic design automation (EDA). Beban kerja ini biasanya membutuhkan data untuk disajikan menggunakan antarmuka sistem file berkecepatan tinggi yang dapat diskalakan untuk akses data. Seringkali, kumpulan data yang digunakan untuk beban kerja ini disimpan dalam repositori data jangka panjang di Amazon S3. FSx for Lustre terintegrasi secara native dengan Amazon S3, membuatnya lebih mudah untuk memproses dataset dengan sistem file Lustre.

Note

Pencadangan sistem file tidak didukung pada sistem file yang ditautkan ke repositori data. Untuk informasi selengkapnya, lihat [Bekerja dengan backup](#).

Topik

- [Gambaran umum tentang repositori data](#)
- [Dukungan metadata POSIX untuk repositori data](#)
- [Menautkan sistem file Anda ke bucket S3](#)
- [Mengimpor perubahan dari repositori data](#)
- [Mengekspor perubahan ke repositori data](#)
- [Tugas repositori data](#)
- [Melepaskan file](#)
- [Menggunakan Amazon FSx dengan data lokal](#)
- [Log peristiwa repositori data](#)
- [Bekerja dengan jenis penyebaran yang lebih lama](#)

Gambaran umum tentang repositori data

Saat Anda menggunakan Amazon FSx for Lustre dengan repositori data, Anda dapat menelan dan memproses volume besar data file dalam sistem file berkinerja tinggi dengan menggunakan tugas repositori data impor dan impor otomatis. Pada saat yang sama, Anda dapat menulis hasil ke repositori data Anda dengan menggunakan tugas repositori data ekspor atau ekspor otomatis. Dengan fitur-fitur ini, Anda dapat memulai ulang beban kerja Anda kapan saja menggunakan data terbaru yang disimpan di repositori data Anda.

Note

Asosiasi repositori data, ekspor otomatis, dan dukungan untuk beberapa repositori data tidak tersedia di FSx for Lustre 2.10 sistem file atau sistem file. Scratch 1

FSx for Lustre sangat terintegrasi dengan Amazon S3. Integrasi ini berarti Anda dapat mengakses objek yang disimpan di bucket Amazon S3 dengan mulus dari aplikasi yang memasang sistem file FSx for Lustre Anda. Anda juga dapat menjalankan beban kerja intensif komputasi di instans Amazon EC2 di AWS Cloud dan mengeksport hasilnya ke repositori data setelah beban kerja selesai.

Untuk mengakses objek di repositori data Amazon S3 sebagai file dan direktori pada sistem file, metadata file dan direktori harus dimuat ke dalam sistem file. Anda dapat memuat metadata dari repositori data tertaut saat membuat asosiasi repositori data.

Selain itu, Anda dapat mengimpor metadata file dan direktori dari repositori data tertaut ke sistem file menggunakan impor otomatis atau menggunakan tugas repositori data impor. Saat Anda mengaktifkan impor otomatis untuk asosiasi repositori data, sistem file Anda secara otomatis mengimpor metadata file saat file dibuat, dimodifikasi, dan/atau dihapus di repositori data S3. Atau, Anda dapat mengimpor metadata untuk file dan direktori baru atau yang diubah menggunakan tugas repositori data impor.

Note

Tugas repositori data impor dan impor otomatis dapat digunakan secara bersamaan pada sistem file.

Anda juga dapat mengeksport file dan metadata terkait di sistem file Anda ke repositori data Anda menggunakan ekspor otomatis atau menggunakan tugas repositori data ekspor. Saat Anda

mengaktifkan ekspor otomatis pada asosiasi repositori data, sistem file Anda secara otomatis mengekspor data file dan metadata saat file dibuat, dimodifikasi, atau dihapus. Atau, Anda dapat mengekspor file atau direktori menggunakan tugas repositori data ekspor. Saat Anda menggunakan tugas repositori data ekspor, data file dan metadata yang dibuat atau dimodifikasi sejak tugas terakhir tersebut diekspor.

Note

- Tugas repositori data ekspor dan ekspor otomatis tidak dapat digunakan secara bersamaan pada sistem file.
- Asosiasi repositori data hanya mengekspor file biasa, symlink dan direktori. Ini berarti semua jenis file lainnya (khusus FIFO, khusus blok, khusus karakter, dan soket) tidak akan diekspor sebagai bagian dari proses ekspor seperti tugas repositori data ekspor dan ekspor otomatis.

FSx for Lustre juga mendukung beban kerja cloud bursting dengan sistem file lokal dengan memungkinkan Anda menyalin data dari klien lokal menggunakan atau VPN. AWS Direct Connect

Important

Jika Anda telah menautkan satu atau beberapa sistem file FSx for Lustre ke repositori data di Amazon S3, jangan hapus bucket Amazon S3 hingga Anda menghapus atau memutuskan tautan semua sistem file yang ditautkan.

Dukungan metadata POSIX untuk repositori data

Amazon FSx for Lustre secara otomatis mentransfer metadata Portable Operating System Interface (POSIX) untuk file, direktori, dan tautan simbolis (symlink) saat mengimpor dan mengekspor data ke dan dari repositori data tertaut di Amazon S3. Saat Anda mengekspor perubahan dalam sistem file Anda ke repositori data tertaut, FSx for Lustre juga mengekspor perubahan metadata POSIX sebagai metadata objek S3. Ini berarti bahwa jika sistem file FSx for Lustre lain mengimpor file yang sama dari S3, file akan memiliki metadata POSIX yang sama dalam sistem file itu, termasuk kepemilikan dan izin.

FSx for Lustre hanya mengimpor objek S3 yang memiliki kunci objek yang sesuai dengan POSIX, seperti berikut ini.

```
mydir/  
mydir/myfile1  
mydir/mysubdir/  
mydir/mysubdir/myfile2.txt
```

FSx for Lustre menyimpan direktori dan symlink sebagai objek terpisah dalam repositori data tertaut pada S3. Untuk direktori, FSx for Lustre membuat objek S3 dengan nama kunci yang diakhiri dengan garis miring ("/"), sebagai berikut:

- Kunci objek S3 `mydir/` memetakan ke direktori FSx for Lustre. `mydir/`
- Kunci objek S3 `mydir/mysubdir/` memetakan ke direktori FSx for Lustre. `mydir/mysubdir/`

Untuk symlink, FSx for Lustre menggunakan skema Amazon S3 berikut:

- Kunci objek S3 - Jalur ke tautan, relatif terhadap direktori pemasangan FSx for Lustre
- Data objek S3 - Jalur target symlink ini
- Metadata objek S3 — Metadata untuk symlink

FSx for Lustre menyimpan metadata POSIX, termasuk kepemilikan, izin, dan stempel waktu untuk file, direktori, dan tautan simbolik, dalam objek S3 sebagai berikut:

- `Content-Type` header entitas HTTP yang digunakan untuk menunjukkan jenis media sumber daya untuk browser web.
- `x-amz-meta-file-permissions`— Jenis file dan izin dalam format `<octal file type><octal permission mask>`, konsisten dengan `st_mode` di [halaman manual stat Linux \(2\)](#).

Note

FSx for Lustre tidak mengimpor atau menyimpan informasi. `setuid`

- `x-amz-meta-file-owner`— User ID pemilik (UID) dinyatakan sebagai integer.
- `x-amz-meta-file-groupID` grup (GID) dinyatakan sebagai integer.

- `x-amz-meta-file-atime`— Waktu terakhir yang diakses dalam nanodetik sejak awal zaman Unix. Hentikan nilai waktu dengannya; jika tidak FSx for Lustre menafsirkan nilai sebagai milidetik.
- `x-amz-meta-file-mtime`— Waktu terakhir yang dimodifikasi dalam nanodetik sejak awal zaman Unix. Hentikan nilai waktu dengannya; jika tidak, FSx for Lustre menafsirkan nilai sebagai milidetik.
- `x-amz-meta-user-agent`— Agen pengguna, diabaikan selama FSx for Lustre impor. Selama ekspor, FSx for Lustre menetapkan nilai ini ke `aws-fsx-lustre`

Saat mengimpor objek dari S3 yang tidak memiliki izin POSIX terkait, izin POSIX default yang diberikan FSx for Lustre ke file adalah `755`. Izin ini memungkinkan akses baca dan eksekusi untuk semua pengguna dan akses tulis untuk pemilik file.

Note

FSx for Lustre tidak mempertahankan metadata kustom yang ditentukan pengguna pada objek S3.

Tautan keras dan mengekspor ke S3

Jika ekspor otomatis (dengan kebijakan `BARU` dan `CHANGED`) diaktifkan pada DRA di sistem file Anda, setiap hard link yang terkandung dalam DRA diekspor ke Amazon S3 sebagai objek S3 terpisah untuk setiap hard link. Jika file dengan beberapa hard link dimodifikasi pada sistem file, semua salinan di S3 diperbarui, terlepas dari hard link mana yang digunakan saat mengubah file.

Jika hard link diekspor ke S3 menggunakan tugas repositori data (DRT), setiap hard link yang terkandung dalam jalur yang ditentukan untuk DRT diekspor ke S3 sebagai objek S3 terpisah untuk setiap hard link. Jika file dengan beberapa hard link dimodifikasi pada sistem file, setiap salinan di S3 diperbarui pada saat hard link masing-masing diekspor, terlepas dari hard link mana yang digunakan saat mengubah file.

Important

Ketika sistem file FSx for Lustre baru ditautkan ke bucket S3 di mana hard link sebelumnya diekspor oleh sistem file FSx for Lustre lain, atau Amazon FSx AWS DataSync File Gateway, hard link kemudian diimpor sebagai file terpisah pada sistem file baru.

Tautan keras dan file yang dirilis

File yang dirilis adalah file yang metadatanya ada dalam sistem file, tetapi isinya hanya disimpan di S3. Untuk informasi selengkapnya tentang file yang dirilis, lihat [Melepaskan file](#).

Important

Penggunaan hard link dalam sistem file yang memiliki asosiasi repositori data (DRA) tunduk pada batasan berikut:

- Menghapus dan membuat ulang file yang dirilis yang memiliki beberapa tautan keras dapat menyebabkan konten semua tautan keras ditimpa.
- Menghapus file yang dirilis akan menghapus konten dari semua tautan keras yang berada di luar asosiasi repositori data.
- Membuat hard link ke file yang dirilis yang objek S3 yang sesuai ada di salah satu kelas penyimpanan S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive tidak akan membuat objek baru di S3 untuk hard link.

Panduan: Melampirkan izin POSIX saat mengunggah objek ke bucket Amazon S3

Prosedur berikut menjalankan proses pengunggahan objek ke Amazon S3 dengan izin POSIX. Melakukan hal ini memungkinkan Anda untuk mengimpor izin POSIX ketika Anda membuat sistem file Amazon FSx yang terkait dengan bucket S3.

Untuk mengunggah objek dengan izin POSIX ke Amazon S3

1. Dari komputer atau mesin lokal Anda, gunakan perintah contoh berikut untuk membuat direktori pengujian (`s3cptestdir`) dan file (`s3cptest.txt`) yang akan diunggah ke bucket S3.

```
$ mkdir s3cptestdir
$ echo "S3cp metadata import test" >> s3cptestdir/s3cptest.txt
$ ls -ld s3cptestdir/ s3cptestdir/s3cptest.txt
drwxr-xr-x 3 500 500 96 Jan 8 11:29 s3cptestdir/
-rw-r--r-- 1 500 500 26 Jan 8 11:29 s3cptestdir/s3cptest.txt
```

File dan direktori yang baru dibuat memiliki ID pengguna pemilik file (UID) dan ID grup (GID) 500 dan izin seperti yang ditunjukkan pada contoh sebelumnya.

2. Panggil API Amazon S3 untuk membuat direktori `s3cptestdir` dengan izin metadata. Anda harus menentukan nama direktori dengan garis miring (`/`). Untuk informasi tentang metadata POSIX yang didukung, lihat [Dukungan metadata POSIX untuk repositori data](#)

Ganti `bucket_name` dengan nama bucket S3 Anda yang sebenarnya.

```
$ aws s3api put-object --bucket bucket_name --key s3cptestdir/ --metadata '{"user-agent":"aws-fsx-lustre" , \
    "file-atime":"159500292000000000ns" , "file-owner":"500" , "file-permissions":"0100664","file-group":"500" , \
    "file-mtime":"159500292000000000ns"}'
```

3. Verifikasi izin POSIX ditandai ke metadata objek S3.

```
$ aws s3api head-object --bucket bucket_name --key s3cptestdir/
{
  "AcceptRanges": "bytes",
  "LastModified": "Fri, 08 Jan 2021 17:32:27 GMT",
  "ContentLength": 0,
  "ETag": "\"d41d8cd98f00b204e9800998ecf8427e\"",
  "VersionId": "bAlhCoWq7aIEjc3R6Myc6U0b8sHHtJkR",
  "ContentType": "binary/octet-stream",
  "Metadata": {
    "user-agent": "aws-fsx-lustre",
    "file-atime": "159500292000000000ns",
    "file-owner": "500",
    "file-permissions": "0100664",
    "file-group": "500",
    "file-mtime": "159500292000000000ns"
  }
}
```

4. Unggah file uji (yang dibuat pada langkah 1) dari komputer Anda ke bucket S3 dengan izin metadata.

```
$ aws s3 cp s3cptestdir/s3cptest.txt s3://bucket_name/s3cptestdir/s3cptest.txt \
  --metadata '{"user-agent":"aws-fsx-lustre" , "file-atime":"159500292000000000ns" , \
```

```
"file-owner":"500" , "file-permissions":"0100664","file-group":"500" , "file-
mtime":"159500292000000000ns"}
```

5. Verifikasi izin POSIX ditandai metadata objek S3.

```
$ aws s3api head-object --bucket bucket_name --key s3cptestdir/s3cptest.txt
{
  "AcceptRanges": "bytes",
  "LastModified": "Fri, 08 Jan 2021 17:33:35 GMT",
  "ContentLength": 26,
  "ETag": "\"eb33f7e1f44a14a8e2f9475ae3fc45d3\"",
  "VersionId": "w9ztRoEhB832m8NC3a_JTlTyIx7Uzql6",
  "ContentType": "text/plain",
  "Metadata": {
    "user-agent": "aws-fsx-lustre",
    "file-atime": "159500292000000000ns",
    "file-owner": "500",
    "file-permissions": "0100664",
    "file-group": "500",
    "file-mtime": "159500292000000000ns"
  }
}
```

6. Verifikasi izin pada sistem file Amazon FSx yang terhubung ke bucket S3.

```
$ sudo lfs df -h /fsx
UUID                               bytes      Used    Available Use% Mounted on
3rxnfbmv-MDT0000_UUID              34.4G     6.1M    34.4G    0% /fsx[MDT:0]
3rxnfbmv-OST0000_UUID              1.1T     4.5M    1.1T    0% /fsx[OST:0]

filesystem_summary:                1.1T     4.5M    1.1T    0% /fsx

$ cd /fsx/s3cptestdir/
$ ls -ld s3cptestdir/
drw-rw-r-- 2 500 500 25600 Jan  8 17:33 s3cptestdir/

$ ls -ld s3cptestdir/s3cptest.txt
-rw-rw-r-- 1 500 500 26 Jan 8 17:33 s3cptestdir/s3cptest.txt
```

Baik `s3cptestdir` direktori dan `s3cptest.txt` file memiliki izin POSIX yang diimpor.

Menautkan sistem file Anda ke bucket S3

Anda dapat menautkan sistem file Amazon FSx for Lustre ke repositori data di Amazon S3. Anda dapat membuat tautan saat membuat sistem file atau kapan saja setelah sistem file dibuat.

Tautan antara direktori pada sistem file dan bucket atau awalan S3 disebut data repository association (DRA). Anda dapat mengonfigurasi maksimal 8 asosiasi repositori data pada sistem file FSx for Lustre. Maksimal 8 permintaan DRA dapat diantrian, tetapi hanya satu permintaan yang dapat dikerjakan pada satu waktu untuk sistem file. Setiap DRA harus memiliki direktori sistem file FSx for Lustre yang unik dan bucket atau awalan S3 unik yang terkait dengannya.

Note

Asosiasi repositori data, ekspor otomatis, dan dukungan untuk beberapa repositori data tidak tersedia di FSx for Lustre 2.10 sistem file atau sistem file. Scratch 1

Untuk mengakses objek pada repositori data S3 sebagai file dan direktori pada sistem file, metadata file dan direktori harus dimuat ke dalam sistem file. Anda dapat memuat metadata dari repositori data tertaut saat Anda membuat DRA atau memuat metadata untuk kumpulan file dan direktori yang ingin Anda akses menggunakan sistem file FSx for Lustre di lain waktu menggunakan tugas repositori data impor, atau menggunakan ekspor otomatis untuk memuat metadata secara otomatis ketika objek ditambahkan, diubah, atau dihapus dari repositori data.

Anda dapat mengonfigurasi DRA hanya untuk impor otomatis, hanya untuk ekspor otomatis, atau untuk keduanya. Asosiasi repositori data yang dikonfigurasi dengan impor otomatis dan ekspor otomatis menyebarkan data di kedua arah antara sistem file dan bucket S3 yang ditautkan. Saat Anda membuat perubahan pada data di repositori data S3 Anda, FSx for Lustre mendeteksi perubahan dan kemudian secara otomatis mengimpor perubahan ke sistem file Anda. Saat Anda membuat, memodifikasi, atau menghapus file, FSx for Lustre secara otomatis mengeksport perubahan ke Amazon S3 secara asinkron setelah aplikasi Anda selesai memodifikasi file.

Important

- Jika Anda memodifikasi file yang sama di sistem file dan bucket S3, Anda harus memastikan koordinasi tingkat aplikasi untuk mencegah konflik. FSx for Lustre tidak mencegah penulisan yang bertentangan di beberapa lokasi.

- Untuk file yang ditandai dengan atribut yang tidak dapat diubah, FSx for Lustre tidak dapat menyinkronkan perubahan antara sistem file FSx for Lustre dan bucket S3 yang ditautkan ke sistem file. Menyetel flag yang tidak dapat diubah untuk jangka waktu yang lama dapat menyebabkan kinerja pergerakan data antara Amazon FSx dan S3 menurun.

Saat Anda membuat asosiasi repositori data, Anda dapat mengonfigurasi properti berikut:

- Jalur sistem file — Masukkan jalur lokal pada sistem file yang menunjuk ke direktori (seperti `/ns1/`) atau subdirektori (seperti `/ns1/subdir/`) yang akan dipetakan one-to-one dengan jalur repositori data yang ditentukan di bawah ini. Garis miring ke depan dalam nama diperlukan. Dua asosiasi repositori data tidak dapat memiliki jalur sistem file yang tumpang tindih. Misalnya, jika repositori data dikaitkan dengan jalur sistem file `/ns1`, maka Anda tidak dapat menautkan repositori data lain dengan jalur sistem file `/ns1/ns2`

Note

Jika Anda hanya menentukan garis miring (`/`) sebagai jalur sistem file, Anda hanya dapat menautkan satu repositori data ke sistem file. Anda hanya dapat menentukan `/` sebagai jalur sistem file untuk repositori data pertama yang terkait dengan sistem file.

- Jalur repositori data - Masukkan jalur di repositori data S3. Path dapat berupa bucket S3 atau awalan dalam format `s3://myBucket/myPrefix/`. Properti ini menentukan di mana dalam file repositori data S3 akan diimpor dari atau diekspor ke. FSx for Lustre akan menambahkan trailing `/` ke jalur repositori data Anda jika Anda tidak menyediakannya. Misalnya, jika Anda menyediakan jalur repositori data `s3://myBucket/myPrefix`, FSx for Lustre akan menafsirkannya sebagai `s3://myBucket/myPrefix/`

Dua asosiasi repositori data tidak dapat memiliki jalur repositori data yang tumpang tindih.

Misalnya, jika repositori data dengan jalur `s3://myBucket/myPrefix/` ditautkan ke sistem file, maka Anda tidak dapat membuat asosiasi repositori data lain dengan jalur repositori data `s3://myBucket/myPrefix/mySubPrefix`

- Impor metadata dari repositori — Anda dapat memilih opsi ini untuk mengimpor metadata dari seluruh repositori data segera setelah membuat asosiasi repositori data. Atau, Anda dapat menjalankan tugas repositori data impor untuk memuat semua atau subset metadata dari repositori data tertaut ke dalam sistem file kapan saja setelah asosiasi repositori data dibuat.

- Pengaturan impor — Pilih kebijakan impor yang menentukan jenis objek yang diperbarui (kombinasi apa pun yang baru, diubah, dan dihapus) yang akan secara otomatis diimpor dari bucket S3 yang ditautkan ke sistem file Anda. Impor otomatis (baru, diubah, dihapus) diaktifkan secara default saat Anda menambahkan repositori data dari konsol, tetapi dinonaktifkan secara default saat menggunakan atau AWS CLI Amazon FSx API.
- Pengaturan ekspor — Pilih kebijakan ekspor yang menentukan jenis objek yang diperbarui (kombinasi apa pun yang baru, diubah, dan dihapus) yang akan secara otomatis diekspor ke bucket S3. Ekspor otomatis (baru, diubah, dihapus) diaktifkan secara default saat Anda menambahkan repositori data dari konsol, tetapi dinonaktifkan secara default saat menggunakan atau AWS CLI Amazon FSx API.

Jalur sistem File dan pengaturan jalur repositori Data menyediakan pemetaan 1:1 antara jalur di Amazon FSx dan kunci objek di S3.

Dukungan wilayah dan akun untuk bucket S3 yang ditautkan

Saat Anda membuat tautan ke bucket S3, ingatlah batasan dukungan Wilayah dan akun berikut:

- Ekspor otomatis mendukung konfigurasi lintas wilayah. Sistem file Amazon FSx dan bucket S3 yang ditautkan dapat ditemukan di tempat yang sama Wilayah AWS atau berbeda. Wilayah AWS
- Impor otomatis tidak mendukung konfigurasi lintas wilayah. Baik sistem file Amazon FSx dan bucket S3 yang ditautkan harus berada di tempat yang sama. Wilayah AWS
- Baik ekspor otomatis dan impor otomatis mendukung konfigurasi lintas akun. Sistem file Amazon FSx dan bucket S3 yang ditautkan dapat milik yang sama Akun AWS atau berbeda. Akun AWS

Membuat tautan ke bucket S3

Prosedur berikut memandu Anda melalui proses pembuatan asosiasi repositori data untuk sistem file FSx for Lustre ke bucket S3 yang ada, menggunakan dan (). AWS Management Console AWS Command Line Interface AWS CLI Untuk informasi tentang menambahkan izin ke bucket S3 untuk menautkannya ke sistem file Anda, lihat. [Menambahkan izin untuk menggunakan repositori data di Amazon S3](#)

Note

Repositori data tidak dapat ditautkan ke sistem file yang memiliki cadangan sistem file yang diaktifkan. Nonaktifkan cadangan sebelum menautkan ke repositori data.

Untuk menautkan bucket S3 saat membuat sistem file (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Ikuti prosedur untuk membuat sistem file baru yang dijelaskan di [Buat sistem file FSx for Lustre Anda](#) pada bagian Mulai.
3. Buka Impor/Ekspor Repositori Data - bagian opsional. Fitur ini dinonaktifkan secara default.
4. Pilih Impor data dari dan ekspor data ke S3.
5. Dalam dialog Informasi asosiasi repositori data, berikan informasi untuk bidang berikut.
 - Jalur sistem file: Masukkan nama direktori tingkat tinggi (seperti/ns1) atau subdirektori (seperti/ns1/subdir) dalam sistem file Amazon FSx yang akan dikaitkan dengan repositori data S3. Diperlukan garis miring ke depan di jalan. Dua asosiasi repositori data tidak dapat memiliki jalur sistem file yang tumpang tindih. Misalnya, jika repositori data dikaitkan dengan jalur sistem file/ns1, maka Anda tidak dapat menautkan repositori data lain dengan jalur sistem file. /ns1/ns2 Pengaturan jalur sistem File harus unik di semua asosiasi repositori data untuk sistem file.
 - Jalur repositori data: Masukkan jalur bucket atau awalan S3 yang ada untuk diasosiasikan dengan sistem file Anda (misalnya, s3://my-bucket/my-prefix/ Dua asosiasi repositori data tidak dapat memiliki jalur repositori data yang tumpang tindih. Misalnya, jika repositori data dengan jalur s3://myBucket/myPrefix/ ditautkan ke sistem file, maka Anda tidak dapat membuat asosiasi repositori data lain dengan jalur repositori data. s3://myBucket/myPrefix/mySubPrefix Pengaturan jalur repositori data harus unik di semua asosiasi repositori data untuk sistem file.
 - Impor metadata dari repositori: Pilih properti ini untuk menjalankan tugas repositori data impor secara opsional untuk mengimpor metadata segera setelah tautan dibuat.

Data repository association information

File system path [Info](#)

The path on the file system to be associated with this data repository

Data repository path [Info](#)

The name of the S3 bucket or an S3 prefix to be associated with this file system

Import metadata from repository - optional [Info](#)

6. Untuk pengaturan Impor - opsional, setel Kebijakan Impor yang menentukan bagaimana file dan daftar direktori Anda tetap up to date saat Anda menambahkan, mengubah, atau menghapus objek di bucket S3 Anda. Misalnya, pilih Baru untuk mengimpor metadata ke sistem file Anda untuk objek baru yang dibuat di bucket S3. Untuk informasi selengkapnya tentang kebijakan impor, lihat [Secara otomatis mengimpor pembaruan dari bucket S3](#).

Import settings - optional

In this section you can configure how updates to the data repository are imported into the file system.

Import policy [Info](#) Deselect all

Choose which updates on the data repository should be propagated to the file system

New

Import metadata as new files are added to the repository

Changed

Update file metadata and invalidate existing file content on the file system as files change in the repository

Deleted

Delete files on the file system as corresponding files are deleted in the repository

7. Untuk kebijakan Ekspor, tetapkan kebijakan ekspor yang menentukan cara file Anda diekspor ke bucket S3 terkait saat menambahkan, mengubah, atau menghapus objek di sistem file. Misalnya, pilih Diubah untuk mengekspor objek yang konten atau metadatanya telah diubah

pada sistem file Anda. Untuk informasi selengkapnya tentang kebijakan ekspor, lihat [Ekspor pembaruan ke bucket S3 Anda secara otomatis](#).

Export settings - optional
In this section, you can configure how updates to the file system are exported to the data repository.

Export policy [Info](#) Deselect all
Choose which updates on the file system should be propagated to the data repository

New
Export new files and directories to the repository as they are added to the file system

Changed
Export changes to files and directories on the file system to the repository

Deleted
Delete files and directories on the data repository when they are deleted from the file system

8. Lanjutkan dengan bagian berikutnya dari wizard pembuatan sistem file.

Untuk menautkan bucket S3 ke sistem file yang ada (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Dari dasbor, pilih Sistem file dan kemudian pilih sistem file yang ingin Anda buat asosiasi repositori data.
3. Pilih tab Repositori data.
4. Di panel Asosiasi repositori data, pilih Buat asosiasi repositori data.
5. Dalam dialog Informasi asosiasi repositori data, berikan informasi untuk bidang berikut.
 - Jalur sistem file: Masukkan nama direktori tingkat tinggi (seperti/ns1) atau subdirektori (seperti/ns1/subdir) dalam sistem file Amazon FSx yang akan dikaitkan dengan repositori data S3. Diperlukan garis miring ke depan di jalan. Dua asosiasi repositori data tidak dapat memiliki jalur sistem file yang tumpang tindih. Misalnya, jika repositori data dikaitkan dengan jalur sistem file/ns1, maka Anda tidak dapat menautkan repositori data lain dengan jalur sistem file. /ns1/ns2 Pengaturan jalur sistem File harus unik di semua asosiasi repositori data untuk sistem file.

- Jalur repositori data: Masukkan jalur bucket atau awalan S3 yang ada untuk diasosiasikan dengan sistem file Anda (misalnya, `s3://my-bucket/my-prefix/`). Dua asosiasi repositori data tidak dapat memiliki jalur repositori data yang tumpang tindih. Misalnya, jika repositori data dengan jalur `s3://myBucket/myPrefix/` ditautkan ke sistem file, maka Anda tidak dapat membuat asosiasi repositori data lain dengan jalur repositori data. `s3://myBucket/myPrefix/mySubPrefix` Pengaturan jalur repositori data harus unik di semua asosiasi repositori data untuk sistem file.
- Impor metadata dari repositori: Pilih properti ini untuk menjalankan tugas repositori data impor secara opsional untuk mengimpor metadata segera setelah tautan dibuat.

Create data repository association

Link a data repository to your file system

Data repository association information

File system path [Info](#)

The path on the file system to be associated with this data repository

Data repository path [Info](#)

The name of the S3 bucket or an S3 prefix to be associated with this file system

Import metadata from repository - optional [Info](#)

6. Untuk pengaturan Impor - opsional, setel Kebijakan Impor yang menentukan bagaimana file dan daftar direktori Anda tetap up to date saat Anda menambahkan, mengubah, atau menghapus objek di bucket S3 Anda. Misalnya, pilih Baru untuk mengimpor metadata ke sistem file Anda untuk objek baru yang dibuat di bucket S3. Untuk informasi selengkapnya tentang kebijakan impor, lihat [Secara otomatis mengimpor pembaruan dari bucket S3](#).

Import settings - optional
In this section you can configure how updates to the data repository are imported into the file system.

Import policy [Info](#) Deselect all

Choose which updates on the data repository should be propagated to the file system

New

Import metadata as new files are added to the repository

Changed

Update file metadata and invalidate existing file content on the file system as files change in the repository

Deleted

Delete files on the file system as corresponding files are deleted in the repository

7. Untuk kebijakan Ekspor, tetapkan kebijakan ekspor yang menentukan cara file Anda diekspor ke bucket S3 tertaut saat menambahkan, mengubah, atau menghapus objek di sistem file. Misalnya, pilih Diubah untuk mengekspor objek yang konten atau metadatanya telah diubah pada sistem file Anda. Untuk informasi selengkapnya tentang kebijakan ekspor, lihat [Ekspor pembaruan ke bucket S3 Anda secara otomatis](#).

Export settings - optional
In this section, you can configure how updates to the file system are exported to the data repository.

Export policy [Info](#) Deselect all

Choose which updates on the file system should be propagated to the data repository

New

Export new files and directories to the repository as they are added to the file system

Changed

Export changes to files and directories on the file system to the repository

Deleted

Delete files and directories on the data repository when they are deleted from the file system

8. Pilih Buat.

Untuk menautkan sistem file ke bucket S3 (AWS CLI)

Contoh berikut membuat asosiasi repositori data yang menautkan sistem file Amazon FSx ke bucket S3, dengan kebijakan impor yang mengimpor file baru atau yang diubah ke sistem file dan kebijakan ekspor yang mengekspor file baru, diubah, atau dihapus ke bucket S3 yang ditautkan.

- Untuk membuat asosiasi repositori data, gunakan perintah Amazon FSx CLI, seperti yang ditunjukkan berikut. `create-data-repository-association`

```
$ aws fsx create-data-repository-association \  
  --file-system-id fs-0123456789abcdef0 \  
  --file-system-path /ns1/path1/ \  
  --data-repository-path s3://mybucket/myprefix/ \  
  --s3  
  "AutoImportPolicy={Events=[NEW,CHANGED,DELETED]},AutoExportPolicy={Events=[NEW,CHANGED,DEL
```

Amazon FSx segera mengembalikan deskripsi JSON tentang DRA. DRA dibuat secara asinkron.

Anda dapat menggunakan perintah ini untuk membuat asosiasi repositori data bahkan sebelum sistem file selesai dibuat. Permintaan akan antri dan asosiasi repositori data akan dibuat setelah sistem file tersedia.

Memperbarui pengaturan asosiasi repositori data

Anda dapat memperbarui pengaturan asosiasi repositori data yang ada menggunakan AWS Management Console, API AWS CLI, dan Amazon fsX, seperti yang ditunjukkan dalam prosedur berikut.

Note

Anda tidak dapat memperbarui File system path atau Data repository path dari DRA setelah dibuat. Jika Anda ingin mengubah File system path atau Data repository path, Anda harus menghapus DRA dan membuatnya lagi.

Untuk memperbarui pengaturan untuk asosiasi repositori data yang ada (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Dari dasbor, pilih Sistem file, lalu pilih sistem file yang ingin Anda kelola.
3. Pilih tab Repositori data.
4. Di panel Asosiasi repositori data, pilih asosiasi repositori data yang ingin Anda ubah.
5. Pilih Perbarui. Dialog edit ditampilkan untuk asosiasi repositori data.
6. Untuk pengaturan Impor - opsional, Anda dapat memperbarui Kebijakan Impor Anda. Untuk informasi selengkapnya tentang kebijakan impor, lihat [Secara otomatis mengimpor pembaruan dari bucket S3](#).

7. Untuk pengaturan Ekspor - opsional, Anda dapat memperbarui kebijakan ekspor Anda. Untuk informasi selengkapnya tentang kebijakan ekspor, lihat [Ekspor pembaruan ke bucket S3 Anda secara otomatis](#).
8. Pilih Perbarui.

Untuk memperbarui pengaturan untuk asosiasi repositori data (CLI) yang ada

- Untuk memperbarui asosiasi repositori data, gunakan perintah Amazon FSx CLI, seperti yang ditunjukkan berikut. `update-data-repository-association`

```
$ aws fsx update-data-repository-association \
  --association-id 'dra-872abab4b4503bfc2' \
  --s3
  "AutoImportPolicy={Events=[NEW,CHANGED,DELETED]},AutoExportPolicy={Events=[NEW,CHANGED,DEL
```

Setelah berhasil memperbarui kebijakan impor dan ekspor asosiasi repositori data, Amazon FSx mengembalikan deskripsi asosiasi repositori data yang diperbarui sebagai JSON.

Menghapus asosiasi ke bucket S3

Prosedur berikut memandu Anda melalui proses menghapus asosiasi repositori data dari sistem file Amazon FSx yang ada ke bucket S3 yang ada, menggunakan dan (). AWS Management Console AWS Command Line Interface AWS CLI Menghapus asosiasi repositori data memutuskan tautan sistem file dari bucket S3.

Untuk menghapus tautan dari sistem file ke bucket S3 (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Dari dasbor, pilih Sistem file dan kemudian pilih sistem file yang ingin Anda hapus asosiasi repositori data.
3. Pilih tab Repositori data.
4. Di panel Asosiasi repositori data, pilih asosiasi repositori data yang ingin Anda hapus.
5. Untuk Tindakan, pilih Hapus asosiasi.
6. (Opsional) Dalam Hapus dialog, Anda dapat memilih Hapus data dalam sistem file untuk menghapus data secara fisik dalam sistem file yang sesuai dengan asosiasi repositori data.
7. Pilih Hapus untuk menghapus asosiasi repositori data dari sistem file.

Untuk menghapus tautan dari sistem file ke bucket S3 ()AWS CLI

Contoh berikut menghapus asosiasi repositori data yang menautkan sistem file Amazon FSx ke bucket S3. `--association-id` Parameter menentukan ID asosiasi repositori data yang akan dihapus.

- Untuk menghapus asosiasi repositori data, gunakan perintah Amazon FSx CLI, seperti yang ditunjukkan berikut. `delete-data-repository-association`

```
$ aws fsx delete-data-repository-association \  
    --association-id dra-872abab4b4503bfc \  
    --delete-data-in-file-system false
```

Setelah berhasil menghapus asosiasi repositori data, Amazon FSx mengembalikan deskripsinya sebagai JSON.

Melihat detail asosiasi repositori data

Anda dapat melihat detail asosiasi repositori data menggunakan konsol FSx for Lustre, the, dan API. AWS CLI Rinciannya termasuk ID asosiasi DRA, jalur sistem file, jalur repositori data, pengaturan impor, pengaturan ekspor, status, dan ID sistem file terkait.

Untuk melihat detail DRA (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Dari dasbor, pilih Sistem file dan kemudian pilih sistem file yang ingin Anda lihat detail asosiasi repositori data.
3. Pilih tab Repositori data.
4. Di panel Asosiasi repositori data, pilih asosiasi repositori data yang ingin Anda lihat. Halaman Ringkasan muncul, menampilkan detail DRA.

dra-05e0aa72d9374ec21
Update

Summary

Association id dra-05e0aa72d9374ec21	File system path /fs2	Status Creating
File system id fs-02217d7be6c80a4e2	Data repository path s3://test/path/	

Import | Export

Import settings

Import policy
Choose which event changes should cause your file system to get an update from the connected data repository

<p>New <input checked="" type="checkbox"/></p> <p>Import metadata as new files are added to the repository</p>	<p>Changed <input checked="" type="checkbox"/></p> <p>Update file metadata and invalidate existing file content on the file system as files change in the repository</p>	<p>Deleted <input checked="" type="checkbox"/></p> <p>Delete files on the file system as corresponding files are deleted in the repository</p>
---	---	---

Untuk melihat detail DRA (CLI)

- Untuk melihat detail asosiasi repositori data tertentu, gunakan perintah Amazon FSx CLI, seperti yang ditunjukkan berikut. `describe-data-repository-associations`

```
$ aws fsx describe-data-repository-associations \
  --association-ids dra-872abab4b4503bfc2
```

Amazon FSx mengembalikan deskripsi asosiasi repositori data sebagai JSON.

Status siklus hidup asosiasi repositori data

Status siklus hidup asosiasi repositori data memberikan informasi status tentang DRA tertentu. Asosiasi repositori data dapat memiliki status Siklus Hidup berikut:

- **Membuat** - Amazon FSx membuat asosiasi repositori data antara sistem file dan repositori data tertaut. Repositori data tidak tersedia.
- **Tersedia** - Asosiasi repositori data tersedia untuk digunakan.
- **Memperbarui** - Asosiasi repositori data sedang menjalani pembaruan yang dimulai pelanggan yang dapat memengaruhi ketersediaannya.
- **Menghapus** - Asosiasi repositori data sedang mengalami penghapusan yang dimulai oleh pelanggan.

- Salah konfigurasi - Amazon FSx tidak dapat secara otomatis mengimpor pembaruan dari bucket S3 atau secara otomatis mengeksport pembaruan ke bucket S3 hingga konfigurasi asosiasi repositori data diperbaiki.
- Gagal - Asosiasi repositori data berada dalam status terminal yang tidak dapat dipulihkan (misalnya, karena jalur sistem filenya dihapus atau bucket S3 dihapus).

Anda dapat melihat status siklus hidup asosiasi repositori data menggunakan konsol Amazon FSx, API Amazon FSx, dan AWS Command Line Interface Amazon FSx. Untuk informasi selengkapnya, lihat [Melihat detail asosiasi repositori data](#).

Bekerja dengan bucket Amazon S3 yang dienkripsi sisi server

FSx for Lustre mendukung bucket Amazon S3 yang menggunakan enkripsi sisi server dengan kunci yang dikelola S3 (SSE-S3), dan dengan disimpan di (SSE-KMS). AWS KMS keys AWS Key Management Service

Jika Anda ingin Amazon FSx mengenkripsi data saat menulis ke bucket S3 Anda, Anda perlu mengatur enkripsi default pada bucket S3 Anda ke SSE-S3 atau SSE-KMS. Untuk informasi selengkapnya, lihat [Mengonfigurasi enkripsi default](#) di Panduan Pengguna Amazon S3. Saat menulis file ke bucket S3 Anda, Amazon FSx mengikuti kebijakan enkripsi default bucket S3 Anda.

Secara default, Amazon FSx mendukung bucket S3 yang dienkripsi menggunakan SSE-S3. Jika Anda ingin menautkan sistem file Amazon FSx ke bucket S3 yang dienkripsi menggunakan enkripsi SSE-KMS, Anda perlu menambahkan pernyataan ke kebijakan kunci terkelola pelanggan yang memungkinkan Amazon FSx mengenkripsi dan mendekripsi objek di bucket S3 menggunakan kunci KMS Anda.

Pernyataan berikut memungkinkan sistem file Amazon FSx tertentu untuk mengenkripsi dan mendekripsi objek untuk bucket S3 tertentu, *bucket_name*.

```
{
  "Sid": "Allow access through S3 for the FSx SLR to use the KMS key on the objects
in the given S3 bucket",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::aws_account_id:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fsx_file_system_id"
  },
  "Action": [
```

```

    "kms:Encrypt",
    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:CallerAccount": "aws_account_id",
      "kms:ViaService": "s3.bucket-region.amazonaws.com"
    },
    "StringLike": {
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
    }
  }
}

```

Note

Jika Anda menggunakan KMS dengan CMK untuk mengenkripsi bucket S3 Anda dengan kunci bucket S3 diaktifkan, setel ke EncryptionContext bucket ARN, bukan objek ARN, seperti dalam contoh ini:

```

"StringLike": {
  "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name"
}

```

Pernyataan kebijakan berikut memungkinkan semua sistem file Amazon FSx di akun Anda untuk tertaut ke bucket S3 tertentu.

```

{
  "Sid": "Allow access through S3 for the FSx SLR to use the KMS key on the objects
in the given S3 bucket",
  "Effect": "Allow",
  "Principal": {
    "AWS": "*"
  },
  "Action": [
    "kms:Encrypt",

```

```

    "kms:Decrypt",
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*",
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:CallerAccount": "aws_account_id",
      "kms:ViaService": "s3.bucket-region.amazonaws.com"
    },
    "StringLike": {
      "aws:userid": "*:FSx",
      "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
    }
  }
}
}

```

Mengakses bucket Amazon S3 terenkripsi sisi server dengan cara yang berbeda Akun AWS

Setelah membuat sistem file FSx for Lustre yang ditautkan ke bucket Amazon S3 terenkripsi, Anda harus `AWSServiceRoleForFSxS3Access_fs-01234567890` memberikan akses peran terkait layanan (SLR) ke kunci KMS yang digunakan untuk mengenkripsi bucket S3 sebelum membaca atau menulis data dari bucket S3 yang ditautkan. Anda dapat menggunakan peran IAM yang sudah memiliki izin ke kunci KMS.

Note

Peran IAM ini harus ada di akun tempat sistem file FSx for Lustre dibuat (yang merupakan akun yang sama dengan S3 SLR), bukan akun tempat kunci KMS/ember S3 milik.

Anda menggunakan peran IAM untuk memanggil AWS KMS API berikut untuk membuat hibah untuk SLR S3 sehingga SLR mendapatkan izin ke objek S3. Untuk menemukan ARN yang terkait dengan SLR Anda, cari peran IAM Anda menggunakan ID sistem file Anda sebagai string pencarian.

```

$ aws kms create-grant --region fs_account_region \
  --key-id arn:aws:kms:s3_bucket_account_region:s3_bucket_account:key/key_id \
  --grantee-principal arn:aws:iam::fs_account_id:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_file-system-id \

```

```
--operations "Decrypt" "Encrypt" "GenerateDataKey"  
"GenerateDataKeyWithoutPlaintext" "CreateGrant" "DescribeKey" "ReEncryptFrom"  
"ReEncryptTo"
```

Untuk mengetahui informasi selengkapnya tentang peran terkait layanan, lihat [Menggunakan peran terkait layanan untuk Amazon FSx](#).

Mengimpor perubahan dari repositori data

Anda dapat mengimpor perubahan pada data dan metadata POSIX dari repositori data tertaut ke sistem file Amazon FSx Anda. Metadata POSIX terkait mencakup kepemilikan, izin, dan stempel waktu.

Untuk mengimpor perubahan ke sistem file, gunakan salah satu metode berikut:

- Konfigurasi sistem file Anda untuk secara otomatis mengimpor file baru, diubah, atau dihapus dari repositori data tertaut Anda. Untuk informasi selengkapnya, lihat [Secara otomatis mengimpor pembaruan dari bucket S3](#).
- Pilih opsi untuk mengimpor metadata saat Anda membuat asosiasi repositori data. Ini akan memulai tugas repositori data impor segera setelah membuat asosiasi repositori data.
- Gunakan tugas repositori data impor sesuai permintaan. Untuk informasi selengkapnya, lihat [Menggunakan tugas repositori data untuk mengimpor perubahan](#).

Tugas repositori data impor dan impor otomatis dapat berjalan pada saat yang bersamaan.

Saat Anda mengaktifkan impor otomatis untuk asosiasi repositori data, sistem file Anda secara otomatis memperbarui metadata file saat objek dibuat, dimodifikasi, atau dihapus di S3. Ketika Anda memilih opsi untuk mengimpor metadata saat membuat asosiasi repositori data, sistem file Anda mengimpor metadata untuk semua objek dalam repositori data. Saat Anda mengimpor menggunakan tugas repositori data impor, sistem file Anda hanya mengimpor metadata untuk objek yang dibuat atau dimodifikasi sejak impor terakhir.

FSx for Lustre secara otomatis menyalin konten file dari repositori data Anda dan memuatnya ke dalam sistem file saat aplikasi Anda pertama kali mengakses file dalam sistem file. Pergerakan data ini dikelola oleh FSx for Lustre dan transparan untuk aplikasi Anda. Pembacaan selanjutnya dari file-file ini disajikan langsung dari sistem file dengan latensi sub-milidetik.

Anda juga dapat memuat seluruh sistem file atau direktori di dalam sistem file Anda. Untuk informasi selengkapnya, lihat [Terlebih dulu memuat file ke dalam sistem file Anda](#). Jika Anda meminta pramuat

beberapa file secara bersamaan, FSx for Lustre memuat file dari repositori data Amazon S3 Anda secara paralel.

FSx for Lustre hanya mengimpor objek S3 yang memiliki kunci objek yang sesuai dengan POSIX. Baik tugas repositori data impor dan impor otomatis mengimpor metadata POSIX. Untuk informasi selengkapnya, lihat [Dukungan metadata POSIX untuk repositori data](#).

Note

FSx for Lustre tidak mendukung pengimporan metadata untuk tautan simbolik (symlink) dari kelas penyimpanan S3 Glacier Flexible Retrieval dan S3 Glacier Deep Archive. Metadata untuk S3 Glacier Flexible Retrieval atau objek S3 Glacier Deep Archive yang bukan symlink dapat diimpor (yaitu, inode dibuat pada sistem file FSx for Lustre dengan metadata yang benar). Namun, untuk membaca data ini dari sistem file, Anda harus terlebih dahulu mengembalikan objek S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive. Mengimpor data file langsung dari objek Amazon S3 di kelas penyimpanan S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive ke FSx for Lustre tidak didukung.

Secara otomatis mengimpor pembaruan dari bucket S3

Anda dapat mengonfigurasi FSx for Lustre untuk memperbarui metadata secara otomatis dalam sistem file saat objek ditambahkan, diubah, atau dihapus dari bucket S3 Anda. FSx for Lustre membuat, memperbarui, atau menghapus daftar file dan direktori, sesuai dengan perubahan di S3. Jika objek yang diubah dalam bucket S3 tidak lagi berisi metadatanya, fsX for Lustre mempertahankan nilai metadata file saat ini, termasuk izin saat ini.

Note

Sistem file FSx for Lustre dan bucket S3 yang ditautkan harus berada di tempat yang sama untuk mengimpor pembaruan secara Wilayah AWS otomatis.

Anda dapat mengonfigurasi impor otomatis saat membuat asosiasi repositori data, dan Anda dapat memperbarui pengaturan impor otomatis kapan saja menggunakan konsol manajemen FSx, API, atau API AWS CLI. AWS

 Note

Anda dapat mengonfigurasi impor otomatis dan ekspor otomatis pada asosiasi repositori data yang sama. Topik ini hanya menjelaskan fitur impor otomatis.

 Important

- Jika objek dimodifikasi di S3 dengan semua kebijakan impor otomatis diaktifkan dan ekspor otomatis dinonaktifkan, konten objek itu selalu diimpor ke file yang sesuai dalam sistem file. Jika file sudah ada di lokasi target, file akan ditimpa.
- Jika file dimodifikasi di sistem file dan S3, dengan semua impor otomatis dan kebijakan ekspor otomatis diaktifkan, baik file dalam sistem file atau objek di S3 dapat ditimpa oleh yang lain. Tidak dijamin bahwa pengeditan nanti di satu lokasi akan menimpa suntingan sebelumnya di lokasi lain. Jika Anda memodifikasi file yang sama di sistem file dan bucket S3, Anda harus memastikan koordinasi tingkat aplikasi untuk mencegah konflik tersebut. FSx for Lustre tidak mencegah penulisan yang bertentangan di beberapa lokasi.

Kebijakan impor menentukan bagaimana Anda ingin FSx for Lustre memperbarui sistem file Anda saat konten berubah di bucket S3 yang ditautkan. Asosiasi repositori data dapat memiliki salah satu kebijakan impor berikut:

- Baru - FSx for Lustre secara otomatis memperbarui metadata file dan direktori hanya ketika objek baru ditambahkan ke repositori data S3 yang ditautkan.
- Berubah - FSx for Lustre secara otomatis memperbarui metadata file dan direktori hanya ketika objek yang ada di repositori data diubah.
- Dihapus - FSx for Lustre secara otomatis memperbarui metadata file dan direktori hanya ketika objek dalam repositori data dihapus.
- Kombinasi apa pun dari Baru, Diubah, dan Dihapus - FSx for Lustre secara otomatis memperbarui metadata file dan direktori ketika salah satu tindakan yang ditentukan terjadi di repositori data S3. Misalnya, Anda dapat menentukan bahwa sistem file diperbarui ketika objek ditambahkan ke (Baru) atau dihapus dari (Dihapus) repositori S3, tetapi tidak diperbarui ketika objek diubah.
- Tidak ada kebijakan yang dikonfigurasi - FSx for Lustre tidak memperbarui metadata file dan direktori pada sistem file saat objek ditambahkan, diubah, atau dihapus dari repositori data S3. Jika Anda tidak mengonfigurasi kebijakan impor, impor otomatis dinonaktifkan untuk asosiasi repositori

data. Anda masih dapat mengimpor perubahan metadata secara manual dengan menggunakan tugas repositori data impor, seperti yang dijelaskan dalam [Menggunakan tugas repositori data untuk mengimpor perubahan](#)

 Important

Impor otomatis tidak akan menyinkronkan tindakan S3 berikut dengan sistem file FSx for Lustre yang ditautkan:

- Menghapus objek menggunakan kedaluwarsa siklus hidup objek S3
- Menghapus versi objek saat ini secara permanen dalam bucket berkemampuan versi
- Membatalkan penghapusan objek dalam bucket berkemampuan versi

Untuk sebagian besar kasus penggunaan, sebaiknya Anda mengonfigurasi kebijakan impor Baru, Diubah, dan Dihapus. Kebijakan ini memastikan bahwa semua pembaruan yang dibuat di repositori data S3 tertaut Anda secara otomatis diimpor ke sistem file Anda.

Saat Anda menetapkan kebijakan impor untuk memperbarui file sistem file dan metadata direktori berdasarkan perubahan dalam repositori data S3 tertaut, FSx for Lustre akan membuat konfigurasi notifikasi peristiwa pada bucket S3 yang ditautkan. Konfigurasi pemberitahuan acara diberi nama FSx. Jangan mengubah atau menghapus konfigurasi pemberitahuan FSx acara pada bucket S3 — hal itu akan mencegah impor otomatis file dan metadata direktori yang diperbarui ke sistem file Anda.

Ketika FSx for Lustre memperbarui daftar file yang telah berubah pada repositori data S3 tertaut, itu menimpa file lokal dengan versi yang diperbarui, bahkan jika file tersebut dikunci tulis.

FSx for Lustre melakukan upaya terbaik untuk memperbarui sistem file Anda. FSx for Lustre tidak dapat memperbarui sistem file dalam situasi berikut:

- Jika FSx for Lustre tidak memiliki izin untuk membuka objek S3 yang diubah atau baru. Dalam hal ini, FSx for Lustre melewati objek dan melanjutkan. Status siklus hidup DRA tidak terpengaruh.
- Jika FSx for Lustre tidak memiliki izin tingkat ember, seperti untuk. `GetBucketAc1` Ini akan menyebabkan status siklus hidup repositori data menjadi Salah konfigurasi. Untuk informasi selengkapnya, lihat [Status siklus hidup asosiasi repositori data](#).
- Jika konfigurasi pemberitahuan acara FSx pada bucket S3 terkait dihapus atau diubah. Ini akan menyebabkan status siklus hidup repositori data menjadi Salah konfigurasi. Untuk informasi selengkapnya, lihat [Status siklus hidup asosiasi repositori data](#).

Kami menyarankan Anda [mengaktifkan CloudWatch log](#) ke Log untuk mencatat informasi tentang file atau direktori apa pun yang tidak dapat diimpor secara otomatis. Peringatan dan kesalahan dalam log berisi informasi tentang alasan kegagalan. Untuk informasi selengkapnya, lihat [Log peristiwa repositori data](#).

Prasyarat

Kondisi berikut diperlukan agar FSx for Lustre mengimpor file baru, diubah, atau dihapus secara otomatis dari bucket S3 yang ditautkan:

- Sistem file dan bucket S3 yang ditautkan terletak di tempat yang sama Wilayah AWS.
- Bucket S3 tidak memiliki status Siklus Hidup yang salah dikonfigurasi. Untuk informasi selengkapnya, lihat [Status siklus hidup asosiasi repositori data](#).
- Akun Anda memiliki izin yang diperlukan untuk mengkonfigurasi dan menerima pemberitahuan acara pada bucket S3 yang tertaut.

Jenis perubahan file yang didukung

FSx for Lustre mendukung pengimporan perubahan berikut ke file dan direktori yang terjadi di bucket S3 yang ditautkan:

- Perubahan pada isi file.
- Perubahan pada metadata file atau direktori.
- Perubahan pada target symlink atau metadata.
- Penghapusan file dan direktori. Jika Anda menghapus objek di bucket S3 tertaut yang sesuai dengan direktori dalam sistem file (yaitu, objek dengan nama kunci yang diakhiri dengan garis miring), FSx for Lustre menghapus direktori yang sesuai pada sistem file hanya jika kosong.

Memperbarui pengaturan impor

Anda dapat menyetel setelah impor sistem file untuk bucket S3 tertaut saat membuat asosiasi repositori data. Untuk informasi selengkapnya, lihat [Membuat tautan ke bucket S3](#).

Anda juga dapat memperbarui pengaturan impor kapan saja, termasuk kebijakan impor. Untuk informasi selengkapnya, lihat [Memperbarui pengaturan asosiasi repositori data](#).

Memantau impor otomatis

Jika laju perubahan dalam bucket S3 Anda melebihi laju impor otomatis dapat memproses perubahan ini, perubahan metadata terkait yang diimpor ke sistem file FSx for Lustre Anda akan tertunda. Jika ini terjadi, Anda dapat menggunakan `AgeOf01destQueuedMessage` metrik untuk memantau usia perubahan tertua yang menunggu untuk diproses oleh impor otomatis. Untuk informasi lebih lanjut tentang metrik ini, lihat [AutoImport dan AutoExport metrik](#).

Jika penundaan dalam mengimpor metadata berubah melebihi 14 hari (yang diukur menggunakan `AgeOf01destQueuedMessage` metrik), perubahan dalam bucket S3 Anda yang belum diproses oleh impor otomatis tidak akan diimpor ke sistem file Anda. Selain itu, siklus hidup asosiasi repositori data Anda ditandai sebagai SALAH KONFIGURASI dan impor otomatis dihentikan. Jika Anda mengaktifkan ekspor otomatis, ekspor otomatis terus memantau sistem file FSx for Lustre Anda untuk perubahan. Namun, perubahan tambahan tidak disinkronkan dari sistem file FSx for Lustre Anda ke S3.

Untuk mengembalikan asosiasi repositori data Anda dari status siklus hidup SALAH KONFIGURASI ke status siklus hidup TERSEDIA, Anda harus memperbarui asosiasi repositori data Anda. Anda dapat memperbarui asosiasi repositori data menggunakan perintah CLI [update-repository-association](#) (atau operasi API terkait). [UpdateDataRepositoryAssociation](#) Satu-satunya parameter permintaan yang Anda butuhkan adalah asosiasi repositori data yang ingin Anda perbarui. `AssociationID`

Setelah status siklus hidup asosiasi repositori data berubah menjadi TERSEDIA, impor otomatis (dan ekspor otomatis jika diaktifkan) dimulai ulang. Setelah memulai ulang, ekspor otomatis melanjutkan sinkronisasi perubahan sistem file ke S3. [Untuk menyinkronkan metadata objek baru dan yang diubah di S3 dengan sistem file FSx for Lustre Anda yang tidak diimpor atau berasal dari saat asosiasi repositori data berada dalam status salah konfigurasi, jalankan tugas repositori data impor.](#) Impor tugas repositori data tidak menyinkronkan penghapusan di bucket S3 Anda dengan sistem file FSx for Lustre Anda. Jika Anda ingin sepenuhnya menyinkronkan S3 dengan sistem file Anda (termasuk penghapusan), Anda harus membuat ulang sistem file Anda.

Untuk memastikan bahwa penundaan mengimpor perubahan metadata tidak melebihi 14 hari, sebaiknya Anda menyetel alarm pada `AgeOf01destQueuedMessage` metrik dan mengurangi aktivitas di bucket S3 jika `AgeOf01destQueuedMessage` metrik tumbuh melampaui ambang batas alarm Anda. Untuk sistem file FSx for Lustre yang terhubung ke bucket S3 dengan pecahan tunggal terus mengirimkan jumlah maksimum kemungkinan perubahan dari S3, dengan hanya impor otomatis yang berjalan pada sistem file FSx for Lustre, impor otomatis dapat memproses backlog 7 jam perubahan S3 dalam 14 hari.

Selain itu, dengan satu tindakan S3, Anda dapat menghasilkan lebih banyak perubahan daripada impor otomatis yang akan diproses dalam 14 hari. Contoh dari jenis tindakan ini termasuk, namun tidak terbatas pada, AWS Snowball upload ke S3 dan penghapusan skala besar. Jika Anda membuat perubahan skala besar pada bucket S3 yang ingin disinkronkan dengan sistem file FSx for Lustre, untuk mencegah perubahan impor otomatis melebihi 14 hari, Anda harus menghapus sistem file Anda dan membuatnya kembali setelah perubahan S3 selesai.

Jika `AgeOfOldestQueuedMessage` metrik Anda bertambah, tinjau `bucketGetRequests`, `PutRequests`, `PostRequests`, dan `DeleteRequests` metrik S3 Anda untuk perubahan aktivitas yang akan menyebabkan peningkatan tarif dan/atau jumlah perubahan yang dikirim ke impor otomatis. Untuk informasi tentang metrik S3 yang tersedia, lihat [Memantau Amazon S3](#) di Panduan Pengguna Amazon S3.

Untuk daftar semua metrik FSx for Lustre yang tersedia, lihat [Pemantauan CloudWatch dengan Amazon](#)

Menggunakan tugas repositori data untuk mengimpor perubahan

Tugas repositori data impor mengimpor metadata objek yang baru atau diubah dalam repositori data S3 Anda, membuat daftar file atau direktori baru untuk objek baru apa pun di repositori data S3. Untuk objek apa pun yang telah diubah dalam repositori data, daftar file atau direktori yang sesuai diperbarui dengan metadata baru. Tidak ada tindakan yang diambil untuk objek yang telah dihapus dari repositori data.

Gunakan prosedur berikut untuk mengimpor perubahan metadata menggunakan konsol Amazon FSx dan CLI. Perhatikan bahwa Anda dapat menggunakan satu tugas repositori data untuk beberapa DRA.

Untuk mengimpor perubahan metadata (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Pada panel navigasi, pilih Sistem file, lalu pilih sistem file Lustre Anda.
3. Pilih tab Repositori data.
4. Di panel Asosiasi repositori data, pilih asosiasi repositori data yang ingin Anda buat tugas impor.
5. Dari menu Tindakan, pilih Impor tugas. Pilihan ini tidak tersedia jika sistem file tidak ditautkan ke repositori data. Halaman tugas Create import data repository muncul.

Create import data repository task ✕

The Import data repository task imports POSIX metadata changes from your linked data repository to the FSx file system.

Data repository paths to import - *optional*

You can enter up to 32 import paths, each on its own line.

Completion report

Enable

Disable

Cancel Create data repository task

- (Opsional) Tentukan hingga 32 direktori atau file yang akan diimpor dari bucket S3 tertaut Anda dengan menyediakan jalur ke direktori atau file tersebut di jalur repositori Data untuk diimpor.

Note

Jika jalan yang Anda berikan tidak valid, tugas gagal.

- (Opsional) Pilih Aktifkan di Laporan penyelesaian untuk membuat laporan penyelesaian tugas setelah tugas selesai. Laporan penyelesaian tugas menyediakan detail tentang file yang diproses oleh tugas yang memenuhi lingkup yang disediakan di Lingkup laporan. Untuk menentukan lokasi Amazon FSx untuk mengirimkan laporan, masukkan jalur relatif pada repositori data S3 tertaut untuk jalur Laporan.
- Pilih Buat.

Pemberitahuan di bagian atas halaman Sistem file menampilkan tugas yang baru saja Anda buat dalam proses.

Untuk melihat status tugas dan detail, gulir ke bawah ke panel Tugas Repositori Data di tab Repositori Data untuk sistem file. Urutan default menampilkan tugas terbaru di bagian atas daftar.

Untuk melihat ringkasan tugas dari halaman ini, pilih ID tugas untuk tugas yang baru saja Anda buat. Halaman Ringkasan untuk tugas muncul.

Untuk mengimpor perubahan metadata (CLI)

- Gunakan perintah [create-data-repository-task](#) CLI untuk mengimpor perubahan metadata pada sistem file FSx for Lustre Anda. Operasi API yang sesuai adalah [CreateDataRepositoryTask](#).

```
$ aws fsx create-data-repository-task \
  --file-system-id fs-0123456789abcdef0 \
  --type IMPORT_METADATA_FROM_REPOSITORY \
  --paths s3://bucketname1/dir1/path1 \
  --report Enabled=true,Path=s3://bucketname1/dir1/
path1,Format=REPORT_CSV_20191124,Scope=FAILED_FILES_ONLY
```

Setelah berhasil membuat tugas repositori data, Amazon FSx mengembalikan deskripsi tugas sebagai JSON.

Setelah membuat tugas untuk mengimpor metadata dari repositori data tertaut, Anda dapat memeriksa status tugas repositori data impor. Untuk informasi selengkapnya tentang melihat tugas repositori data, lihat [Mengakses tugas repositori data](#).

Terlebih dulu memuat file ke dalam sistem file Anda

Amazon FSx menyalin data dari repositori data Amazon S3 Anda saat file pertama kali diakses. Karena pendekatan ini, pembacaan atau penulisan awal ke file menimbulkan sejumlah kecil latensi. Jika aplikasi Anda sensitif terhadap latensi ini, dan Anda tahu file atau direktori mana yang aplikasinya perlu akses, Anda dapat memilih terlebih dulu memuat isi file individu atau direktori. Anda melakukannya dengan menggunakan perintah `hsm_restore`, sebagai berikut.

Anda dapat menggunakan perintah `hsm_action` (yang dikeluarkan dengan utilitas pengguna `lfs`) untuk memverifikasi bahwa isi file telah selesai dimuat ke dalam sistem file. Sebuah nilai kembali `N00P` menunjukkan bahwa file telah berhasil dimuat. Jalankan perintah berikut dari instans komputasi dengan sistem file yang terpasang. Ganti *path/to/file* dengan path file yang Anda preloading ke sistem file Anda.

```
sudo lfs hsm_restore path/to/file  
sudo lfs hsm_action path/to/file
```

Anda dapat terlebih dulu memuat seluruh sistem file Anda atau seluruh direktori dalam sistem file Anda dengan menggunakan perintah berikut. (tanda ampersand yang mengikuti membuat perintah dijalankan sebagai proses latar belakang.) Jika Anda meminta pemuatan awal beberapa file secara bersamaan, Amazon FSx memuat file Anda dari repositori data Amazon S3 secara paralel. Jika file telah dimuat ke sistem file, `hsm_restore` perintah tidak memuat ulang.

```
nohup find local/directory -type f -print0 | xargs -0 -n 1 sudo lfs hsm_restore &
```

Note

Jika bucket S3 tertaut Anda lebih besar dari sistem file Anda, Anda harus dapat mengimpor semua metadata file ke dalam sistem file Anda. Namun, Anda hanya dapat memuat sebanyak data file aktual yang akan muat ke dalam ruang penyimpanan sistem file yang tersisa. Anda akan menerima pesan kesalahan jika mencoba mengakses data file saat tidak ada lagi penyimpanan yang tersisa di sistem file. Jika ini terjadi, Anda dapat meningkatkan jumlah kapasitas penyimpanan sesuai kebutuhan. Untuk informasi selengkapnya, lihat [Mengelola kapasitas penyimpanan](#).

Mengekspor perubahan ke repositori data

Anda dapat mengekspor perubahan data dan perubahan metadata POSIX dari sistem file FSx for Lustre Anda ke repositori data tertaut. Metadata POSIX terkait mencakup kepemilikan, izin, dan stempel waktu.

Untuk mengekspor perubahan dari sistem file, gunakan salah satu metode berikut.

- Konfigurasi sistem file Anda untuk secara otomatis mengekspor file baru, diubah, atau dihapus ke repositori data tertaut Anda. Untuk informasi selengkapnya, lihat [Ekspor pembaruan ke bucket S3 Anda secara otomatis](#).
- Gunakan tugas repositori data ekspor sesuai permintaan. Untuk informasi selengkapnya, lihat [Menggunakan tugas repositori data untuk mengekspor perubahan](#)

Tugas repositori data ekspor dan ekspor otomatis tidak dapat berjalan pada saat yang bersamaan.

⚠ Important

Ekspor otomatis tidak akan menyinkronkan operasi metadata berikut pada sistem file Anda dengan S3 jika objek yang sesuai disimpan di S3 Glacier Flexible Retrieval:

- `chmod`
- `tercekik`
- `ganti nama`

Saat Anda mengaktifkan ekspor otomatis untuk asosiasi repositori data, sistem file Anda secara otomatis mengeksport data file dan perubahan metadata saat file dibuat, dimodifikasi, atau dihapus. Saat Anda mengeksport file atau direktori menggunakan tugas repositori data ekspor, sistem file Anda hanya mengeksport file data dan metadata yang dibuat atau dimodifikasi sejak ekspor terakhir.

Baik tugas repositori data ekspor dan ekspor otomatis mengeksport metadata POSIX. Untuk informasi selengkapnya, lihat [Dukungan metadata POSIX untuk repositori data](#).

⚠ Important

- Untuk memastikan bahwa FSx for Lustre dapat mengeksport data Anda ke bucket S3 Anda, data tersebut harus disimpan dalam format yang kompatibel dengan UTF-8.
- Tombol objek S3 memiliki panjang maksimum 1.024 byte. FSx for Lustre tidak akan mengeksport file yang kunci objek S3 yang sesuai akan lebih panjang dari 1.024 byte.

i Note

Semua objek yang dibuat oleh tugas repositori data ekspor dan ekspor otomatis ditulis menggunakan kelas penyimpanan Standar S3.

Topik

- [Ekspor pembaruan ke bucket S3 Anda secara otomatis](#)
- [Menggunakan tugas repositori data untuk mengeksport perubahan](#)
- [Mengeksport file menggunakan perintah HSM](#)

Ekspor pembaruan ke bucket S3 Anda secara otomatis

Anda dapat mengonfigurasi sistem file FSx for Lustre untuk memperbarui konten bucket S3 yang ditautkan secara otomatis saat file ditambahkan, diubah, atau dihapus pada sistem file. FSx for Lustre membuat, memperbarui, atau menghapus objek di S3, sesuai dengan perubahan dalam sistem file.

Note

Ekspor otomatis tidak tersedia di FSx for Lustre 2.10 sistem file atau sistem file. Scratch 1

Anda dapat mengekspor ke repositori data yang Wilayah AWS sama dengan sistem file atau yang berbeda. Wilayah AWS

Anda dapat mengonfigurasi ekspor otomatis saat membuat asosiasi repositori data dan memperbarui pengaturan ekspor otomatis kapan saja menggunakan konsol manajemen FSx, API, dan API AWS CLI. AWS

Note

Anda dapat mengonfigurasi ekspor otomatis dan impor otomatis pada asosiasi repositori data yang sama. Topik ini hanya menjelaskan fitur ekspor otomatis.

Important

- Jika file dimodifikasi dalam sistem file dengan semua kebijakan ekspor otomatis diaktifkan dan impor otomatis dinonaktifkan, konten file itu selalu diekspor ke objek yang sesuai di S3. Jika objek sudah ada di lokasi target, objek akan ditimpa.
- Jika file dimodifikasi di sistem file dan S3, dengan semua impor otomatis dan kebijakan ekspor otomatis diaktifkan, baik file dalam sistem file atau objek di S3 dapat ditimpa oleh yang lain. Tidak dijamin bahwa pengeditan nanti di satu lokasi akan menimpa suntingan sebelumnya di lokasi lain. Jika Anda memodifikasi file yang sama di sistem file dan bucket S3, Anda harus memastikan koordinasi tingkat aplikasi untuk mencegah konflik tersebut. FSx for Lustre tidak mencegah penulisan yang bertentangan di beberapa lokasi.

Kebijakan ekspor menentukan bagaimana Anda ingin FSx for Lustre memperbarui bucket S3 terkait Anda saat konten berubah dalam sistem file. Asosiasi repositori data dapat memiliki salah satu kebijakan ekspor otomatis berikut:

- Baru - FSx for Lustre secara otomatis memperbarui repositori data S3 hanya ketika file, direktori, atau symlink baru dibuat pada sistem file.
- Berubah - FSx for Lustre secara otomatis memperbarui repositori data S3 hanya ketika file yang ada dalam sistem file diubah. Untuk perubahan konten file, file harus ditutup sebelum disebarkan ke repositori S3. Perubahan metadata (ganti nama, kepemilikan, izin, dan stempel waktu) disebarkan saat operasi selesai. Untuk mengubah nama perubahan (termasuk pemindahan), objek S3 yang ada (telah diganti namanya) dihapus dan objek S3 baru dibuat dengan nama baru.
- Dihapus - FSx for Lustre secara otomatis memperbarui repositori data S3 hanya ketika file, direktori, atau symlink dihapus dalam sistem file.
- Kombinasi apa pun dari New, Changed, dan Deleted - FSx for Lustre secara otomatis memperbarui repositori data S3 ketika salah satu tindakan yang ditentukan terjadi dalam sistem file. Misalnya, Anda dapat menentukan bahwa repositori S3 diperbarui ketika file ditambahkan ke (Baru) atau dihapus dari (Dihapus) sistem file, tetapi tidak ketika file diubah.
- Tidak ada kebijakan yang dikonfigurasi - FSx for Lustre tidak secara otomatis memperbarui repositori data S3 ketika file ditambahkan ke, diubah, atau dihapus dari sistem file. Jika Anda tidak mengonfigurasi kebijakan ekspor, ekspor otomatis akan dinonaktifkan. Anda masih dapat mengekspor perubahan secara manual dengan menggunakan tugas repositori data ekspor, seperti yang dijelaskan dalam [Menggunakan tugas repositori data untuk mengekspor perubahan](#)

Untuk sebagian besar kasus penggunaan, sebaiknya Anda mengonfigurasi kebijakan ekspor New, Changed, dan Deleted. Kebijakan ini memastikan bahwa semua pembaruan yang dilakukan pada sistem file Anda secara otomatis diekspor ke repositori data S3 terkait Anda.

Kami menyarankan Anda [mengaktifkan CloudWatch log](#) ke Log untuk mencatat informasi tentang file atau direktori apa pun yang tidak dapat diekspor secara otomatis. Peringatan dan kesalahan dalam log berisi informasi tentang alasan kegagalan. Untuk informasi selengkapnya, lihat [Log peristiwa repositori data](#).

Memperbarui pengaturan ekspor

Anda dapat menyetel setelan ekspor sistem file ke bucket S3 yang ditautkan saat membuat asosiasi repositori data. Untuk informasi selengkapnya, lihat [Membuat tautan ke bucket S3](#).

Anda juga dapat memperbarui pengaturan ekspor kapan saja, termasuk kebijakan ekspor. Untuk informasi selengkapnya, lihat [Memperbarui pengaturan asosiasi repositori data](#).

Memantau ekspor otomatis

Anda dapat memantau asosiasi repositori data yang diaktifkan ekspor otomatis menggunakan satu set metrik yang dipublikasikan ke Amazon. CloudWatch `AgeOf01destQueuedMessage` metrik mewakili usia pembaruan tertua yang dibuat untuk sistem file yang belum diekspor ke S3. Jika `AgeOf01destQueuedMessage` lebih besar dari nol untuk jangka waktu yang lama, kami sarankan untuk sementara mengurangi jumlah perubahan (penggantian nama direktori khususnya) yang secara aktif sedang dibuat ke sistem file sampai antrian pesan telah berkurang. Untuk informasi selengkapnya, lihat [AutoImport dan AutoExport metrik](#).

Important

Saat menghapus asosiasi repositori data atau sistem file dengan ekspor otomatis diaktifkan, Anda harus terlebih dahulu memastikan bahwa `AgeOf01destQueuedMessage` itu nol, artinya tidak ada perubahan yang belum diekspor. Jika `AgeOf01destQueuedMessage` lebih besar dari nol saat Anda menghapus asosiasi repositori data atau sistem file, perubahan yang belum diekspor tidak akan mencapai bucket S3 tertaut Anda. Untuk menghindari hal ini, tunggu `AgeOf01destQueuedMessage` hingga mencapai nol sebelum menghapus asosiasi repositori data atau sistem file Anda.

Menggunakan tugas repositori data untuk mengekspor perubahan

Tugas repositori data ekspor mengekspor file yang baru atau diubah dalam sistem file Anda. Ini menciptakan objek baru di S3 untuk file baru pada sistem file. Untuk file apa pun yang telah dimodifikasi pada sistem file, atau yang metadatanya telah dimodifikasi, objek yang sesuai di S3 diganti dengan objek baru dengan data dan metadata baru. Tidak ada tindakan yang diambil untuk file yang telah dihapus dari sistem file.

Note

Ingatlah hal berikut saat menggunakan tugas repositori data ekspor:

- Penggunaan wildcard untuk menyertakan atau mengecualikan file untuk ekspor tidak didukung.

- Saat melakukan mv operasi, file target setelah dipindahkan akan diekspor ke S3 meskipun tidak ada UID, GID, izin, atau perubahan konten.

Gunakan prosedur berikut untuk mengekspor data dan perubahan metadata pada sistem file ke bucket S3 tertaut dengan menggunakan konsol Amazon FSx dan CLI. Perhatikan bahwa Anda dapat menggunakan satu tugas repositori data untuk beberapa DRA.

Untuk mengekspor perubahan (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Pada panel navigasi, pilih Sistem file, lalu pilih sistem file Lustre Anda.
3. Pilih tab Repositori data.
4. Di panel Asosiasi repositori data, pilih asosiasi repositori data yang ingin Anda buat tugas ekspor.
5. Untuk Tindakan, pilih tugas Ekspor. Pilihan ini tidak tersedia jika sistem file tidak ditautkan ke repositori data di S3. Dialog tugas repositori data ekspor akan muncul.

Create export data repository task



The Export data repository task exports data and POSIX metadata changes from your FSx file system to its linked data repository.

File system paths to export - *optional*

You can enter up to 32 export paths, each on its own line.

Completion report

- Enable
 Disable

Cancel

Create data repository task

- (Opsional) Tentukan hingga 32 direktori atau file yang akan diekspor dari sistem file Amazon FSx Anda dengan menyediakan jalur ke direktori atau file tersebut di jalur sistem File untuk diekspor. Jalur yang Anda berikan harus relatif terhadap titik pemasangan dari sistem file. Jika titik pemasangan adalah `/mnt/fsx` dan `/mnt/fsx/path1` adalah direktori atau file pada sistem file yang ingin Anda ekspor, maka jalur untuk menyediakan adalah `path1`.

Note

Jika jalan yang Anda berikan tidak valid, tugas gagal.

- (Opsional) Pilih Aktifkan di Laporan penyelesaian untuk membuat laporan penyelesaian tugas setelah tugas selesai. Laporan penyelesaian tugas menyediakan detail mengenai file-file yang diproses berdasarkan tugas yang memenuhi cakupan yang ada di Cakupan laporan. Untuk menentukan lokasi Amazon FSx guna menyampaikan laporan, masukkan jalur relatif pada repositori data S3 tertaut dari sistem file untuk Jalur laporan.
- Pilih Buat.

Pemberitahuan di bagian atas halaman Sistem file menampilkan tugas yang baru saja Anda buat dalam proses.

Untuk melihat status tugas dan detail, gulir ke bawah ke panel Tugas Repositori Data di tab Repositori Data untuk sistem file. Urutan default menampilkan tugas terbaru di bagian atas daftar.

Untuk melihat ringkasan tugas dari halaman ini, pilih ID tugas untuk tugas yang baru saja Anda buat. Halaman Ringkasan untuk tugas muncul.

Untuk mengekspor perubahan (CLI)

- Gunakan perintah [create-data-repository-task](#) CLI untuk mengekspor data dan perubahan metadata pada sistem file FSx for Lustre Anda. Operasi API yang sesuai adalah [CreateDataRepositoryTask](#).

```
$ aws fsx create-data-repository-task \
  --file-system-id fs-0123456789abcdef0 \
  --type EXPORT_TO_REPOSITORY \
  --paths path1,path2/file1 \
  --report Enabled=true
```

Setelah berhasil membuat tugas repositori data, Amazon FSx mengembalikan deskripsi tugas sebagai JSON, seperti yang ditunjukkan dalam contoh berikut.

```
{
  "Task": {
    "TaskId": "task-123f8cd8e330c1321",
    "Type": "EXPORT_TO_REPOSITORY",
    "Lifecycle": "PENDING",
    "FileSystemId": "fs-0123456789abcdef0",
    "Paths": ["path1", "path2/file1"],
    "Report": {
      "Path": "s3://dataset-01/reports",
      "Format": "REPORT_CSV_20191124",
      "Enabled": true,
      "Scope": "FAILED_FILES_ONLY"
    },
    "CreationTime": "1545070680.120",
    "ClientRequestToken": "10192019-drt-12",
```

```
"ResourceARN": "arn:aws:fsx:us-  
east-1:123456789012:task:task-123f8cd8e330c1321"  
  }  
}
```

Setelah membuat tugas untuk mengekspor data ke repositori data tertaut, Anda dapat memeriksa status tugas repositori data ekspor. Untuk informasi selengkapnya tentang melihat tugas repositori data, lihat [Mengakses tugas repositori data](#).

Mengekspor file menggunakan perintah HSM

Note

Untuk mengekspor perubahan dalam data dan metadata sistem file FSx for Lustre Anda ke repositori data tahan lama di Amazon S3, gunakan fitur ekspor otomatis yang dijelaskan di [Ekspor pembaruan ke bucket S3 Anda secara otomatis](#) Anda juga dapat menggunakan tugas repositori data ekspor, dijelaskan dalam [Menggunakan tugas repositori data untuk mengekspor perubahan](#)

Untuk mengekspor file individual ke repositori data Anda dan memverifikasi bahwa file telah berhasil diekspor ke repositori data Anda, Anda dapat menjalankan perintah yang ditampilkan berikut. Sebuah nilai kembali `states: (0x00000009) exists archived` menunjukkan bahwa file telah berhasil diekspor.

```
sudo lfs hsm_archive path/to/export/file  
sudo lfs hsm_state path/to/export/file
```

Note

Anda harus menjalankan perintah HSM (seperti `hsm_archive`) sebagai pengguna root atau menggunakan `sudo`.

Untuk mengekspor seluruh sistem file Anda atau seluruh direktori dalam sistem file Anda, jalankan perintah berikut. Jika Anda mengekspor beberapa file secara bersamaan, Amazon FSx for Lustre mengekspor file Anda ke repositori data Amazon S3 Anda secara paralel.

```
nohup find local/directory -type f -print0 | xargs -0 -n 1 sudo lfs hsm_archive &
```

Untuk menentukan apakah ekspor telah selesai, jalankan perintah berikut.

```
find path/to/export/file -type f -print0 | xargs -0 -n 1 -P 8 sudo lfs hsm_state | awk '!/\<archived\>/ || /\<dirty\>/' | wc -l
```

Jika perintah kembali dengan nol file yang tersisa, ekspor selesai.

Tugas repositori data

Dengan menggunakan tugas repositori data impor dan ekspor, Anda dapat mengelola transfer data dan metadata antara sistem file FSx for Lustre dan repositori data tahan lama di Amazon S3.

Tugas repositori data mengoptimalkan transfer data dan metadata antara sistem file FSx for Lustre Anda dan repositori data di S3. Salah satu cara yang mereka lakukan adalah dengan melacak perubahan antara sistem file Amazon FSx Anda dan repositori data yang tertaut dengannya. Mereka juga melakukan ini dengan menggunakan teknik transfer paralel untuk mentransfer data dengan kecepatan hingga ratusan GB/s. Anda membuat dan melihat tugas repositori data menggunakan konsol Amazon FSx, API Amazon FSx, AWS CLI dan Amazon FSx.

Tugas repositori data mempertahankan sistem file dari metadata Antarmuka Sistem Operasi Portabel (POSIX), termasuk kepemilikan, izin, dan timestamp. Karena tugas mempertahankan metadata ini, Anda dapat menerapkan dan memelihara kontrol akses antara sistem file FSx for Lustre dan repositori data tertautnya.

Anda dapat menggunakan tugas repositori data rilis untuk mengosongkan ruang sistem file untuk file baru dengan merilis file yang diekspor ke Amazon S3. Konten file yang dirilis dihapus, tetapi metadata dari file yang dirilis tetap ada di sistem file. Pengguna dan aplikasi masih dapat mengakses file yang dirilis dengan membaca file lagi. Saat pengguna atau aplikasi membaca file yang dirilis, FSx for Lustre secara transparan mengambil konten file dari Amazon S3.

Jenis-jenis tugas repositori data

Ada tiga jenis tugas repositori data:

- Ekspor tugas repositori data ekspor dari sistem file Lustre Anda ke bucket S3 yang ditautkan.

- Impor tugas repositori data yang diimpor dari bucket S3 tertaut ke sistem file Lustre Anda.
- Tugas repositori data rilis file yang diekspor ke bucket S3 tertaut dari sistem file Lustre Anda.

Untuk informasi selengkapnya, lihat [Membuat tugas repositori data](#).

Topik

- [Memahami status dan detail tugas](#)
- [Menggunakan tugas repositori data](#)
- [Bekerja dengan laporan penyelesaian tugas](#)
- [Memecahkan masalah kegagalan tugas repositori data](#)

Memahami status dan detail tugas

Sebuah tugas repositori data dapat memiliki salah satu dari status-status berikut:

- TERTUNDA menunjukkan bahwa Amazon FSx belum mulai mengerjakan tugas.
- MENGEKSEKUSI menunjukkan bahwa Amazon FSx sedang memproses tugas.
- GAGAL menunjukkan bahwa Amazon FSx tidak berhasil memproses tugas. Sebagai contoh, kemungkinan ada file-file yang tugasnya gagal diproses. Detail tugas memberikan informasi lebih lanjut tentang kegagalan tugas. Untuk informasi selengkapnya tentang tugas yang gagal, lihat [Memecahkan masalah kegagalan tugas repositori data](#).
- BERHASIL menunjukkan bahwa Amazon FSx telah menyelesaikan tugas dengan sukses.
- DIBATALKAN menunjukkan bahwa tugas dibatalkan dan tidak terselesaikan.
- MEMBATALKAN menunjukkan bahwa Amazon FSx sedang dalam proses membatalkan tugas.

Setelah sebuah tugas dibuat, Anda dapat melihat informasi dengan detail sebagai berikut untuk tugas repositori data menggunakan konsol, CLI, atau API Amazon FSx:

- Jenis tugas:
 - EXPORT_TO_REPOSITORY menunjukkan tugas ekspor.
 - IMPORT_METADATA_FROM_REPOSITORY menunjukkan tugas impor.
 - RELEASE_DATA_FROM_FILESYSTEM menunjukkan tugas rilis.
- Sistem file tempat tugas dikerjakan.

- Waktu pengerjaan tugas.
- Status tugas.
- Jumlah total file yang tugasnya diproses.
- Jumlah total file yang tugasnya berhasil diproses.
- Jumlah total file yang tugasnya gagal diproses. Nilai ini lebih besar dari nol ketika status tugas GAGAL. Informasi mendetail tentang file-file yang gagal ada di laporan penyelesaian tugas. Untuk informasi selengkapnya, lihat [Bekerja dengan laporan penyelesaian tugas](#).
- Waktu ketika tugas dimulai.
- Waktu ketika status tugas terakhir diperbarui. Status tugas diperbarui setiap 30 detik.

Untuk informasi selengkapnya tentang mengakses tugas repositori data yang ada, lihat [Mengakses tugas repositori data](#).

Menggunakan tugas repositori data

Anda dapat membuat, menduplikasi, melihat detail, dan membatalkan tugas repositori data menggunakan konsol, CLI, atau API Amazon FSx.

Topik

- [Membuat tugas repositori data](#)
- [Menduplikasi sebuah tugas](#)
- [Mengakses tugas repositori data](#)
- [Membatalkan tugas repositori data](#)

Membuat tugas repositori data

Anda dapat membuat tugas repositori data dengan menggunakan konsol, CLI, atau API Amazon FSx. Setelah Anda membuat tugas, Anda dapat melihat kemajuan dan status pengerjaan tugas dengan menggunakan konsol tersebut, CLI, atau API.

Anda dapat membuat tiga jenis tugas repositori data:

- Tugas repositori data Ekspor mengeksport dari sistem file Lustre Anda ke bucket S3 yang ditautkan. Untuk informasi selengkapnya, lihat [Menggunakan tugas repositori data untuk mengeksport perubahan](#).

- Tugas Impor data repositori mengimpor dari bucket S3 tertaut ke sistem file Lustre Anda. Untuk informasi selengkapnya, lihat [Menggunakan tugas repositori data untuk mengimpor perubahan](#).
- Tugas repositori data rilis merilis file dari sistem file Lustre Anda yang telah diekspor ke bucket S3 tertaut. Untuk informasi selengkapnya, lihat [Menggunakan tugas repositori data untuk merilis file](#).

Menduplikasi sebuah tugas

Anda dapat menduplikasi tugas repositori data yang ada di konsol Amazon FSx. Saat Anda menduplikasi tugas, salinan persis dari tugas yang ada ditampilkan di tugas Buat repositori data impor atau Buat halaman tugas repositori data ekspor. Anda dapat membuat perubahan pada jalur untuk mengekspor atau mengimpor, sesuai kebutuhan, sebelum membuat dan menjalankan tugas baru.

Note

Permintaan untuk menjalankan tugas duplikat akan gagal jika salinan persis tugas itu sudah berjalan. Salinan persis tugas yang sudah berjalan berisi jalur atau jalur sistem file yang sama dalam kasus tugas ekspor atau jalur repositori data yang sama dalam kasus tugas impor.

Anda dapat menduplikasi tugas dari tampilan detail tugas, panel Tugas Repositori Data di tab Repositori Data untuk sistem file, atau dari halaman tugas repositori data.

Untuk menduplikasi tugas yang ada

1. Pilih tugas pada panel Tugas Repositori Data di tab Repositori Data untuk sistem file.
2. Pilih Tugas duplikasi. Bergantung pada jenis tugas yang Anda pilih, tugas Buat repositori data impor atau Buat halaman tugas repositori data ekspor muncul. Semua pengaturan untuk tugas baru identik dengan tugas yang Anda duplikasi.
3. Ubah atau tambahkan jalur yang ingin Anda impor atau ekspor.
4. Pilih Buat.

Mengakses tugas repositori data

Setelah Anda membuat sebuah tugas repositori data, Anda dapat mengakses tugas, dan semua tugas yang ada di akun Anda, menggunakan konsol, CLI, dan API Amazon FSx. Amazon FSx menyediakan informasi tugas dengan detail sebagai berikut:

- Semua tugas yang ada.
- Semua tugas untuk sistem file tertentu.
- Semua tugas untuk asosiasi repositori data tertentu.
- Semua tugas dengan status siklus hidup tertentu. Untuk informasi selengkapnya tentang nilai status siklus hidup tugas, lihat [Memahami status dan detail tugas](#).

Anda dapat mengakses semua tugas repositori data yang ada di akun Anda dengan menggunakan konsol, CLI, atau API Amazon FSx, sebagaimana yang dijelaskan berikut.

Untuk melihat tugas repositori data dan detail tugas (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Pada panel navigasi, pilih Tugas-tugas repositori data (Lustre). Halaman Tugas repositori data akan muncul, menampilkan tugas yang ada.
3. Untuk melihat detail tugas, pilih ID tugas atau Nama tugas di halaman tugas repositori data. Halaman detail tugas akan muncul.

Task status Info		
 Canceled	Total number of files to export Info 0 Files successfully exported Info 0 Files failed to export Info 0	Task start time Info 2019-12-17T17:21:15-05:00 Task end time Info 2019-12-17T17:22:13-05:00 Task last updated time Info 2019-12-17T17:21:36-05:00
Completion report		
 Enabled	Report format REPORT_CSV_20191124 Report scope FAILED_FILES_ONLY	Report path s3://completion-report-test/FSxLustre20191217T214233Z/.aws-fsx-data-repository-tasks

Untuk mengambil tugas repositori data dan detail tugas (CLI)

Dengan menggunakan Amazon FSx untuk melakukan perintah CLI [describe-data-repository-tasks](#), Anda dapat melihat semua tugas data repositori, dan detail-detailnya, di akun Anda. [DescribeDataRepositoryTasks](#) adalah setara dengan perintah API.

- Gunakan perintah berikut untuk menampilkan semua objek tugas repositori data di akun Anda.

```
aws fsx describe-data-repository-tasks
```

Jika perintah berhasil, Amazon FSx mengembalikan respons dalam format JSON.

```
{
  "DataRepositoryTasks": [
    {
      "Lifecycle": "EXECUTING",
      "Paths": [],
      "Report": {
        "Path": "s3://dataset-01/reports",
        "Format": "REPORT_CSV_20191124",
        "Enabled": true,
        "Scope": "FAILED_FILES_ONLY"
      },
      "StartTime": 1591863862.288,
      "EndTime": ,
      "Type": "EXPORT_TO_REPOSITORY",
      "Tags": [],
      "TaskId": "task-0123456789abcdef3",
      "Status": {
        "SucceededCount": 4255,
        "TotalCount": 4200,
        "FailedCount": 55,
        "LastUpdatedTime": 1571863875.289
      },
      "FileSystemId": "fs-0123456789a7",
      "CreationTime": 1571863850.075,
      "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef3"
    },
    {
      "Lifecycle": "FAILED",
      "Paths": [],
      "Report": {
        "Enabled": false,
      },
      "StartTime": 1571863862.288,
      "EndTime": 1571863905.292,
      "Type": "EXPORT_TO_REPOSITORY",
      "Tags": [],
    }
  ]
}
```

```

    "TaskId": "task-0123456789abcdef1",
    "Status": {
      "SucceededCount": 1153,
      "TotalCount": 1156,
      "FailedCount": 3,
      "LastUpdatedTime": 1571863875.289
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "CreationTime": 1571863850.075,
    "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef1"
  },
  {
    "Lifecycle": "SUCCEEDED",
    "Paths": [],
    "Report": {
      "Path": "s3://dataset-04/reports",
      "Format": "REPORT_CSV_20191124",
      "Enabled": true,
      "Scope": "FAILED_FILES_ONLY"
    },
    "StartTime": 1571863862.288,
    "EndTime": 1571863905.292,
    "Type": "EXPORT_TO_REPOSITORY",
    "Tags": [],
    "TaskId": "task-04299453935122318",
    "Status": {
      "SucceededCount": 258,
      "TotalCount": 258,
      "FailedCount": 0,
      "LastUpdatedTime": 1771848950.012,
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "CreationTime": 1771848950.012,
    "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef0"
  }
]
}

```

Melihat tugas berdasarkan sistem file

Anda dapat melihat semua tugas untuk sistem file tertentu menggunakan konsol, CLI, atau API Amazon FSx, sebagaimana yang dijelaskan berikut.

Untuk menampilkan tugas berdasarkan sistem file (konsol)

1. Pilih Sistem file pada panel navigasi. Halaman Sistem file akan muncul.
2. Pilih sistem file yang ingin Anda lihat tugas repositori data-nya. Halaman detail sistem file akan muncul.
3. Pada halaman detail sistem file, pilih tab Repositori data. Setiap tugas untuk sistem file ini muncul di panel tugas repositori data.

Untuk mengambil tugas berdasarkan sistem file (CLI)

- Gunakan perintah berikut untuk menampilkan semua tugas repositori data untuk sistem file fs-0123456789abcdef0.

```
aws fsx describe-data-repository-tasks \  
  --filters Name=file-system-id,Values=fs-0123456789abcdef0
```

Jika perintah berhasil, Amazon FSx mengembalikan respons dalam format JSON.

```
{  
  "DataRepositoryTasks": [  
    {  
      "Lifecycle": "FAILED",  
      "Paths": [],  
      "Report": {  
        "Path": "s3://dataset-04/reports",  
        "Format": "REPORT_CSV_20191124",  
        "Enabled": true,  
        "Scope": "FAILED_FILES_ONLY"  
      },  
      "StartTime": 1571863862.288,  
      "EndTime": 1571863905.292,  
      "Type": "EXPORT_TO_REPOSITORY",  
      "Tags": [],  
      "TaskId": "task-0123456789abcdef1",  
      "Status": {  
        "SucceededCount": 1153,  
        "FailedCount": 0,  
        "CancelledCount": 0,  
        "TotalCount": 1153,  
        "Status": "SUCCEEDED"  
      }  
    }  
  ]  
}
```

```

        "TotalCount": 1156,
        "FailedCount": 3,
        "LastUpdatedTime": 1571863875.289
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "CreationTime": 1571863850.075,
    "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef1"
    },
    {
        "Lifecycle": "SUCCEEDED",
        "Paths": [],
        "Report": {
            "Enabled": false,
        },
        "StartTime": 1571863862.288,
        "EndTime": 1571863905.292,
        "Type": "EXPORT_TO_REPOSITORY",
        "Tags": [],
        "TaskId": "task-0123456789abcdef0",
        "Status": {
            "SucceededCount": 258,
            "TotalCount": 258,
            "FailedCount": 0,
            "LastUpdatedTime": 1771848950.012,
        },
        "FileSystemId": "fs-0123456789abcdef0",
        "CreationTime": 1771848950.012,
        "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef0"
    }
]
}

```

Membatalkan tugas repositori data

Anda dapat membatalkan tugas repositori data ketika berstatus baik TERTUNDA maupun MENGEKSEKUSI. Ketika Anda membatalkan sebuah tugas, hal berikut ini terjadi:

- Amazon FSx tidak memproses file apa pun yang sedang dalam antrean untuk diproses.
- Amazon FSx terus memproses file apa pun yang sedang dalam proses.

- Amazon FSx tidak mengembalikan file yang tugasnya sudah diproses.

Untuk membatalkan tugas repositori data (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Klik pada sistem file yang ingin Anda batalkan tugas repositori data.
3. Buka tab Data Repository dan gulir ke bawah untuk melihat panel Data Repository Tasks.
4. Pilih ID tugas atau Nama tugas untuk tugas yang ingin Anda batalkan.
5. Pilih Batalkan tugas untuk membatalkan tugas.
6. Masukkan ID tugas untuk mengonfirmasi permintaan pembatalan.

Untuk membatalkan tugas repositori data (CLI)

Gunakan perintah Amazon FSx [cancel-data-repository-task](#) CLI, untuk membatalkan tugas. [CancelDataRepositoryTask](#) adalah perintah API yang setara.

- Gunakan perintah berikut untuk membatalkan tugas repositori data.

```
aws fsx cancel-data-repository-task \  
  --task-id task-0123456789abcdef0
```

Jika perintah berhasil, Amazon FSx mengembalikan respons dalam format JSON.

```
{  
  "Status": "CANCELING",  
  "TaskId": "task-0123456789abcdef0"  
}
```

Bekerja dengan laporan penyelesaian tugas

Laporan penyelesaian tugas memberikan rincian tentang hasil tugas repositori data ekspor, impor, atau rilis. Laporan ini termasuk hasil untuk file-file yang diproses oleh tugas yang sesuai dengan cakupan laporan. Anda dapat menentukan apakah Anda ingin menghasilkan laporan atas sebuah tugas dengan menggunakan parameter `Enabled`.

Amazon FSx menyampaikan laporan ke repositori data tertaut pada sistem file di Amazon S3, menggunakan jalur yang Anda tentukan saat Anda mengaktifkan laporan untuk tugas. Nama file laporan adalah `report.csv` untuk tugas impor dan `failures.csv` untuk tugas ekspor atau rilis.

Format laporan adalah file CSV (nilai yang dipisahkan koma) yang memiliki tiga bidang: `FilePath`, `FileStatus`, dan `ErrorCode`.

Laporan dikodekan menggunakan format encode RFC-4180 sebagai berikut:

- Jalur dimulai dengan salah satu karakter berikut yang berada dalam tanda kutip tunggal: @ + - =
- String yang memiliki setidaknya salah satu dari karakter-karakter berikut yang terkandung dalam tanda kutip ganda: " ,
- Semua tanda kutip ganda lolos dengan tanda kutip ganda tambahan.

Berikut ini adalah beberapa contoh dari pengkodean laporan:

- `@filename.txt` menjadi `"@filename.txt"`
- `+filename.txt` menjadi `"+filename.txt"`
- `file,name.txt` menjadi `"file,name.txt"`
- `file"name.txt` menjadi `"file""name.txt"`

Untuk informasi selengkapnya tentang pengkodean RFC-4180, lihat [RFC-4180 - Format Umum dan Jenis MIME untuk File CSV \(Nilai yang Dipisahkan Koma\)](#) di situs web IETF.

Berikut ini adalah contoh dari informasi yang diberikan dalam laporan penyelesaian tugas yang berisikan file gagal saja.

```
myRestrictedFile,failed,S3AccessDenied
dir1/myLargeFile,failed,FileSizeTooLarge
dir2/anotherLargeFile,failed,FileSizeTooLarge
```

Untuk informasi lebih lanjut tentang kegagalan tugas dan cara mengubahnya, lihat [Memecahkan masalah kegagalan tugas repositori data](#).

Memecahkan masalah kegagalan tugas repositori data

Anda dapat [mengaktifkan logging](#) ke CloudWatch Log untuk mencatat informasi tentang kegagalan yang dialami saat mengimpor atau mengekspor file menggunakan tugas repositori data. Untuk informasi tentang CloudWatch log peristiwa Log, lihat [Log peristiwa repositori data](#).

Ketika tugas repositori data gagal, Anda dapat menemukan jumlah file yang gagal diproses Amazon FSx di File-file yang gagal diekspor di halaman Status tugas pada konsol tersebut. Atau Anda dapat menggunakan CLI atau API dan melihat hal yang Status: FailedCount pada tugas. Untuk informasi tentang mengakses informasi ini, lihat [Mengakses tugas repositori data](#).

Untuk tugas repositori data, Amazon FSx juga secara opsional memberikan informasi tentang file dan direktori tertentu yang gagal dalam laporan penyelesaian. Laporan penyelesaian tugas berisikan jalur file atau direktori pada sistem file Lustre yang gagal, statusnya, dan alasan kegagalannya. Untuk informasi selengkapnya, lihat [Bekerja dengan laporan penyelesaian tugas](#).

Tugas repositori data dapat gagal karena beberapa alasan, termasuk hal-hal yang tercantum berikut ini.

Kode Kesalahan	Penjelasan
FileSizeTooLarge	Ukuran objek maksimum yang didukung oleh Amazon S3 adalah 5 TiB.
InternalError	Terjadi kesalahan dalam sistem file Amazon FSx untuk tugas impor, ekspor, atau rilis. Umumnya, kode kesalahan ini berarti bahwa sistem file Amazon FSx yang menjalankan tugas gagal berada dalam status siklus hidup GAGAL. Ketika hal ini terjadi, file-file yang terpengaruh mungkin tidak dapat dipulihkan karena hilangnya data. Jika tidak, Anda dapat menggunakan perintah manajemen penyimpanan hirarkis (HSM) untuk mengekspor file dan direktori ke repositori data pada S3. Untuk informasi selengkapnya, lihat Mengekspor file menggunakan perintah HSM .

Kode Kesalahan	Penjelasan
OperationNotPermitted	Amazon FSx tidak dapat menulis file karena belum diekspor ke bucket S3 yang ditautkan. Anda harus menggunakan tugas repositori data ekspor atau ekspor otomatis untuk memastikan bahwa file Anda diekspor terlebih dahulu ke bucket Amazon S3 yang ditautkan.
PathSizeTooLong	Jalur ekspor terlalu panjang. Panjang kunci objek maksimum yang didukung oleh S3 adalah 1.024 karakter.
ResourceBusy	Amazon FSx tidak dapat mengekspor atau menulis file karena sedang diakses oleh klien lain pada sistem file. Anda dapat mencoba lagi DataRepositoryTask setelah alur kerja Anda selesai menulis ke file.

Kode Kesalahan	Penjelasan
S3AccessDenied	<p>Akses ditolak ke Amazon S3 untuk tugas ekspor atau impor repositori data.</p> <p>Untuk tugas ekspor, sistem file Amazon FSx harus memiliki izin untuk melakukan <code>S3:PutObject</code> operasi untuk mengekspor ke repositori data tertaut pada S3. Izin ini diberikan dalam peran yang terhubung dengan layanan <code>AWSServiceRoleForFSxS3Access_ fs-0123456789abcdef0</code> . Untuk informasi selengkapnya, lihat Menggunakan peran terkait layanan untuk Amazon FSx.</p> <p>Untuk tugas ekspor, karena tugas ekspor memerlukan data mengalir di luar VPC sistem file, kesalahan ini dapat terjadi jika repositori target memiliki kebijakan bucket yang berisi salah satu kunci kondisi global IAM <code>aws:SourceVpc</code> atau <code>aws:SourceVpc: IAM</code>.</p> <p>Untuk tugas impor, sistem file Amazon FSx harus memiliki izin untuk melakukan <code>S3:HeadObject</code> dan <code>S3:GetObject</code> operasi untuk mengimpor dari repositori data tertaut di S3.</p> <p>Untuk tugas impor, jika bucket S3 Anda menggunakan enkripsi sisi server dengan kunci terkelola pelanggan yang disimpan di AWS Key Management Service (SSE-KMS), Anda harus mengikuti konfigurasi kebijakan di Bekerja dengan bucket Amazon S3 yang dienkrpsi sisi server</p>

Kode Kesalahan	Penjelasan
	<p>Jika bucket S3 berisi objek yang diunggah dari akun bucket S3 yang berbeda Akun AWS dari sistem file yang ditautkan, Anda dapat memastikan bahwa tugas repositori data Anda dapat mengubah metadata S3 atau menimpa objek S3 terlepas dari akun mana yang mengunggahnya. Kami menyarankan Anda mengaktifkan fitur Kepemilikan Objek S3 untuk bucket S3 Anda. Fitur ini memungkinkan Anda untuk mengambil kepemilikan objek baru yang Akun AWS diunggah lain ke bucket Anda, dengan memaksa unggahan untuk menyediakan an ACL <code>-/-acl bucket-owner-full-control</code> kalengan. Aktifkan Kepemilikan Objek S3 dengan memilih opsi pilihan pemilik bucket di bucket S3 Anda. Untuk informasi selengkapnya, lihat Mengendalikan kepemilikan objek yang diunggah dengan menggunakan Kepemilikan Objek S3 di Panduan Pengguna Amazon S3.</p>
S3Error	Amazon FSx mengalami kesalahan terkait S3 yang bukan S3AccessDenied .
S3FileDeleted	Amazon FSx tidak dapat mengekspor file hard link karena file sumber tidak ada di repositori data.

Kode Kesalahan	Penjelasan
S3objectInUnsupportedTier	Amazon FSx berhasil mengimpor objek non-symlink dari S3 Glacier Flexible Retrieval atau kelas penyimpanan S3 Glacier Deep Archive. <code>FileStatus</code> Akan ada <code>succeeded with warning</code> dalam laporan penyelesaian tugas. Peringatan menunjukkan bahwa untuk mengambil data, Anda harus memulihkan objek S3 Glacier Flexible Retrieval atau S3 Glacier Deep Archive terlebih dahulu dan kemudian menggunakan perintah untuk mengimpor objek. <code>hsm_restore</code>
S3objectNotFound	Amazon FSx tidak dapat mengimpor atau mengeksport file karena tidak ada di repositori data.
S3objectPathNotPosixCompliant	Objek Amazon S3 ada tetapi tidak dapat diimpor karena bukan objek yang sesuai dengan POSIX. Untuk informasi tentang metadata POSIX yang didukung, lihat. Dukungan metadata POSIX untuk repositori data
S3objectUpdateInProgressFromFileRename	Amazon FSx tidak dapat merilis file karena ekspor otomatis memproses penggantian nama file. Proses penggantian nama ekspor otomatis harus selesai sebelum file dapat dirilis.
S3SymlinkInUnsupportedTier	Amazon FSx tidak dapat mengimpor objek symlink karena berada di kelas penyimpanan Amazon S3 yang tidak didukung, seperti S3 Glacier Flexible Retrieval atau kelas penyimpanan S3 Glacier Deep Archive. <code>FileStatus</code> Akan ada <code>failed</code> dalam laporan penyelesaian tugas.

Kode Kesalahan	Penjelasan
SourceObjectDeletedBeforeReleasing	Amazon FSx tidak dapat melepaskan file dari sistem file karena file tersebut dihapus dari repositori data sebelum dapat dirilis.

Melepaskan file

Rilis tugas repositori data rilis data file dari sistem file FSx for Lustre Anda untuk mengosongkan ruang untuk file baru. Melepaskan file akan mempertahankan daftar file dan metadata, tetapi menghapus salinan lokal dari isi file tersebut. Jika pengguna atau aplikasi mengakses file yang dirilis, data akan dimuat kembali secara otomatis dan transparan ke sistem file Anda dari bucket Amazon S3 yang ditautkan.

Note

Tugas repositori data rilis tidak tersedia di FSx for Lustre 2.10 sistem file.

Parameter Jalur sistem file untuk dirilis dan Durasi minimum sejak akses terakhir menentukan file mana yang akan dirilis.

- Jalur sistem file untuk dirilis: Menentukan jalur dari mana file akan dirilis.
- Durasi minimum sejak akses terakhir: Menentukan durasi, dalam beberapa hari, sehingga file apa pun yang tidak diakses dalam durasi itu harus dirilis. Durasi sejak file terakhir diakses dihitung dengan mengambil perbedaan antara waktu pembuatan tugas rilis dan terakhir kali file diakses (nilai maksimum `mtime`, dan `ctime`).

File hanya akan dirilis di sepanjang jalur file jika telah diekspor ke S3 dan memiliki durasi sejak akses terakhir yang lebih besar dari durasi minimum sejak nilai akses terakhir. Memberikan durasi minimum sejak akses terakhir 0 hari akan merilis file terlepas dari durasinya sejak akses terakhir.

Note

Penggunaan wildcard untuk menyertakan atau mengecualikan file untuk dirilis tidak didukung.

Tugas repositori data rilis hanya akan merilis data dari file yang telah diekspor ke repositori data S3 tertaut. Anda dapat mengekspor data ke S3 menggunakan fitur ekspor otomatis, tugas repositori data ekspor, atau perintah HSM. Untuk memverifikasi bahwa file telah diekspor ke repositori data Anda, Anda dapat menjalankan perintah berikut. Sebuah nilai kembali `states: (0x00000009) exists archived` menunjukkan bahwa file telah berhasil diekspor.

```
sudo lfs hsm_state path/to/export/file
```

Note

Anda harus menjalankan perintah HSM sebagai pengguna root atau menggunakan `sudo`.

Untuk merilis data file pada interval reguler, Anda dapat menjadwalkan tugas repositori data rilis berulang menggunakan Amazon Scheduler. EventBridge Untuk informasi selengkapnya, lihat [Memulai EventBridge Penjadwal](#) di Panduan Pengguna EventBridge Penjadwal Amazon.

Topik

- [Menggunakan tugas repositori data untuk merilis file](#)

Menggunakan tugas repositori data untuk merilis file

Gunakan prosedur berikut untuk membuat tugas yang melepaskan file dari sistem file dengan menggunakan konsol Amazon FSx dan CLI. Melepaskan file akan mempertahankan daftar file dan metadata, tetapi menghapus salinan lokal dari isi file tersebut.

Untuk melepaskan file (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Sistem file, lalu pilih sistem file Lustre Anda.
3. Pilih tab Repositori data.
4. Di panel Asosiasi repositori data, pilih asosiasi repositori data yang ingin Anda buat tugas rilis.
5. Untuk Tindakan, pilih Buat tugas rilis. Pilihan ini hanya tersedia jika sistem file ditautkan ke repositori data pada S3. Dialog tugas repositori data rilis Buat muncul.

Create release data repository task ✕

The release data repository task reduces the used storage capacity of your file system by removing file data that is synchronized with a linked data repository. File metadata will remain on the file system.

File system paths to release

/ns1

You can enter up to 32 release paths, each on its own line.

Minimum duration since last access

⌵ Days

Completion report

- Enable
 Disable

Report path

s3://my-bucket/optional-prefix

Report format

REPORT_CSV_20191124

Report scope

FAILED_FILES_ONLY

Cancel

Create data repository task

- Di jalur sistem File yang akan dirilis, tentukan hingga 32 direktori atau file yang akan dirilis dari sistem file Amazon FSx Anda dengan menyediakan jalur ke direktori atau file tersebut. Jalur yang Anda berikan harus relatif terhadap titik pemasangan sistem file. Misalnya, jika titik pemasangan adalah `/mnt/fsx` dan `/mnt/fsx/path1` merupakan file pada sistem file yang ingin Anda lepaskan, maka jalur yang akan disediakan adalah `path1`. Untuk melepaskan semua file dalam sistem file, tentukan garis miring maju (`/`) sebagai jalur.

 Note

Jika jalan yang Anda berikan tidak valid, tugas gagal.

- Untuk Durasi minimum sejak akses terakhir, tentukan durasinya, dalam beberapa hari, sehingga file apa pun yang tidak diakses dalam durasi tersebut harus dirilis. Waktu akses terakhir dihitung menggunakan nilai maksimum `time`, `mtime`, dan `ctime`. File dengan periode durasi akses terakhir lebih besar dari durasi minimum sejak akses terakhir (relatif terhadap waktu pembuatan tugas) akan dirilis. File dengan periode durasi akses terakhir kurang dari jumlah hari ini tidak akan dirilis, bahkan jika mereka berada di bidang jalur sistem File ke rilis. Berikan durasi `0` hari untuk merilis file terlepas dari durasi sejak akses terakhir.
- (Opsional) Di bawah Laporan penyelesaian, pilih Aktifkan untuk menghasilkan laporan penyelesaian tugas yang memberikan detail tentang file yang memenuhi cakupan yang disediakan dalam lingkup Laporan. Untuk menentukan lokasi Amazon FSx untuk mengirimkan laporan, masukkan jalur relatif pada repositori data S3 tertaut sistem file untuk jalur Laporan.
- Pilih Buat tugas repositori data.

Pemberitahuan di bagian atas halaman Sistem file menampilkan tugas yang baru saja Anda buat dalam proses.

Untuk melihat status tugas dan detail, di tab Repositori Data, gulir ke bawah ke Tugas Repositori Data. Urutan default menampilkan tugas terbaru di bagian atas daftar.

Untuk melihat ringkasan tugas dari halaman ini, pilih ID tugas untuk tugas yang baru saja Anda buat.

Untuk melepaskan file (CLI)

- Gunakan perintah [create-data-repository-task](#) CLI untuk membuat tugas yang melepaskan file pada sistem file FSx for Lustre Anda. Operasi API yang sesuai adalah [CreateDataRepositoryTask](#).

Atur parameter berikut:

- Setel `--file-system-id` ke ID sistem file tempat Anda melepaskan file dari.
- Atur `--paths` ke jalur pada sistem file dari mana data akan dirilis. Jika direktori ditentukan, file dalam direktori dilepaskan. Jika jalur file ditentukan, hanya file itu yang dirilis. Untuk melepaskan semua file dalam sistem file yang telah diekspor ke bucket S3 tertaut, tentukan garis miring ke depan (/) untuk jalur tersebut.
- Atur `--type` ke `RELEASE_DATA_FROM_FILESYSTEM`.
- Atur `--release-configuration DurationSinceLastAccess` opsi sebagai berikut:
 - Unit – Atur ke `DAYS`.
 - Value— Tentukan bilangan bulat yang mewakili durasi, dalam beberapa hari, sehingga file apa pun yang tidak diakses dalam durasi itu harus dirilis. File yang diakses selama periode kurang dari jumlah hari ini tidak akan dirilis, bahkan jika mereka berada dalam `--paths` parameter. Berikan durasi 0 hari untuk merilis file terlepas dari durasi sejak akses terakhir.

Perintah sampel ini menetapkan bahwa file yang telah diekspor ke bucket S3 tertaut dan memenuhi `--release-configuration` kriteria akan dirilis dari direktori di jalur yang ditentukan.

```
$ aws fsx create-data-repository-task \  
  --file-system-id fs-0123456789abcdef0 \  
  --type RELEASE_DATA_FROM_FILESYSTEM \  
  --paths path1,path2/file1 \  
  --release-configuration '{"DurationSinceLastAccess":  
{"Unit":"DAYS","Value":10}}' \  
  --report Enabled=false
```

Setelah berhasil membuat tugas repositori data, Amazon FSx mengembalikan deskripsi tugas sebagai JSON.

Setelah membuat tugas untuk melepaskan file, Anda dapat memeriksa status tugas. Untuk informasi selengkapnya tentang melihat tugas repositori data, lihat [Mengakses tugas repositori data](#).

Menggunakan Amazon FSx dengan data lokal

Anda dapat menggunakan FSx for Lustre untuk memproses data lokal Anda dengan instans komputasi in-cloud. FSx for Lustre mendukung AWS Direct Connect akses melalui dan VPN, memungkinkan Anda untuk me-mount sistem file Anda dari klien lokal.

Untuk menggunakan FSx for Lustre dengan data lokal

1. Buat sistem file. Untuk informasi selengkapnya, lihat [Buat sistem file FSx for Lustre Anda](#) dalam latihan memulai.
2. Pasang sistem file dari klien on-premise. Untuk informasi selengkapnya, lihat [Memasang sistem file Amazon FSx dari on-premise atau Amazon VPC hasil peering](#).
3. Salin data yang ingin Anda proses ke sistem file FSx for Lustre Anda.
4. Jalankan beban kerja komputasi intensif Anda pada instans Amazon EC2 di cloud yang memasang sistem file Anda.
5. Setelah selesai, salin hasil akhir dari sistem file Anda kembali ke lokasi data lokal, dan hapus sistem file FSx for Lustre Anda.

Log peristiwa repositori data

Anda dapat mengaktifkan logging ke CloudWatch Log untuk mencatat informasi tentang kegagalan yang dialami saat mengimpor atau mengeksport file menggunakan impor otomatis, ekspor otomatis, dan tugas repositori data. Untuk informasi selengkapnya, lihat [Logging dengan Amazon CloudWatch Logs](#).

Note

Ketika tugas repositori data gagal, Amazon FSx juga menulis informasi kegagalan ke laporan penyelesaian tugas. Untuk informasi selengkapnya tentang informasi kegagalan dalam laporan penyelesaian, lihat [Memecahkan masalah kegagalan tugas repositori data](#).

Impor otomatis, ekspor otomatis, dan tugas repositori data dapat gagal karena beberapa alasan, termasuk yang tercantum di bawah ini. Untuk informasi tentang melihat log ini, lihat [Melihat log](#).

Impor acara

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ImportListObjectError	ERROR	<i>Gagal mencantumkan objek S3 di bucket S3 bucket_name dengan awalan awalan.</i>	Amazon FSx gagal mencantumkan objek S3 di bucket S3. Ini dapat terjadi jika kebijakan bucket S3 tidak memberikan izin yang memadai ke Amazon FSx.	N/A
S3ImportUnsupportedTierWarning	PERINGATAN	<i>Gagal mengimpor objek S3 dengan key_value kunci di bucket S3 bucket_name karena objek S3 di tingkat S3_tier_name yang tidak didukung.</i>	Amazon FSx tidak dapat mengimpor objek S3 karena berada di kelas penyimpanan Amazon S3 yang tidak didukung, seperti S3 Glacier Flexible Retrieval atau kelas penyimpanan S3 Glacier Deep Archive.	S3objectInUnsupportedTier

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ImportSymlinkInUnsupportedTierWarning	PERINC N	<i>Gagal mengimpor objek S3 dengan key_value kunci di bucket S3 bucket_name karena objek symlink S3 di tingkat S3_tier_name yang tidak didukung.</i>	Amazon FSx tidak dapat mengimpor objek symlink karena berada di kelas penyimpanan Amazon S3 yang tidak didukung, seperti S3 Glacier Flexible Retrieval atau kelas penyimpanan S3 Glacier Deep Archive.	S3SymlinkInUnsupportedTier

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ImportAccessDenied	ERROR	<p>Gagal mengimpor objek S3 dengan <i>key_value</i> kunci di bucket S3 <i>bucket_name</i> karena akses ke objek S3 ditolak.</p>	<p>Akses ditolak ke Amazon S3 untuk tugas impor ekspor repositori data.</p> <p>Untuk tugas impor, sistem file Amazon FSx harus memiliki izin untuk melakukan <code>s3:HeadObject</code> dan <code>s3:GetObject</code> operasi untuk mengimpor dari repositori data tertaut di S3.</p> <p>Untuk tugas impor, jika bucket S3 Anda menggunakan enkripsi sisi server dengan kunci terkelola pelanggan</p>	S3AccessDenied

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
			yang disimpan di AWS Key Management Service (SSE-KMS) , Anda harus mengikuti konfigurasi kebijakan di. Bekerja dengan bucket Amazon S3 yang dienkripsi sisi server	
S3ImportDeleteAccessDenied	ERROR	Gagal menghapus file lokal untuk objek S3 dengan kunci <i>key_value</i> di bucket S3 <i>bucket_name</i> karena akses ke objek S3 ditolak.	Impor otomatis ditolak akses ke objek S3.	N/A

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ImportObjectPathNotPosixCompliant	ERROR	Gagal mengimpor objek S3 dengan <i>key_value kunci di bucket S3 bucket_name</i> karena objek S3 tidak sesuai POSIX.	Objek Amazon S3 ada tetapi tidak dapat diimpor karena bukan objek yang sesuai dengan POSIX. Untuk informasi tentang metadata POSIX yang didukung, lihat. Dukungan metadata POSIX untuk repositori data	S3ObjectPathNotPosixCompliant

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ImportObjectTypeMismatch	ERROR	Gagal mengimpor objek S3 dengan <i>key_value</i> kunci di bucket S3 <i>bucket_name karena objek S3 dengan nama</i> yang sama telah diimpor ke sistem file.	Objek S3 yang diimpor adalah jenis yang berbeda (file atau direktori) dari objek yang ada dengan nama yang sama dalam sistem file.	S3objectTypeMismatch
S3ImportDirectoryMetadataUpdateError	ERROR	Gagal memperbaiki metadata direktori lokal karena kesalahan internal.	Metadata direktori tidak dapat diimpor karena kesalahan internal.	N/A

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ImportObjectDeleted	ERROR	<i>Gagal mengimpor objek S3 dengan key_value kunci karena tidak ditemukan di bucket S3 bucket_name.</i>	Amazon FSx tidak dapat mengimpor metadata file karena objek yang sesuai tidak ada di repositori data.	S3FileDeleted
S3ImportBucketDoesNotExist	ERROR	Gagal mengimpor objek S3 dengan <i>key_value</i> kunci di bucket S3 <i>bucket_name</i> karena bucket tidak ada.	Amazon FSx tidak dapat secara otomatis mengimpor objek S3 ke sistem file karena bucket S3 tidak ada lagi.	N/A

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ImportDeleteBucketDoesNotExist	ERROR	Gagal menghapus file lokal untuk objek S3 dengan kunci <i>key_value</i> di bucket S3 <i>bucket_name</i> karena bucket tidak ada.	Amazon FSx tidak dapat menghapus file yang ditautkan ke objek S3 pada sistem file karena bucket S3 tidak ada lagi.	N/A
S3ImportDirectoryCreateError	ERROR	Gagal membuat direktori lokal karena kesalahan internal.	Amazon FSx gagal mengimpor pembuatan direktori secara otomatis pada sistem file karena kesalahan internal.	N/A

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
NoDiskSpace	ERROR	Gagal mengimpor objek S3 dengan kunci <i>key_value</i> di bucket S3 <i>bucket_name</i> karena sistem file penuh.	Sistem file kehabisan ruang disk pada server metadata saat membuat file atau direktori.	N/A

Acara ekspor

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ExportInternalError	ERROR	Gagal mengekspor objek S3 dengan kunci di bucket S3 <i>bucket_name</i> karena kesalahan internal.	Objek tidak diekspor karena kesalahan internal.	INTERNAL_ERROR
S3ExportAccessDenied	ERROR	<i>Gagal mengekspor file karena akses ditolak ke</i>	Akses ditolak ke Amazon S3 untuk tugas ekspor repositori data.	S3AccessDenied

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
		<p><i>objek S3 dengan kunci key_value di bucket S3 bucket_name .</i></p>	<p>Untuk tugas ekspor, sistem file Amazon FSx harus memiliki izin untuk melakukan s3:PutObject operasi untuk mengekspor ke repositori data tertaut pada S3. Izin ini diberikan dalam peran yang terhubung dengan layanan AWSServiceRoleForFSxS3Access_ <i>fs-0123456789abcde</i> <i>f0</i> . Untuk informasi selengkapnya, lihat Menganalisis peran terkait layanan untuk Amazon FSx.</p> <p>Karena tugas ekspor memerlukan data mengalir di</p>	

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
			<p>luar VPC sistem file, kesalahan ini dapat terjadi jika repositori target memiliki kebijakan bucket yang berisi salah satu kunci kondisi global IAM <code>aws:SourceVpc</code> atau <code>aws:SourceVpc</code> IAM.</p> <p>Jika bucket S3 berisi objek yang diunggah dari akun bucket S3 yang berbeda Akun AWS dari sistem file yang ditautkan, Anda dapat memastikan bahwa tugas repositori data Anda dapat mengubah metadata S3 atau menimpa objek S3 terlepas dari akun mana yang mengunggah</p>	

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
			<p>hnya. Kami menyarankan Anda mengaktifkan fitur Kepemilikan Objek S3 untuk bucket S3 Anda. Fitur ini memungkinkan Anda untuk mengambil kepemilikan objek baru yang Akun AWS diunggah lain ke bucket Anda, dengan memaksa unggahan untuk menyediakan ACL <code>--acl bucket-owner-full-control</code> kalengan. Aktifkan Kepemilikan Objek S3 dengan memilih opsi pilihan pemilik bucket di bucket S3 Anda. Untuk informasi</p>	

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
			selengkapnya, lihat Mengendalikan kepemilikan objek yang diunggah dengan menggunakan Kepemilikan Objek S3 di Panduan Pengguna Amazon S3.	
S3ExportPathSizeTooLong	ERROR	Gagal mengekspor file karena ukuran jalur file lokal melebihi panjang kunci objek maksimum yang didukung oleh S3.	Jalur ekspor terlalu panjang. Panjang kunci objek maksimum yang didukung oleh S3 adalah 1.024 karakter.	PathSizeTooLong
S3ExportFileSizeTooLarge	ERROR	Gagal mengekspor file karena ukuran file melebihi ukuran objek S3 maksimum yang didukung.	Ukuran objek maksimum yang didukung oleh Amazon S3 adalah 5 TiB.	FileSizeTooLarge

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ExportKMSKeyNotFound	ERROR	Gagal mengekspor file untuk objek S3 dengan kunci <i>key_value</i> di bucket S3 <i>bucket_name</i> karena kunci KMS bucket tidak ditemukan.	Amazon FSx tidak dapat mengekspor file karena AWS KMS key tidak dapat ditemukan. Pastikan untuk menggunakan kunci yang Wilayah AWS sama dengan bucket S3. Untuk informasi selengkapnya tentang membuat kunci KMS, lihat Membuat kunci di Panduan AWS Key Management Service Pengembang.	N/A

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ExportResourceBusy	ERROR	Gagal mengekspor file karena sedang digunakan oleh proses lain.	Amazon FSx tidak dapat mengekspor file karena sedang dimodifikasi oleh klien lain pada sistem file. Anda dapat mencoba kembali tugas setelah alur kerja Anda selesai menulis ke file.	ResourceBusy
S3ExportLocalObjectReleaseWithoutSource	PERINGATAN	<i>Ekspor dilewati: File lokal dalam keadaan dirilis dan objek S3 tertaut dengan key_value kunci tidak ditemukan di bucket bucket_name .</i>	Amazon FSx tidak dapat mengekspor file karena berada dalam keadaan dirilis pada sistem file.	N/A

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3ExportLocalObjectNotMatchDra	PERINGATAN	Ekspor dilewati: file lokal bukan milik jalur sistem file yang ditautkan repositori data.	Amazon FSx tidak dapat mengekspor karena objek tersebut bukan milik jalur sistem file yang ditautkan ke repositori data.	N/A
InternalAutoExportError	ERROR	Ekspor otomatis mengalami kesalahan internal saat mengekspor objek sistem file	Ekspor gagal karena kesalahan internal (ekspor otomatis atau tingkat kilau).	N/A
S3CompletionReportUploadFailure	ERROR	<i>Gagal mengunggah laporan penyelesaian tugas repositori data ke bucket_name</i>	Amazon FSx tidak dapat mengunggah laporan penyelesaian.	N/A

Kode kesalahan	Tingkat log	Pesan log	Penyebab galat	Kode kesalahan dalam laporan penyelesaian
S3CompletionReportValidateFailure	ERROR	Gagal mengunggah laporan penyelesaian tugas repositori data ke bucket <i>bucket_name</i> karena jalur laporan penyelesaian <i>report_path</i> bukan milik repositori data yang terkait dengan sistem file ini	Amazon FSx tidak dapat mengunggah laporan penyelesaian karena jalur S3 yang disediakan pelanggan bukan milik repositori data tertaut.	N/A

Bekerja dengan jenis penyebaran yang lebih lama

Bagian ini berlaku untuk sistem file dengan jenis penyebaran Scratch 1, dan juga untuk sistem file dengan Scratch 2 atau Persistent 1 jenis penyebaran yang tidak menggunakan asosiasi repositori data.

Topik

- [Tautkan sistem file Anda ke bucket Amazon S3](#)
- [Secara otomatis mengimpor pembaruan dari bucket S3](#)

Tautkan sistem file Anda ke bucket Amazon S3

Bila Anda membuat sistem file Amazon FSx for Lustre, Anda dapat menghubungkannya ke repositori data yang tahan lama di Amazon S3. Sebelum Anda membuat sistem file, pastikan Anda telah

membuat bucket Amazon S3 yang Anda tautkan. Dalam Buat sistem file wizard, Anda mengatur properti konfigurasi repositori data berikut di opsi Impor/Ekspor Repositori Data panel.

- Pilih bagaimana Amazon FSx terus memperbarui daftar file dan direktori Anda saat Anda menambahkan atau mengubah objek dalam bucket S3 Anda setelah sistem file dibuat. Untuk informasi selengkapnya, lihat [Secara otomatis mengimpor pembaruan dari bucket S3](#).
- Impor ember: Masukkan nama bucket S3 yang Anda gunakan untuk repositori tertaut.
- Awalan impor: Masukkan awalan impor opsional jika Anda ingin mengimpor hanya beberapa daftar file dan direktori data di bucket S3 Anda ke dalam sistem file Anda. Prefiks impor menentukan tempat di bucket S3 yang menjadi sumber pengimporan data.
- Awalan ekspor: Mendefinisikan tempat Amazon FSx mengeksport konten sistem file Anda ke bucket S3 yang ditautkan.

Anda dapat memiliki pemetaan 1:1 di mana Amazon FSx mengeksport data dari sistem file FSx for Lustre Anda kembali ke direktori yang sama pada bucket S3 yang diimpor. Untuk memiliki pemetaan 1:1, tentukan jalur ekspor ke bucket S3 tanpa awalan apa pun saat Anda membuat sistem file.

- Saat Anda membuat sistem file menggunakan konsol, pilih Awalan ekspor > Awalan yang Anda tentukan pilihan, dan menjaga bidang awalan kosong.
- Ketika Anda membuat sistem file menggunakan AWS CLI atau API, tentukan jalur ekspor sebagai nama bucket S3 tanpa awalan tambahan, misalnya, `ExportPath=s3://lustre-export-test-bucket/`.

Dengan menggunakan metode ini, Anda dapat menyertakan awalan impor saat menentukan jalur impor, dan itu tidak memengaruhi pemetaan 1:1 untuk ekspor.

Membuat sistem file yang terhubung ke bucket S3

Prosedur berikut memandu Anda melalui proses pembuatan sistem file Amazon FSx yang ditautkan ke bucket S3 menggunakan AWS Konsol Manajemen dan AWS Antarmuka Baris Perintah (AWS CLI).

Console

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Dari dasbor, pilih Buat sistem file.
3. Untuk jenis sistem file, pilih FSx untuk Lustre, dan kemudian pilih Berikutnya.

4. Berikan informasi yang diperlukan untuk Detail sistem file dan bagian Jaringan dan keamanan. Untuk informasi selengkapnya, lihat [Buat sistem file FSx for Lustre Anda](#).
5. Anda menggunakan panel Impor/ekspor repositori data untuk mengkonfigurasi repositori data terkait di Amazon S3. Pilih Impor data dari dan ekspor data ke S3 untuk memperluas Impor/ Ekspor Repositori Data bagian dan mengkonfigurasi pengaturan repositori data.

▼ Data Repository Import/Export - optional

Import data from and export data to S3 [Info](#)

When you create your file system, your existing S3 objects will appear as file and directory listings. After you create your file system, how do you want to update it as the contents of your S3 bucket are updated?

Update my file and directory listing as objects are added to my S3 bucket

Update my file and directory listing as objects are added to or changed in my S3 bucket

Update my file and directory listing as objects are added to, changed in, or deleted from my S3 bucket

Do not update my file and directory listing when objects are added to or changed in my S3 bucket

Import bucket

s3://my-bucket

The name of an existing S3 bucket

Import prefix - optional [Info](#)

s3-import-prefix/

The prefix containing the data to import

Export prefix [Info](#)

The prefix to which data is exported

A unique prefix that FSx creates in your bucket

The same prefix that you imported from (replace existing objects with updated ones)

A prefix you specify

FSxLustre20211123T184808Z

6. Pilih bagaimana Amazon FSx memperbarui daftar file dan direktori Anda saat Anda menambahkan atau memodifikasi objek dalam bucket S3 Anda. Ketika Anda membuat sistem file Anda, objek S3 yang ada muncul sebagai daftar file dan direktori.
 - Perbarui daftar file dan direktori saya saat objek ditambahkan ke bucket S3 saya: (Default) Amazon FSx secara otomatis memperbarui daftar file dan direktori dari setiap objek baru yang ditambahkan ke bucket S3 terkait yang saat ini tidak ada di sistem file FSx. Amazon

FSx tidak memperbarui daftar untuk objek yang telah berubah di bucket S3. Amazon FSx tidak menghapus daftar objek yang dihapus dalam bucket S3.

 Note

Pengaturan preferensi impor default untuk mengimpor data dari bucket S3 tertaut menggunakan CLI dan API adalah NONE. Pengaturan preferensi impor default saat menggunakan konsol adalah memperbarui Lustre karena objek baru ditambahkan ke bucket S3.

- Perbarui daftar file dan direktori saya saat objek ditambahkan atau diubah di bucket S3 saya: Amazon FSx secara otomatis memperbarui daftar file dan direktori dari setiap objek baru yang ditambahkan ke bucket S3 dan objek yang ada yang diubah dalam bucket S3 setelah Anda memilih opsi ini. Amazon FSx tidak menghapus daftar objek yang dihapus dalam bucket S3.
 - Perbarui daftar file dan direktori saya saat objek ditambahkan, diubah, atau dihapus dari bucket S3 saya: Amazon FSx secara otomatis memperbarui daftar file dan direktori dari setiap objek baru yang ditambahkan ke bucket S3, objek yang ada yang diubah dalam bucket S3, dan objek apa pun yang ada yang dihapus di bucket S3 setelah Anda memilih opsi ini.
 - Jangan perbarui file saya dan daftar langsung saat objek ditambahkan, diubah, atau dihapus dari bucket S3 saya- Amazon FSx hanya memperbarui daftar file dan direktori dari bucket S3 yang ditautkan saat sistem file dibuat. FSx tidak memperbarui daftar file dan direktori untuk objek baru, diubah, atau dihapus setelah memilih opsi ini.
7. Masukkan prefiks impor opsional jika Anda ingin mengimpor hanya beberapa daftar file dan direktori data dalam bucket S3 Anda ke dalam sistem file Anda. Prefiks impor menentukan tempat di bucket S3 yang menjadi sumber pengimporan data. Untuk informasi selengkapnya, lihat [Secara otomatis mengimpor pembaruan dari bucket S3](#).
8. Pilih salah satu yang tersediaAwalan eksporPilihan:
- Awalan unik yang dibuat Amazon FSx di bucket Anda: Pilih opsi ini untuk mengekspor objek baru dan diubah menggunakan awalan yang dihasilkan oleh FSx untuk Lustre. Kode prefiks terlihat seperti ini: /FSxLustre*file-system-creation- timestamp*. Stempel waktu dalam format UTC, misalnya FSxLustre20181105T222312Z.
 - Awalan yang sama yang Anda impor dari (ganti objek yang ada dengan yang diperbarui): Pilih opsi ini untuk mengganti objek yang ada dengan yang diperbarui.

- Awalan yang Anda tentukan: Pilih opsi ini untuk menyimpan data yang diimpor dan mengekspor objek baru dan diubah menggunakan awalan yang Anda tentukan. Untuk mencapai pemetaan 1:1 saat mengekspor data ke bucket S3, pilih opsi ini dan biarkan bidang prefiks kosong. FSx akan mengekspor data ke direktori yang sama yang darinya direktori tersebut diimpor.
9. (Opsional) Atur Preferensi pemeliharaan, atau gunakan default sistem.
 10. Pilih Selanjutnya, dan tinjau pengaturan sistem file. Buat perubahan jika diperlukan.
 11. Pilih Buat sistem file.

AWS CLI

Contoh berikut membuat sistem file Amazon FSx yang ditautkan ke `lustre-export-test-bucket`, dengan preferensi impor yang mengimpor file baru, diubah, dan dihapus dalam repositori data terkait setelah sistem file dibuat.

Note

Pengaturan preferensi impor default untuk mengimpor data dari bucket S3 tertaut menggunakan CLI dan API adalah NONE, yang berbeda dari perilaku default saat menggunakan konsol.

Untuk membuat sistem file FSx for Lustre, gunakan perintah Amazon FSx CLI [create-file-system](#), seperti yang ditunjukkan di bawah ini. Operasi API yang sesuai adalah [CreateFileSystem](#).

```
$ aws fsx create-file-system \
--client-request-token CRT1234 \
--file-system-type LUSTRE \
--file-system-type-version 2.10 \
--lustre-configuration
AutoImportPolicy=NEW_CHANGED_DELETED,DeploymentType=SCRATCH_1,ImportPath=s
3://lustre-export-test-bucket/,ExportPath=s3://lustre-export-test-bucket/export,
PerUnitStorageThroughput=50 \
--storage-capacity 2400 \
--subnet-ids subnet-123456 \
--tags Key=Name,Value=Lustre-TEST-1 \
--region us-east-2
```

Setelah Anda berhasil membuat sistem file, Amazon FSx mengembalikan deskripsi sistem file sebagai JSON, seperti yang ditunjukkan pada contoh berikut.

```
{
  "FileSystems": [
    {
      "OwnerId": "owner-id-string",
      "CreationTime": 1549310341.483,
      "FileSystemId": "fs-0123456789abcdef0",
      "FileSystemType": "LUSTRE",
      "FileSystemTypeVersion": "2.10",
      "Lifecycle": "CREATING",
      "StorageCapacity": 2400,
      "VpcId": "vpc-123456",
      "SubnetIds": [
        "subnet-123456"
      ],
      "NetworkInterfaceIds": [
        "eni-039fcf55123456789"
      ],
      "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
      "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
      "Tags": [
        {
          "Key": "Name",
          "Value": "Lustre-TEST-1"
        }
      ],
      "LustreConfiguration": {
        "DeploymentType": "PERSISTENT_1",
        "DataRepositoryConfiguration": {
          "AutoImportPolicy": "NEW_CHANGED_DELETED",
          "Lifecycle": "UPDATING",
          "ImportPath": "s3://lustre-export-test-bucket/",
          "ExportPath": "s3://lustre-export-test-bucket/export",
          "ImportedFileChunkSize": 1024
        },
        "PerUnitStorageThroughput": 50
      }
    }
  ]
}
```

Melihat jalur ekspor sistem file

Anda dapat melihat jalur ekspor sistem file menggunakan konsol FSx for Lustre, AWS CLI, dan API.

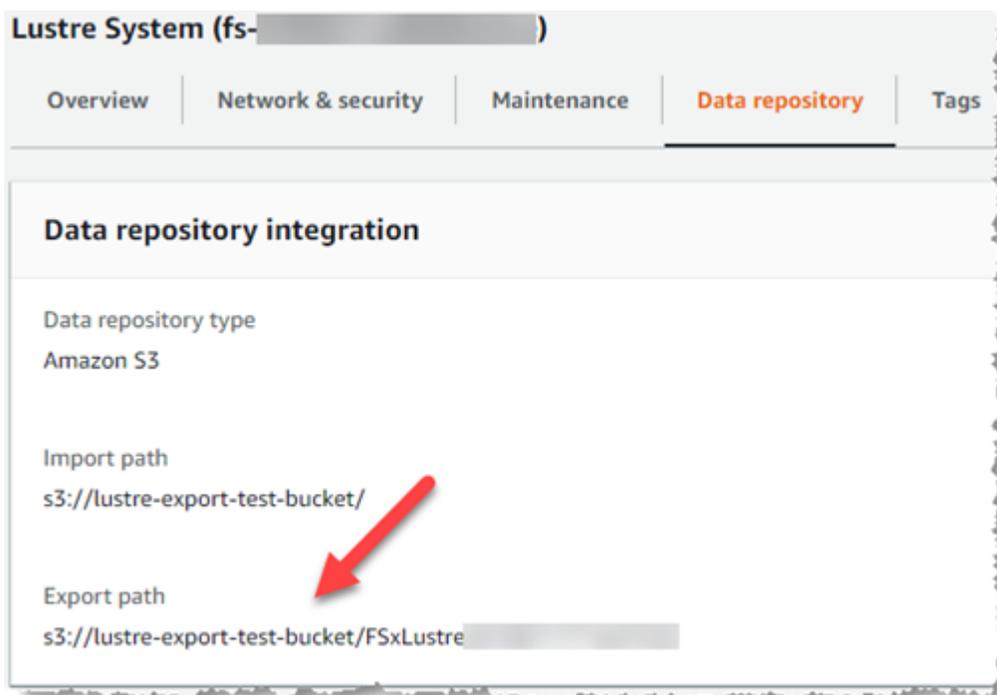
Console

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>
2. Pilih Nama sistem file atau ID sistem file untuk FSx untuk sistem file Lustre yang ingin Anda lihat jalur ekspor.

Halaman detail sistem file muncul untuk sistem file tersebut.

3. Pilih tab Repositori data.

Panel Integrasi repositori data muncul, menampilkan jalur impor dan ekspor.



CLI

Untuk menentukan jalur ekspor untuk sistem file Anda, gunakan [describe-file-systems](#) AWS Perintah CLI.

```
aws fsx describe-file-systems
```

Cari properti `ExportPath` di bawah `LustreConfiguration` dalam respons.

```

{
  "OwnerId": "111122223333",
  "CreationTime": 1563382847.014,
  "FileSystemId": "",
  "FileSystemType": "LUSTRE",
  "Lifecycle": "AVAILABLE",
  "StorageCapacity": 2400,
  "VpcId": "vpc-6296a00a",
  "SubnetIds": [
    "subnet-11111111"
  ],
  "NetworkInterfaceIds": [
    "eni-0c288d5b8cc06c82d",
    "eni-0f38b702442c6918c"
  ],
  "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
  "ResourceARN": "arn:aws:fsx:us-east-2:267731178466:file-system/fs-0123456789abcdef0",
  "Tags": [
    {
      "Key": "Name",
      "Value": "Lustre System"
    }
  ],
  "LustreConfiguration": {
    "DeploymentType": "SCRATCH_1",
    "DataRepositoryConfiguration": {
      "AutoImportPolicy": "NEW_CHANGED_DELETED",
      "Lifecycle": "AVAILABLE",
      "ImportPath": "s3://lustre-export-test-bucket/",
      "ExportPath": "s3://lustre-export-test-bucket/FSxLustre20190717T164753Z",
      "ImportedFileChunkSize": 1024
    }
  },
  "PerUnitStorageThroughput": 50,
  "WeeklyMaintenanceStartTime": "6:09:30"
}

```

Kondisi siklus hidup repositori data

Kondisi siklus hidup repositori data memberikan informasi kondisi repositori data terkait sistem file. Sebuah repositori data dapat memiliki status Siklus Hidup berikut.

- **Menciptakan:** Amazon FSx membuat konfigurasi repositori data antara sistem file dan repositori data yang ditautkan. Repositori data tidak tersedia.
- **Tersedia:** Repositori data tersedia untuk digunakan.
- **Memperbarui:** Konfigurasi repositori data sedang menjalani pembaruan yang diprakarsai pelanggan yang mungkin memengaruhi ketersediaannya.
- **Salah konfigurasi:** Amazon FSx tidak dapat secara otomatis mengimpor pembaruan dari bucket S3 hingga konfigurasi repositori data diperbaiki. Untuk informasi selengkapnya, lihat [Memecahkan masalah bucket S3 terkait yang salah dikonfigurasi](#).

Anda dapat melihat status siklus hidup repositori data terkait sistem file menggunakan konsol Amazon FSx, AWS Antarmuka Baris Perintah, dan API Amazon FSx. Di konsol Amazon FSx, Anda dapat mengakses repositori data Status siklus hidup di dalam Integrasi Repositori Datapanel dari Repositori Data tab untuk sistem file. Properti Lifecycle terletak di objek DataRepositoryConfiguration dalam respon dari perintah CLI [describe-file-systems](#) (tindakan API setara adalah [DescribeFileSystems](#)).

Secara otomatis mengimpor pembaruan dari bucket S3

Secara default, saat Anda membuat sistem file baru, Amazon FSx mengimpor metadata file (nama, kepemilikan, stempel waktu, dan izin) objek dalam bucket S3 terkait pada pembuatan sistem file. Anda dapat mengonfigurasi sistem file FSx untuk Lustre untuk secara otomatis mengimpor metadata objek yang ditambahkan, diubah, atau dihapus dari bucket S3 Anda setelah pembuatan sistem file. FSx untuk Lustre update file dan direktori daftar objek berubah setelah penciptaan dengan cara yang sama seperti mengimpor file metadata pada penciptaan sistem file. Ketika Amazon FSx memperbarui daftar file dan direktori dari objek yang berubah, jika objek yang berubah dalam bucket S3 tidak lagi berisi metadata, Amazon FSx mempertahankan nilai metadata saat ini dari file tersebut, daripada menggunakan izin default.

Note

Pengaturan impor tersedia di FSx untuk sistem file Lustre yang dibuat setelah pukul 15:00 EDT, 23 Juli 2020.

Anda dapat mengatur preferensi impor saat membuat sistem file baru, dan Anda dapat memperbarui pengaturan pada sistem file yang ada menggunakan konsol manajemen FSx, AWS CLI, dan AWS API. Ketika Anda membuat sistem file Anda, objek S3 yang ada muncul sebagai daftar file dan direktori.

Setelah Anda membuat sistem file Anda, bagaimana Anda ingin memperbaruinya ketika isi dari bucket S3 diperbarui? Sistem file dapat memiliki salah satu preferensi Impor berikut:

 Note

FSx untuk sistem file Lustre dan bucket S3 yang terkait harus terletak di samaAWSWilayah untuk secara otomatis mengimpor pembaruan.

- Perbarui daftar file dan direktori saya saat objek ditambahkan ke bucket S3 saya: (Default) Amazon FSx secara otomatis memperbarui daftar file dan direktori dari setiap objek baru yang ditambahkan ke bucket S3 terkait yang saat ini tidak ada di sistem file FSx. Amazon FSx tidak memperbarui daftar untuk objek yang telah berubah di bucket S3. Amazon FSx tidak menghapus daftar objek yang dihapus dalam bucket S3.

 Note

Pengaturan preferensi impor default untuk mengimpor data dari bucket S3 tertaut menggunakan CLI dan API adalah NONE. Pengaturan preferensi impor default saat menggunakan konsol adalah memperbarui Lustre karena objek baru ditambahkan ke bucket S3.

- Perbarui daftar file dan direktori saya saat objek ditambahkan atau diubah di bucket S3 saya: Amazon FSx secara otomatis memperbarui daftar file dan direktori dari setiap objek baru yang ditambahkan ke bucket S3 dan objek yang ada yang diubah dalam bucket S3 setelah Anda memilih opsi ini. Amazon FSx tidak menghapus daftar objek yang dihapus dalam bucket S3.
- Perbarui daftar file dan direktori saya saat objek ditambahkan, diubah, atau dihapus dari bucket S3 saya: Amazon FSx secara otomatis memperbarui daftar file dan direktori dari setiap objek baru yang ditambahkan ke bucket S3, objek yang ada yang diubah dalam bucket S3, dan objek apa pun yang ada yang dihapus di bucket S3 setelah Anda memilih opsi ini.
- Jangan perbarui file saya dan daftar langsung saat objek ditambahkan, diubah, atau dihapus dari bucket S3 saya- Amazon FSx hanya memperbarui daftar file dan direktori dari bucket S3 yang ditautkan saat sistem file dibuat. FSx tidak memperbarui daftar file dan direktori untuk objek baru, diubah, atau dihapus setelah memilih opsi ini.

Ketika Anda mengatur preferensi impor untuk memperbarui daftar file dan direktori file sistem saya berdasarkan perubahan dalam bucket S3 terkait, Amazon FSx membuat konfigurasi pemberitahuan

acara pada bucket S3 terkait bernama FSx. Jangan memodifikasi atau menghapus FSx Konfigurasi pemberitahuan peristiwa pada bucket S3 — dengan demikian mencegah impor otomatis daftar file dan direktori baru atau yang diubah ke sistem file Anda.

Ketika Amazon FSx memperbarui daftar file yang telah berubah pada bucket S3 terkait, itu akan menimpa file lokal dengan versi terbaru, bahkan jika file tersebut dikunci untuk penulisan. Demikian pula, ketika Amazon FSx memperbarui daftar file ketika objek yang sesuai telah dihapus pada bucket S3 yang ditautkan, ia akan menghapus file lokal, bahkan jika file tersebut dikunci secara tulis.

Amazon FSx berusaha sebaik mungkin untuk memperbarui sistem file Anda. Amazon FSx tidak dapat memperbarui sistem file dengan perubahan dalam situasi berikut:

- Ketika Amazon FSx tidak memiliki izin untuk membuka objek S3 yang diubah atau baru.
- Ketika FSx konfigurasi pemberitahuan peristiwa pada bucket S3 terkait dihapus atau diubah.

Salah satu dari kondisi ini menyebabkan status siklus hidup repositori data menjadi Salah konfigurasi. Untuk informasi selengkapnya, lihat [Kondisi siklus hidup repositori data](#).

Prasyarat

Kondisi berikut diperlukan untuk Amazon FSx untuk secara otomatis mengimpor file baru, diubah, atau dihapus dari bucket S3 yang ditautkan:

- Sistem file dan bucket S3 yang terkait harus berada di tempat yang sama AWS Wilayah.
- Bucket S3 tidak memiliki Kondisi siklus hidup yang konfigurasinya salah. Untuk informasi selengkapnya, lihat [Kondisi siklus hidup repositori data](#).
- Akun Anda harus memiliki izin yang diperlukan untuk mengonfigurasi dan menerima pemberitahuan peristiwa pada bucket S3 yang ditautkan.

Jenis perubahan file yang didukung

Amazon FSx mendukung pengimporan perubahan berikut ke file dan folder yang terjadi di bucket S3 terkait:

- Perubahan isi file
- Perubahan metadata file atau folder
- Perubahan target symlink atau metadata

Memperbarui preferensi impor

Anda dapat mengatur preferensi impor sistem file saat membuat sistem file baru. Untuk informasi selengkapnya, lihat [Menautkan sistem file Anda ke bucket S3](#).

Anda juga dapat memperbarui preferensi impor sistem file setelah dibuat menggunakan AWS Management Console, AWS CLI, dan Amazon FSx API, seperti yang ditunjukkan dalam prosedur berikut.

Console

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Dari dasbor, pilih Sistem file.
3. Pilih sistem file yang ingin Anda kelola untuk menampilkan detail sistem file.
4. Pilih Repositori data untuk melihat pengaturan repositori data. Anda dapat mengubah preferensi impor jika kondisi siklus hidup TERSEDIA atau SALAH KONFIGURASI. Untuk informasi selengkapnya, lihat [Kondisi siklus hidup repositori data](#).
5. Pilih Tindakan, lalu pilih Perbarui preferensi impor untuk menampilkan kotak dialog Perbarui preferensi impor.
6. Pilih pengaturan baru, lalu pilih **Memperbarui** untuk membuat perubahan.

CLI

Untuk memperbarui preferensi impor, gunakan perintah CLI [update-file-system](#). Operasi API yang sesuai adalah [UpdateFileSystem](#).

Setelah Anda berhasil memperbarui sistem file `AutoImportPolicy`, Amazon FSx mengembalikan deskripsi sistem file yang diperbarui sebagai JSON, seperti yang ditunjukkan di sini:

```
{
  "FileSystems": [
    {
      "OwnerId": "111122223333",
      "CreationTime": 1549310341.483,
      "FileSystemId": "fs-0123456789abcdef0",
      "FileSystemType": "LUSTRE",
      "Lifecycle": "UPDATING",
      "StorageCapacity": 2400,
    }
  ]
}
```

```
"VpcId": "vpc-123456",
"SubnetIds": [
  "subnet-123456"
],
"NetworkInterfaceIds": [
  "eni-039fcf55123456789"
],
"DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
"ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
"Tags": [
  {
    "Key": "Name",
    "Value": "Lustre-TEST-1"
  }
],
"LustreConfiguration": {
  "DeploymentType": "SCRATCH_1",
  "DataRepositoryConfiguration": {
    "AutoImportPolicy": "NEW_CHANGED_DELETED",
    "Lifecycle": "UPDATING",
    "ImportPath": "s3://lustre-export-test-bucket/",
    "ExportPath": "s3://lustre-export-test-bucket/export",
    "ImportedFileChunkSize": 1024
  }
  "PerUnitStorageThroughput": 50,
  "WeeklyMaintenanceStartTime": "2:04:30"
}
]
}
```

Performa Amazon FSx for Lustre

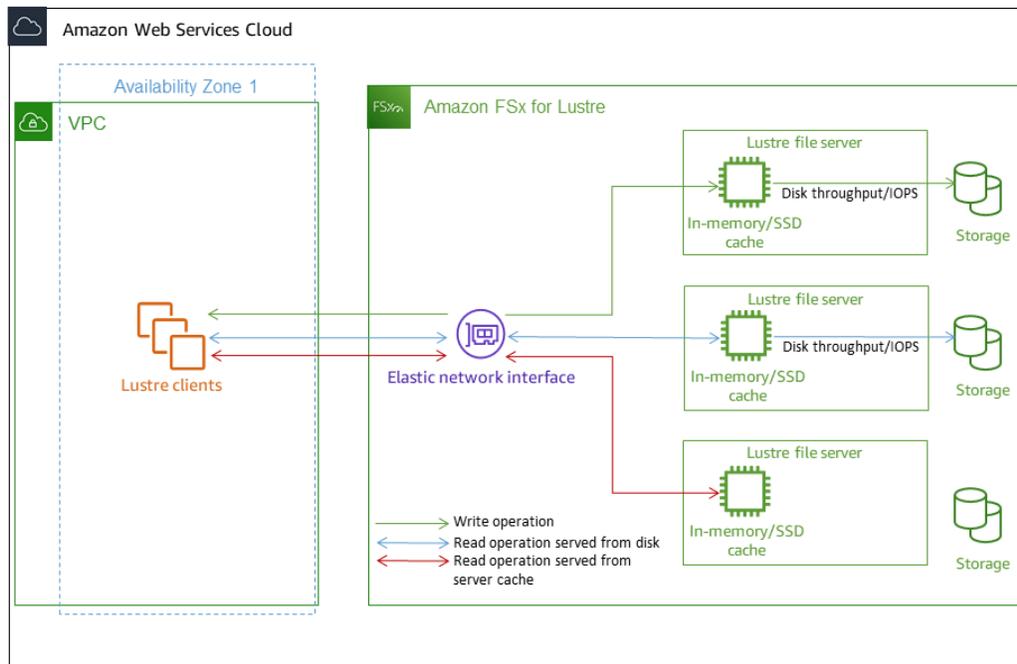
Amazon FSx for Lustre, dibangun di atas Lustre, sistem file dengan performa tinggi yang populer, memberikan kinerja penguatan yang meningkat secara linear berdasarkan ukuran sistem file. Sistem file Lustre terskala secara horizontal di beberapa server file dan disk. Penskalaan ini memberikan setiap klien akses langsung ke data yang disimpan pada setiap disk untuk menghapus banyaknya kemacetan yang ada dalam sistem file tradisional. Amazon FSx for Lustre dibangun di atas arsitektur Lustre yang dapat diskalakan untuk men-support performa tingkat tinggi di seluruh klien yang jumlahnya sangat banyak.

Topik

- [Cara kerja sistem file FSx for Lustre](#)
- [Performa kumpulan sistem file](#)
- [Kinerja metadata sistem file](#)
- [Layout penyimpanan sistem file](#)
- [Sedang melakukan stripe data di sistem file Anda](#)
- [Memantau performa dan penggunaan](#)
- [Tips performa](#)

Cara kerja sistem file FSx for Lustre

Setiap sistem file FSx for Lustre terdiri dari server file yang berkomunikasi dengan klien, dan satu set disk yang dilampirkan ke setiap server file yang menyimpan data Anda. Setiap server file menggunakan cache dalam memori untuk meningkatkan performa untuk data yang diakses paling sering. Sistem file berbasis HDD juga dapat disediakan dengan cache baca berbasis SSD untuk lebih meningkatkan performa untuk data yang paling sering diakses. Ketika klien mengakses data yang disimpan di cache dalam memori atau cache SSD, server file tidak perlu membacanya dari disk, yang mana akan mengurangi latensi dan meningkatkan jumlah total throughput yang dapat Anda drive. Diagram berikut menggambarkan jalur operasi tulis, operasi baca yang disajikan dari disk, dan operasi baca yang disajikan dari cache dalam memori atau SSD.



Ketika Anda membaca data yang disimpan di cache dalam-memori atau cache SSD pada server file, performa sistem file ditentukan oleh throughput jaringan. Ketika Anda menulis data ke sistem file Anda, atau ketika Anda membaca data yang tidak disimpan pada cache dalam memori, kinerja sistem file ditentukan oleh yang lebih rendah dari throughput jaringan dan throughput disk.

Saat Anda menyediakan sistem file HDD Lustre dengan cache SSD, Amazon FSx membuat cache SSD yang secara otomatis berukuran hingga 20 persen dari kapasitas penyimpanan HDD sistem file. Melakukan hal ini memberikan latensi sub-milidetik dan IOPS yang lebih tinggi untuk file yang sering diakses.

Performa kumpulan sistem file

Throughput yang didukung oleh sistem file FSx for Lustre sebanding dengan kapasitas penyimpanannya. Sistem file Amazon FSx for Lustre meningkat skala-nya hingga ratusan GBps throughput dan jutaan IOPS. Amazon FSx for Lustre juga men-support akses bersamaan ke file atau direktori yang sama dari ribuan instans komputasi. Akses ini mengaktifkan checkpointing data cepat dari memori aplikasi ke penyimpanan, yang merupakan teknik umum dalam komputasi performa tinggi (HPC). Anda dapat meningkatkan jumlah penyimpanan dan kapasitas throughput

yang diperlukan setiap saat setelah Anda membuat sistem file. Untuk informasi selengkapnya, lihat [Mengelola kapasitas penyimpanan](#).

Sistem file FSx for Lustre menyediakan throughput burst read menggunakan mekanisme kredit I/O jaringan untuk mengalokasikan bandwidth jaringan berdasarkan pemanfaatan bandwidth rata-rata. Sistem-sistem file memperoleh kredit ketika penggunaan bandwidth jaringan mereka di bawah batas baseline, dan dapat menggunakan kredit ini ketika sistem-sistem file melaksanakan transfer data jaringan.

Tabel berikut menunjukkan kinerja yang dirancang untuk opsi penyebaran FSx for Lustre.

Performa sistem file untuk pilihan penyimpanan SSD

Jenis Deployment	Throughput jaringan (MB/s/ Tib penyimpanan disediakan)	IOPS Jaringan (IOPS/TIB penyimpanan an disediakan)	Penyimpanan an cache (GiB RAM/Tib penyimpanan an disediakan)	Latensi disk per operasi file (mildetik, P50)	Throughput disk (MBPS/Tib penyimpanan atau cache SSD disediakan)
	Baseline	Meledak			Baseline
SCRATCH_2	200	1300	Puluhan ribu baseline	6.7	200 (baca) 100 (tuliskan)
PERSISTEN -125	320	1300	Ratusan ribu burst	3.4	125 500
PERSISTEN -250	640	1300		6.8	250 500
PERSISTEN -500	1300	-		13.7	500 -
PERSISTEN -1000	2600	-		27.3	1000 -

Performa sistem file untuk opsi penyimpanan HDD

Jenis Deployment	Throughput jaringan (MB/s/Tib penyimpanan atau cache SSD disediakan)	IOPS Jaringan (IOPS/TIB penyimpanan disediakan)	Penyimpanan an cache (GiB RAM/Tib penyimpanan an disediakan)	Latensi disk per operasi file (mildetik, P50)	Throughput disk (MBPS/Tib penyimpanan atau cache SSD disediakan)
	Baseline	Meledak			Baseline
PERSISTENT-12					
Penyimpanan an HDD	40	375*	Memori 0,4	Metadata: sub-ms Data: ms ber-digit tunggal	80 (baca) 50 (tuliskan)
Cache baca SSD	200	1.900	200 cache SSD	Data: sub-ms	-
PERSISTENT-40					
Penyimpanan an HDD	150	1.300*	1.5	Metadata: sub-ms Data: ms ber-digit tunggal	250 (baca) 150 (tuliskan)
Cache baca SSD	750	6500	200 cache SSD	Data: sub-ms	-

Kinerja sistem file untuk opsi penyimpanan SSD generasi sebelumnya

Jenis Deployment	Throughput jaringan (MB/s per TiB penyimpanan yang disediakan)	IOPS Jaringan (IOPS per TiB penyimpanan an yang disediakan)	Penyimpanan an cache (GiB per TiB penyimpanan an disediakan)	Latensi disk per operasi file (mildeti k, P50)	Throughput disk (MB/s per TiB penyimpanan atau cache SSD disediakan)
	Baseline	Meledak			Baseline
PERSISTEN T-50	250	1.300*	Puluhan ribu baseline	Metadata: sub-ms	50
PERSISTEN T-100	500	1.300*	Ratusan ribu burst	Data: sub-ms	100
PERSISTEN T-200	750	1.300*	8,8 RAM		200
					240

Note

* Sistem file persisten berikut ini Wilayah AWS menyediakan ledakan jaringan hingga 530 MB/s per TiB penyimpanan: Afrika (Cape Town), Asia Pasifik (Hong Kong), Asia Pasifik (Osaka), Asia Pasifik (Singapura), Kanada (Tengah), Eropa (Frankfurt), Eropa (London), Eropa (Milan), Eropa (Stockholm), Timur Tengah (Bahrain), Amerika Selatan (São Paulo), China, dan AS Barat (Los Angeles).

Contoh: Agregat baseline dan burst throughput

Contoh berikut menggambarkan bagaimana kapasitas penyimpanan dan throughput disk mempengaruhi performa sistem file.

Sistem file persisten dengan kapasitas penyimpanan 4,8 TiB dan 50 MB/s per TiB throughput per unit penyimpanan menyediakan throughput disk dasar agregat 240 MB/s dan throughput disk burst 1,152 Gb/s.

Terlepas dari ukuran sistem file, Amazon FSx for Lustre menyediakan latensi sub-milidetik yang konsisten untuk operasi file.

Kinerja metadata sistem file

Sistem file metadata operasi IO per detik (IOPS) menentukan jumlah file dan direktori yang dapat Anda buat, daftar, baca, dan hapus per detik. Metadata IOPS secara otomatis disediakan pada sistem file FSx for Lustre berdasarkan kapasitas penyimpanan yang Anda berikan.

Sistem file Persistent_2 memungkinkan Anda untuk menyediakan Metadata IOPS independen dari kapasitas penyimpanan dan memberikan peningkatan visibilitas ke dalam jumlah dan jenis metadata yang ditargetkan oleh instans klien IOPS di sistem file Anda.

Dengan sistem file FSx for Lustre Persistent_2, jumlah IOPS metadata yang Anda sediakan dan jenis operasi metadata menentukan tingkat operasi metadata yang dapat didukung oleh sistem file Anda. Tingkat IOPS metadata yang Anda berikan menentukan jumlah IOPS yang disediakan untuk disk metadata sistem file Anda.

Jenis operasi	Operasi yang dapat Anda kendarai per detik untuk setiap metadata yang disediakan IOPS
Buat File, Buka	2
Hapus File	1
Direktori Buat, Ganti Nama	0.1
Direktori Hapus	0,2

Anda dapat memilih untuk menyediakan IOPS metadata menggunakan mode Otomatis atau mode yang disediakan pengguna. Dalam mode Otomatis, Amazon FSx secara otomatis menyediakan IOPS metadata berdasarkan kapasitas penyimpanan sistem file Anda sesuai dengan tabel di bawah ini:

Kapasitas penyimpanan sistem file	Termasuk metadata IOPS dalam mode Otomatis
1200 GiB	1500
2400 GiB	3000
4800—9600 GiB	6000
12000—45600 GiB	12000
≥48000 GiB	12000 IOPS per 24000 GiB

Dalam mode yang disediakan pengguna, Anda dapat memilih untuk menentukan jumlah IOPS metadata yang akan disediakan. Anda membayar Metadata IOPS yang disediakan di atas nomor default Metadata IOPS untuk sistem file Anda.

Layout penyimpanan sistem file

Semua data file di Lustre disimpan di volume penyimpanan yang disebut target penyimpanan objek (OST). Semua metadata file (termasuk nama file, timestamp, izin, dan lainnya) disimpan di volume penyimpanan yang disebut target metadata (MDT). Sistem file Amazon FSx for Lustre terdiri dari

satu atau lebih MDT dan beberapa OST. Setiap OST berukuran sekitar 1 hingga 2 TiB, tergantung dari jenis deployment sistem file. Amazon FSx for Lustre menyebarkan data file Anda ke seluruh OST yang membentuk sistem file Anda untuk menyeimbangkan kapasitas penyimpanan dengan throughput dan beban IOPS.

Untuk melihat penggunaan penyimpanan MDT dan OST yang membentuk sistem file Anda, jalankan perintah berikut dari client yang sistem file-nya sudah terpasang.

```
lfs df -h mount/path
```

Hasil akhir dari perintah ini adalah sebagai berikut.

Example

UUID	bytes	Used	Available	Use%	Mounted on
<i>mountname</i> -MDT0000_UUID	68.7G	5.4M	68.7G	0%	/fsx[MDT:0]
<i>mountname</i> -OST0000_UUID	1.1T	4.5M	1.1T	0%	/fsx[OST:0]
<i>mountname</i> -OST0001_UUID	1.1T	4.5M	1.1T	0%	/fsx[OST:1]
filesystem_summary:	2.2T	9.0M	2.2T	0%	/fsx

Sedang melakukan stripe data di sistem file Anda

Anda dapat mengoptimalkan performa throughput sistem file Anda dengan melakukan file striping. Amazon FSx for Lustre secara otomatis menyebarkan file-file ke seluruh OST untuk memastikan bahwa data dilayani dari semua server penyimpanan. Anda dapat menerapkan konsep yang sama di tingkat file dengan mengonfigurasi bagaimana file-file di-stripe di beberapa OST.

Striping artinya bahwa file-file dapat dibagi menjadi beberapa potongan yang kemudian disimpan di seluruh OST yang berbeda. Ketika sebuah file di-stripe di beberapa OST, pembacaan atau penulisan permintaan ke file tersebar di OST-OST tersebut, meningkatkan throughput agregat atau IOPS yang aplikasi Anda dapat melakukan drive melaluinya.

Berikut ini adalah layout default untuk sistem file Amazon FSx for Lustre.

- Untuk sistem file yang dibuat sebelum 18 Desember 2020, tata letak default menentukan jumlah garis 1. Ini berarti bahwa kecuali sebuah layout yang berbeda ditentukan, setiap file yang dibuat di Amazon FSx for Lustre menggunakan alat-alat Linux standar disimpan di sebuah disk.

- Untuk sistem file yang dibuat setelah 18 Desember 2020, tata letak default adalah tata letak file progresif di mana file di bawah ukuran 1GiB disimpan dalam satu garis, dan file yang lebih besar diberi jumlah garis 5.
- Untuk sistem file yang dibuat setelah 25 Agustus 2023, tata letak default adalah tata letak file progresif 4 komponen yang dijelaskan di [Layout file progresif](#)
- Untuk semua sistem file terlepas dari tanggal pembuatannya, file yang diimpor dari Amazon S3 tidak menggunakan tata letak default, melainkan menggunakan tata letak dalam parameter sistem file. ImportedFileChunkSize File-file yang diimpor dari S3 yang lebih besar dari ImportedFileChunkSize akan disimpan di beberapa OST dengan jumlah stripe sebanyak $(\text{FileSize} / \text{ImportedFileChunksize}) + 1$. Nilai default dari ImportedFileChunkSize adalah 1GiB.

Anda dapat melihat konfigurasi layout dari sebuah file atau direktori menggunakan perintah `lfs getstripe`.

```
lfs getstripe path/to/filename
```

Perintah ini melaporkan jumlah stripe dari file, ukuran stripe, dan offset stripe. Jumlah stripe adalah seberapa banyak OST file yang di-stripe. Ukuran stripe adalah seberapa banyak data berkelanjutan yang disimpan dalam sebuah OST. Offset stripe adalah indeks OST pertama tempat file di-stripe.

Memodifikasi konfigurasi striping Anda

Parameter layout dari sebuah file diatur ketika file pertama kali dibuat. Gunakan perintah `lfs setstripe` untuk membuat sebuah file yang baru, kosong dengan layout yang telah ditentukan.

```
lfs setstripe filename --stripe-count number_of OSTs
```

Perintah `lfs setstripe` mempengaruhi hanya layout dari sebuah file baru. Gunakan perintah tersebut untuk menentukan layout sebuah file sebelum Anda membuatnya. Anda juga dapat menentukan layout untuk sebuah direktori. Setelah ditetapkan pada sebuah direktori, layout diterapkan ke setiap file baru yang ditambahkan ke direktori tersebut, tetapi tidak ke file yang sudah ada. Setiap subdirektori baru yang Anda buat juga mewarisi layout baru, yang kemudian diterapkan ke setiap file atau direktori baru yang Anda buat dalam subdirektori tersebut.

Untuk memodifikasi layout dari file yang ada, gunakan perintah `lfs migrate`. Perintah ini menyalin file sebagaimana diperlukan untuk mendistribusikan isinya berdasarkan layout yang Anda tentukan

di perintah. Misalnya, file-file yang ditambahkan atau ditingkatkan ukurannya tidak akan mengubah jumlah stripe, jadi Anda harus me-migrasi file-file untuk mengubah layout file. Atau, Anda dapat membuat file baru menggunakan perintah `lfs setstripe` untuk menentukan layout-nya, menyalin konten semula ke file yang baru, dan kemudian mengubah nama file yang baru untuk mengganti file semula.

Mungkin ada kasus-kasus di mana konfigurasi layout default tidak optimal untuk beban kerja Anda. Sebagai contoh, sistem file dengan puluhan OST dan sejumlah besar file berukuran multi-gigabyte bisa memiliki performa yang lebih tinggi dengan melakukan stripe file lebih dari nilai jumlah stripe default dari lima OST. Membuat file-file besar dengan jumlah stripe yang rendah dapat menyebabkan kemacetan performa I/O dan juga dapat menyebabkan OST penuh. Dalam hal ini, Anda dapat membuat sebuah direktori dengan jumlah stripe yang lebih besar untuk file-file ini.

Mengatur layout yang ditetapkan stripe-nya untuk file-file besar (terutama file-file yang lebih besar dari ukuran gigabyte) adalah penting karena alasan-alasan berikut ini:

- Tingkatkan throughput dengan mengizinkan beberapa OST dan server mereka yang ter-associate untuk berkontribusi IOPS, bandwidth jaringan, dan sumber daya CPU saat membaca dan menulis file besar.
- Mengurangi kemungkinan subset kecil dari OST menjadi hot spot yang membatasi performa beban kerja secara keseluruhan.
- Mencegah satu file tunggal besar mengisi OST, yang berpotensi menyebabkan error disk penuh.

Tidak ada konfigurasi layout optimal tunggal untuk semua kasus penggunaan. Untuk panduan mendetail tentang layout file, lihat [Mengelola Layout File \(Melakukan Stripe\) dan Ruang Bebas](#) dalam dokumentasi Lustre.org. Berikut ini adalah pedoman umum:

- Layout yang sudah ditentukan stripe-nya adalah masalah bagi file-file besar, terutama dalam kasus penggunaan di mana file-file secara rutin memiliki ukuran ratusan megabyte atau lebih. Untuk alasan ini, layout default untuk sistem file baru menetapkan jumlah stripe sebanyak lima untuk file-file di atas ukuran 1GiB.
- Jumlah Stripe adalah parameter layout yang harus Anda sesuaikan untuk sistem yang men-support file-file besar. Jumlah stripe menentukan jumlah volume OST yang akan menyimpan potongan file yang memiliki stripe. Misalnya, dengan jumlah stripe sebanyak 2 dan sebuah stripe berukuran 1MiB, Lustre menuliskan potongan file 1MiB alternatif ke tiap-tiap dari dua OST.

- Jumlah stripe yang efektif adalah lebih sedikit dari jumlah volume OST yang sebenarnya dan nilai jumlah stripe yang Anda tentukan. Anda dapat menggunakan nilai jumlah stripe sebanyak -1 untuk menunjukkan bahwa stripe harus ditempatkan di semua volume OST.
- Mengatur jumlah stripe yang besar untuk file-file kecil adalah hal yang kurang optimal karena untuk operasi-operasi tertentu Lustre perlu melakukan perjalanan bolak-balik jaringan ke setiap OST di layout, bahkan jika file terlalu kecil untuk menghabiskan ruang di semua volume OST.
- Anda dapat mengatur layout file progresif (PFL) yang mengizinkan layout sebuah file berubah-ubah sesuai ukuran. Konfigurasi PFL dapat menyederhanakan pengelolaan sebuah sistem file yang memiliki kombinasi file besar dan kecil tanpa Anda harus secara eksplisit mengatur konfigurasi untuk setiap file. Untuk informasi selengkapnya, lihat [Layout file progresif](#).
- Ukuran Stripe secara default adalah 1MiB. Menyetel garis offset mungkin berguna dalam keadaan khusus, tetapi secara umum yang terbaik adalah membiarkannya tidak ditentukan dan menggunakan default.

Layout file progresif

Anda dapat menentukan konfigurasi layout file progresif (PFL) untuk sebuah direktori untuk menentukan konfigurasi stripe yang berbeda-beda untuk file kecil dan besar sebelum mengisinya. Misalnya, Anda dapat mengatur PFL di direktori tingkat atas sebelum ada data yang dituliskan ke sistem file yang baru.

Untuk menentukan konfigurasi PFL, gunakan perintah `lfs setstripe` dengan opsi `-E` untuk menentukan komponen layout untuk file dengan ukuran yang berbeda-beda, seperti perintah berikut:

```
lfs setstripe -E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32 /mountname/directory
```

Perintah ini menetapkan empat komponen tata letak:

- Komponen pertama (`-E 100M -c 1`) menunjukkan nilai jumlah stripe sebanyak 1 untuk file-file dengan ukuran 100MiB.
- Komponen kedua (`-E 10G -c 8`) menunjukkan nilai jumlah stripe sebanyak 8 untuk file-file dengan ukuran 10GiB.
- Komponen ketiga (`-E 100G -c 16`) menunjukkan jumlah garis 16 untuk file berukuran hingga 100GiB.
- Komponen keempat (`-E -1 -c 32`) menunjukkan jumlah garis 32 untuk file yang lebih besar dari 100GiB.

⚠ Important

Menambahkan data ke file yang dibuat dengan sebuah layout PFL, data akan mengisi semua komponen layout-nya. Misalnya, dengan perintah 4-komponen yang ditunjukkan di atas, jika Anda membuat file 1MiB dan kemudian menambahkan data ke ujungnya, tata letak file akan diperluas untuk memiliki jumlah garis -1, yang berarti semua OST dalam sistem. Hal ini tidak berarti data akan ditulis ke setiap OST, tetapi sebuah operasi seperti membaca panjang file akan mengirimkan permintaan secara paralel ke setiap OST, menambah beban jaringan yang signifikan ke sistem file.

Oleh karena itu, berhati-hatilah untuk membatasi jumlah stripe untuk panjang file berukuran kecil dan medium yang selanjutnya dapat diisi oleh data ke dalamnya. Karena file berkas log biasanya membesar dengan adanya catatan baru yang ditambahkan, Amazon FSx for Lustre menetapkan jumlah stripe default sebanyak 1 ke setiap file yang dibuat dalam mode tambah, terlepas dari konfigurasi stripe default yang ditentukan oleh direktori induknya.

Konfigurasi PFL default di Amazon FSx for Lustre sistem file yang dibuat setelah 25 Agustus 2023 diatur dengan perintah ini:

```
lfs setstripe -E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32 /mountname
```

Pelanggan dengan beban kerja yang memiliki akses sangat bersamaan pada file sedang dan besar cenderung mendapat manfaat dari tata letak dengan lebih banyak garis pada ukuran yang lebih kecil dan striping di semua OST untuk file terbesar, seperti yang ditunjukkan dalam tata letak contoh empat komponen.

Memantau performa dan penggunaan

Setiap menit, Amazon FSx for Lustre memancarkan metrik penggunaan untuk setiap disk (MDT dan OST) ke Amazon. CloudWatch

Untuk melihat detail penggunaan sistem file agregat, Anda dapat melihat statistik Jumlah dari setiap metrik. Sebagai contoh, Jumlah dari statistik `DataReadBytes` melaporkan total throughput baca yang terlihat oleh semua OST di dalam sebuah sistem file. Sama halnya, Jumlah dari statistik `FreeDataStorageCapacity` melaporkan jumlah kapasitas penyimpanan yang tersedia untuk data file di dalam sistem file.

Untuk informasi selengkapnya tentang pemantauan performa dari sistem file Anda, lihat [Memantau Amazon FSx for Lustre](#).

Tips performa

Saat menggunakan Amazon FSx for Lustre, ingatlah tips performa berikut ini. Untuk batas-batas layanan, lihat [Kuota](#).

- Ukuran I/O rata-rata — Karena Amazon FSx for Lustre adalah sebuah sistem file jaringan, masing-masing operasi file melakukan perjalanan pulang-pergi antara client dan Amazon FSx for Lustre, menimbulkan sedikit overhead latensi. Karena latency per-operasi ini, throughput keseluruhan secara umum meningkat karena ukuran I/O rata-rata yang meningkat, karena overhead diamortisasi melebihi jumlah data yang lebih besar.
- Model permintaan — Dengan mengaktifkan penulisan asinkron ke sistem file Anda, operasi tulis yang tertunda menjadi buffer di instans Amazon EC2 sebelum ditulis di Amazon FSx for Lustre secara asinkron. Penulisan asinkron biasanya memiliki latensi yang lebih rendah. Saat melakukan penulisan asinkron, kernel menggunakan memori tambahan untuk melakukan cache. Sistem file yang telah mengaktifkan penulisan sinkron mengeluarkan permintaan sinkron ke Amazon FSx for Lustre. Setiap operasi melakukan perjalanan pulang-pergi antara client dan Amazon FSx for Lustre.

Note

Model permintaan pilihan Anda telah mengorbankan konsistensi (jika Anda menggunakan beberapa instans Amazon EC2) dan kecepatan.

- Batasi ukuran direktori - Untuk mencapai kinerja metadata yang optimal pada Persistent_2 FSx untuk sistem file Lustre, batasi setiap direktori hingga kurang dari 100K file. Membatasi jumlah file dalam direktori mengurangi waktu yang diperlukan untuk sistem file untuk memperoleh kunci pada direktori induk.
- Instans Amazon EC2 — Aplikasi-aplikasi yang melakukan sejumlah besar operasi baca dan tulis cenderung memerlukan lebih banyak memori atau kapasitas komputasi daripada aplikasi-aplikasi yang tidak melakukannya. Ketika meluncurkan instans-instans Amazon EC2 Anda untuk beban kerja komputasi intensif Anda, pilihlah jenis-jenis instans yang memiliki jumlah sumber daya yang dibutuhkan aplikasi Anda. Karakteristik performa sistem file Amazon FSx for Lustre tidak tergantung pada penggunaan Amazon EBS — instans-instans yang dioptimalkan.
- Penyetelan instans klien yang direkomendasikan untuk kinerja optimal

1. Untuk semua jenis dan ukuran instans klien, kami sarankan untuk menerapkan penyetelan berikut:

```
sudo lctl set_param osc.*.max_dirty_mb=64
```

2. Untuk tipe instance klien dengan memori lebih dari 64 GiB, kami sarankan untuk menerapkan penyetelan berikut:

```
lctl set_param ldlm.namespaces.*.lru_max_age=600000
```

3. Untuk tipe instans klien dengan lebih dari 64 core vCPU, kami sarankan untuk menerapkan penyetelan berikut:

```
echo "options ptlrpc ptlrpcd_per_cpt_max=32" >> /etc/modprobe.d/modprobe.conf
echo "options ksocklnd credits=2560" >> /etc/modprobe.d/modprobe.conf

# reload all kernel modules to apply the above two settings
sudo reboot
```

Setelah klien dipasang, penyetelan berikut perlu diterapkan:

```
sudo lctl set_param osc.*OST*.max_rpcs_in_flight=32
sudo lctl set_param mdc.*.max_rpcs_in_flight=64
sudo lctl set_param mdc.*.max_mod_rpcs_in_flight=50
```

Perhatikan bahwa `lctl set_param` diketahui tidak bertahan selama reboot. Karena parameter ini tidak dapat diatur secara permanen dari sisi klien, disarankan untuk mengimplementasikan pekerjaan boot cron untuk mengatur konfigurasi dengan penyetelan yang disarankan.

- Keseimbangan beban kerja di OST — Dalam beberapa kasus, beban kerja Anda tidak men-drive throughput agregat yang dapat diberikan oleh sistem file Anda (200 MB/s per TiB penyimpanan). Jika demikian, Anda dapat menggunakan CloudWatch metrik untuk memecahkan masalah jika kinerja dipengaruhi oleh ketidakseimbangan dalam pola I/O beban kerja Anda. Untuk mengidentifikasi apakah ini penyebabnya, lihat CloudWatch metrik Maksimum untuk Amazon FSx for Lustre.

Dalam beberapa kasus, statistik ini menunjukkan beban sebesar 240 MBps atau di atasnya throughput (kapasitas throughput dari satu disk Amazon FSx for Lustre 1,2-TiB). Dalam kasus tersebut, beban kerja Anda tidak tersebar secara merata di seluruh disk Anda. Jika demikian

kasusnya, Anda dapat menggunakan perintah `lfs setstripe` untuk memodifikasi striping file yang paling sering diakses oleh beban kerja Anda. Untuk performa optimal, file-file stripe dengan persyaratan throughput yang tinggi di semua OST harus berisikan sistem file Anda.

Jika file Anda diimpor dari repositori data, Anda dapat mengambil pendekatan lain untuk men-stripe file-file ber-throughput tinggi milik Anda secara merata di seluruh OST Anda. Untuk melakukannya, Anda dapat memodifikasi parameter `ImportedFileChunkSize` saat membuat sistem file Amazon FSx for Lustre berikutnya.

Sebagai contoh, misalkan beban kerja Anda menggunakan sistem file 7,0-TiB (yang terdiri dari OSTs 6x 1,17-TiB) dan perlu men-drive throughput tinggi di seluruh file-file berjumlah 2,4-GiB. Dalam hal ini, Anda dapat mengatur nilai `ImportedFileChunkSize` ke $(2.4 \text{ GiB} / 6 \text{ OSTs}) = 400 \text{ MiB}$ sehingga file-file Anda tersebar secara merata di seluruh OST sistem file Anda.

- Klien Lustre untuk Metadata IOPS - Jika sistem file Anda memiliki konfigurasi metadata yang ditentukan, kami sarankan Anda menginstal klien Lustre 2.15 atau klien Lustre 2.12 dengan salah satu versi OS ini: Amazon Linux 2023, Amazon Linux 2, Red Hat/CentOs/Rocky Linux 8.9 atau 9.x, Ubuntu 22 dengan 6.2 kernel, atau Ubuntu 20.

Mengakses sistem file

Menggunakan Amazon FSx, Anda dapat menjalankan beban kerja intensif komputasi dari lokal ke Amazon Web Services Cloud dengan mengimpor data melalui atau VPN. AWS Direct Connect Anda dapat mengakses sistem file Amazon FSx dari on-premise, menyalin data ke sistem file sesuai kebutuhan, dan menjalankan beban kerja komputasi intensif pada instans di cloud.

Di bagian berikut, Anda dapat mempelajari cara mengakses sistem file Amazon FSx for Lustre pada instans Linux. Selain itu, Anda dapat menemukan cara menggunakan file `fstab` untuk secara otomatis memasang kembali sistem file Anda setelah merestart sistem.

Sebelum Anda dapat memasang sistem file, Anda harus membuat, mengkonfigurasi, dan meluncurkan sumber daya AWS terkait. Untuk petunjuk mendetail, lihat [Memulai dengan Amazon FSx for Lustre](#). Selanjutnya, Anda dapat menginstal dan mengkonfigurasi klien Lustre pada instans komputasi Anda.

Topik

- [Sistem file Lustre dan kompatibilitas kernel klien](#)
- [Menginstal klien Lustre](#)
- [Pemasangan dari instans Amazon Elastic Compute Cloud](#)
- [Pemasangan dari Amazon Elastic Container Service](#)
- [Memasang sistem file Amazon FSx dari on-premise atau Amazon VPC hasil peering](#)
- [Memasang sistem file Amazon FSx Anda secara otomatis](#)
- [Memasang fileset spesifik](#)
- [Melepaskan sistem file](#)
- [Mengerjakan Instans Spot Amazon EC2](#)

Sistem file Lustre dan kompatibilitas kernel klien

Kami sangat menyarankan menggunakan versi Lustre untuk sistem file FSx for Lustre Anda yang kompatibel dengan versi kernel Linux dari instance klien Anda.

Klien Amazon Linux

Sistem operasi	Versi OS	Versi kernel minimum	Versi kernel maksimum	Versi sistem file		
				2.10	2.12	2.15
Amazon Linux 2023	6.1	6.1.79-99.167	6.1.79-99.167+	tidak	ya	Ya
Amazon Linux 2	5.10	5.10.144-127.601	5.10.144-127.601+	Ya	Ya	Ya
			<5.10.144-127.601	Ya	ya	tidak
	5.4	5.4.214-120.368	5.4.214-120.368+	Ya	Ya	Ya
			<5.4.214-120.368	Ya	ya	tidak
	4.14	4.14.294-220.533	4.14.294-220.533+	Ya	Ya	Ya
			<4.14.294-220.533	Ya	ya	tidak

Klien Ubuntu

Sistem operasi	Versi OS	Versi kernel minimum	Versi kernel maksimum	Versi sistem file		
				2.10	2.12	2.15
				2.10	2.12	2.15

Sistem operasi	Versi OS	Versi kernel minimum	Versi kernel maksimum	Versi sistem file		
				2.10	2.12	2.15
Ubuntu	22	6.2.0-101 7.17 ~ 22.04	6.2.0. *	tidak	ya	Ya
		5.15.0-10 15-aws	5.15.0-10 31-cakar	Ya	Ya	Ya
	20	5.15.0-10 15-aws	5.15.0+	Ya	Ya	Ya
		5.4.0-101 1-aws	5.13.0-10 31-cakar	Ya	ya	tidak

Klien RHEL/CentOS/Rocky Linux

Sistem operasi	Versi OS	Arsitektur	Versi kernel minimum	Versi kernel maksimum	Versi sistem file		
					2.10	2.12	2.15
RHEL/ CentOS/ Linux berbatu	9.4	Lengan +x86	5.14.0-42 7.13.1	5.14.0-42 7.16.1	tidak	ya	Ya
			5.14.0-36 2.18.1	5.14.0-36 2.18.1	tidak	ya	Ya
	9.0	Lengan +x86	5.14.0-70 .13.1	5.14.0-70 .30.1	tidak	ya	Ya

Sistem operasi	Versi OS	Arsitektur	Versi kernel minimum	Versi kernel maksimum	Versi sistem file		
	8.9	Lengan +x86	4.18.0-513*	4.18.0-513*	Ya	Ya	Ya
	8.8	Lengan +x86	4.18.0-477*	4.18.0-477*	Ya	Ya	Ya
	8.7	Lengan +x86	4.18.0-425*	4.18.0-425*	Ya	Ya	Ya
	8.6	Lengan +x86	4.18.0-372*	4.18.0-372*	Ya	Ya	Ya
	8.5	Lengan +x86	4.18.0-348*	4.18.0-348*	Ya	Ya	Ya
	8.4	Lengan +x86	4.18.0-305*	4.18.0-305*	Ya	Ya	Ya
RHEL/ CentOS	8.3	Lengan +x86	4.18.0-240*	4.18.0-240*	Ya	ya	tidak
	8.2	Lengan +x86	4.18.0-193*	4.18.0-193*	Ya	ya	tidak
	7.9	x86	3.10.0-1160*	3.10.0-1160*	Ya	Ya	Ya
	7.8	x86	3.10.0-1127*	3.10.0-1127*	Ya	ya	tidak
	7.7	x86	3.10.0-1062*	3.10.0-1062*	Ya	ya	tidak
CentOS	7.9	Arm	4.18.0-193*	4.18.0-193*	Ya	Ya	Ya

Sistem operasi	Versi OS	Arsitektur	Versi kernel minimum	Versi kernel maksimum	Versi sistem file		
	7.8	Arm	4.18.0-14 7*	4.18.0-14 7*	Ya	Ya	Ya

Menginstal klien Lustre

Untuk memasang sistem file Amazon FSx for Lustre Anda dari instans Linux, pertama-tama instal klien Lustre sumber terbuka. Kemudian, bergantung pada versi sistem operasi anda, gunakan salah satu prosedur berikut. Untuk informasi dukungan kernel, lihat [Sistem file Lustre dan kompatibilitas kernel klien](#).

Jika instans komputasi Anda tidak menjalankan kernel Linux yang ditentukan dalam petunjuk instalasi, dan Anda tidak dapat mengubah kernel, Anda dapat membangun klien Lustre Anda sendiri. Untuk informasi selengkapnya, lihat: [Mengkompilasi Lustre](#) di Lustre Wiki.

Amazon Linux

Untuk menginstal klien Lustre di Amazon Linux 2023

1. Buka terminal pada klien Anda.
2. Tentukan kernel mana yang sedang berjalan pada instans komputasi Anda dengan menjalankan perintah berikut.

```
uname -r
```

3. Tinjau respons sistem dan bandingkan dengan persyaratan kernel minimum berikut untuk menginstal klien Lustre di Amazon Linux 2023:

- 6.1 persyaratan minimum kernel - 6.1.79-99.167.amzn2023

Jika instans EC2 Anda memenuhi persyaratan kernel minimum, lanjutkan ke langkah dan instal klien lustre.

Jika perintah mengembalikan hasil kurang dari persyaratan minimum kernel, perbarui kernel dan reboot instans Amazon EC2 Anda dengan menjalankan perintah berikut.

```
sudo dnf -y update kernel && sudo reboot
```

Konfirmasikan bahwa kernel telah diperbarui menggunakan perintah `uname -r`.

4. Unduh dan instal klien Lustre dengan perintah berikut.

```
sudo dnf install -y lustre-client
```

Untuk menginstal klien Lustre di Amazon Linux 2

1. Buka terminal pada klien Anda.
2. Tentukan kernel mana yang sedang berjalan pada instans komputasi Anda dengan menjalankan perintah berikut.

```
uname -r
```

3. Tinjau respons sistem dan bandingkan dengan persyaratan kernel minimum berikut untuk menginstal klien Lustre di Amazon Linux 2:

- 5.10 persyaratan minimum kernel - 5.10.144-127.601.amzn2
- 5.4 persyaratan minimum kernel - 5.4.214-120.368.amzn2
- 4.14 persyaratan minimum kernel - 4.14.294-220.533.amzn2

Jika instans EC2 Anda memenuhi persyaratan kernel minimum, lanjutkan ke langkah dan instal klien lustre.

Jika perintah mengembalikan hasil kurang dari persyaratan minimum kernel, perbarui kernel dan reboot instans Amazon EC2 Anda dengan menjalankan perintah berikut.

```
sudo yum -y update kernel && sudo reboot
```

Konfirmasikan bahwa kernel telah diperbarui menggunakan perintah `uname -r`.

4. Unduh dan instal klien Lustre dengan perintah berikut.

```
sudo amazon-linux-extras install -y lustre
```

Jika Anda tidak dapat memutakhirkan kernel ke persyaratan minimum kernel, Anda dapat menginstal klien 2.10 lama dengan perintah berikut.

```
sudo amazon-linux-extras install -y lustre2.10
```

Untuk menginstal klien Lustre di Amazon Linux

1. Buka terminal pada klien Anda.
2. Tentukan kernel mana yang sedang berjalan pada instans komputasi Anda dengan menjalankan perintah berikut. Klien Lustre membutuhkan kernel Amazon Linux 4.14, `version 104` atau versi lebih tinggi.

```
uname -r
```

3. Lakukan salah satu hal berikut ini:

- Jika perintah mengembalikan `4.14.104-78.84.amzn1.x86_64` atau versi yang lebih tinggi dari 4.14, unduh dan instal klien Lustre menggunakan perintah berikut.

```
sudo yum install -y lustre-client
```

- Jika perintah mengembalikan hasil kurang dari `4.14.104-78.84.amzn1.x86_64`, perbarui kernel dan reboot instans Amazon EC2 Anda dengan menjalankan perintah berikut.

```
sudo yum -y update kernel && sudo reboot
```

Konfirmasikan bahwa kernel telah diperbarui menggunakan perintah `uname -r`. Kemudian unduh dan instal klien Lustre seperti yang diterangkan sebelumnya.

CentOS, Rocky Linux, dan Red Hat

Untuk menginstal klien Lustre di CentOS, Red Hat, dan Rocky Linux 9.0, 9.3, atau 9.4

Anda dapat menginstal dan memperbarui paket klien Lustre yang kompatibel dengan Red Hat Enterprise Linux (RHEL), Rocky Linux, dan CentOS dari repositori paket yum klien Amazon FSx Lustre. Paket-paket ini ditandatangani untuk membantu memastikan belum diotak-atik sebelum atau

selama pengunduhan. Instalasi repositori gagal jika Anda tidak menginstal kunci publik yang sesuai pada sistem Anda.

Untuk menambahkan repositori paket yum klien Lustre Amazon FSx

1. Buka terminal pada klien Anda.
2. Instal kunci publik rpm Amazon FSx dengan menggunakan perintah berikut.

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
```

3. Impor kunci dengan menggunakan perintah berikut.

```
sudo rpm --import /tmp/fsx-rpm-public-key.asc
```

4. Tambahkan repositori dan perbarui pengelola paket menggunakan perintah berikut.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/9/fsx-lustre-client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Untuk mengkonfigurasi repositori yum klien Lustre Amazon FSx

Repositori paket yum klien Amazon FSx Lustre dikonfigurasi secara default untuk menginstal klien Lustre yang kompatibel dengan versi kernel yang awalnya dikirimkan dengan rilis CentOS, Rocky Linux, dan RHEL 9 yang didukung terbaru. Untuk menginstal klien Lustre yang kompatibel dengan versi kernel yang Anda gunakan, Anda dapat mengedit file konfigurasi repositori.

Bagian ini menjelaskan cara menentukan kernel mana yang sedang Anda jalankan, apakah Anda perlu mengedit konfigurasi repositori atau tidak, dan cara mengedit file konfigurasi.

1. Tentukan kernel mana yang sedang berjalan pada instans komputasi Anda dengan menjalankan perintah berikut.

```
uname -r
```

2. Lakukan salah satu hal berikut ini:

- Jika perintah mengembalikan `5.14.0-427*`, Anda tidak perlu mengubah konfigurasi repositori. Lanjutkan ke prosedur Untuk menginstal klien Lustre.

- Jika perintah kembali `5.14.0-362.18.1`, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk rilis CentOS, Rocky Linux, dan RHEL 9.3.
 - Jika perintah kembali `5.14.0-70*`, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk rilis CentOS, Rocky Linux, dan RHEL 9.0.
3. Mengedit file konfigurasi repositori untuk menunjuk ke versi tertentu dari RHEL menggunakan perintah berikut. Ganti *specific_RHEL_version* dengan versi RHEL yang perlu Anda gunakan.

```
sudo sed -i 's#9#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
```

Misalnya, untuk menunjuk ke rilis 9.3, gantikan *specific_RHEL_version* dengan `9.3` perintah, seperti pada contoh berikut.

```
sudo sed -i 's#9#9.3#' /etc/yum.repos.d/aws-fsx.repo
```

4. Gunakan perintah berikut untuk menghapus cache yum.

```
sudo yum clean all
```

Untuk menginstal klien Lustre

- Instal paket dari repositori menggunakan perintah berikut.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Informasi tambahan (CentOS, Rocky Linux, dan Red Hat 9.0 dan yang lebih baru)

Perintah sebelumnya menginstal dua paket yang diperlukan untuk pemasangan dan interaksi dengan sistem file Amazon FSx Anda. Repositori mencakup paket Lustre tambahan, seperti paket berisi kode sumber dan paket yang berisi tes, dan Anda dapat menginstalnya secara opsional. Untuk membuat daftar semua paket yang tersedia di repositori, gunakan perintah berikut.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Untuk mengunduh rpm sumber, yang berisi tarball dari kode sumber hulu dan kumpulan patch yang telah kami terapkan, gunakan perintah berikut.

```
sudo yumdownloader --source kmod-lustre-client
```

Ketika Anda menjalankan yum update, versi yang lebih baru dari modul tersebut diinstal jika tersedia, dan menggantikan versi yang ada. Untuk mencegah versi yang sudah terpasang saat ini dihapus saat pembaruan, tambahkan baris seperti berikut pada file `/etc/yum.conf` Anda.

```
installonlypkgs=kernel, kernel-PAE, installonlypkg(kernel), installonlypkg(kernel-  
module),  
installonlypkg(vm), multiversion(kernel), kmod-lustre-client
```

Daftar ini mencakup paket hanya install default, yang disebutkan dalam halaman man `yum.conf`, dan paket `kmod-lustre-client`.

Untuk menginstal klien Lustre di CentOS dan Red Hat 8.2-8.9 atau di Rocky Linux 8.4-8.9

Anda dapat menginstal dan memperbarui paket klien Lustre yang kompatibel dengan Red Hat Enterprise Linux (RHEL), Rocky Linux, dan CentOS dari repositori paket yum klien Amazon FSx Lustre. Paket-paket ini ditandatangani untuk membantu memastikan belum diotak-atik sebelum atau selama pengunduhan. Instalasi repositori gagal jika Anda tidak menginstal kunci publik yang sesuai pada sistem Anda.

Untuk menambahkan repositori paket yum klien Lustre Amazon FSx

1. Buka terminal pada klien Anda.
2. Instal kunci publik rpm Amazon FSx dengan menggunakan perintah berikut.

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-  
key.asc -o /tmp/fsx-rpm-public-key.asc
```

3. Impor kunci dengan menggunakan perintah berikut.

```
sudo rpm --import /tmp/fsx-rpm-public-key.asc
```

4. Tambahkan repositori dan perbarui pengelola paket menggunakan perintah berikut.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/8/fsx-lustre-  
client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Untuk mengkonfigurasi repositori yum klien Lustre Amazon FSx

Repositori paket yum klien Amazon FSx Lustre dikonfigurasi secara default untuk menginstal klien Lustre yang kompatibel dengan versi kernel yang awalnya dikirimkan dengan rilis CentOS, Rocky Linux, dan RHEL 8 yang didukung terbaru. Untuk menginstal klien Lustre yang kompatibel dengan versi kernel yang Anda gunakan, Anda dapat mengedit file konfigurasi repositori.

Bagian ini menjelaskan cara menentukan kernel mana yang sedang Anda jalankan, apakah Anda perlu mengedit konfigurasi repositori atau tidak, dan cara mengedit file konfigurasi.

1. Tentukan kernel mana yang sedang berjalan pada instans komputasi Anda dengan menjalankan perintah berikut.

```
uname -r
```

2. Lakukan salah satu hal berikut ini:

- Jika perintah mengembalikan `4.18.0-513*`, Anda tidak perlu mengubah konfigurasi repositori. Lanjutkan ke prosedur Untuk menginstal klien Lustre.
- Jika perintah kembali `4.18.0-477*`, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk rilis CentOS, Rocky Linux, dan RHEL 8.8.
- Jika perintah kembali `4.18.0-425*`, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk rilis CentOS, Rocky Linux, dan RHEL 8.7.
- Jika perintah kembali `4.18.0-372*`, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk rilis CentOS, Rocky Linux, dan RHEL 8.6.
- Jika perintah kembali `4.18.0-348*`, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk rilis CentOS, Rocky Linux, dan RHEL 8.5.
- Jika perintah kembali `4.18.0-305*`, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk rilis CentOS, Rocky Linux, dan RHEL 8.4.
- Jika perintah mengembalikan `4.18.0-240*`, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk CentOS dan RHEL rilis 8.3.
- Jika perintah mengembalikan `4.18.0-193*`, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk CentOS dan RHEL rilis 8.2.

3. Mengedit file konfigurasi repositori untuk menunjuk ke versi tertentu dari RHEL menggunakan perintah berikut.

```
sudo sed -i 's#8#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
```

Misalnya, untuk menunjuk ke rilis 8.8, gantikan *specific_RHEL_version* 8.8 dengan perintah.

```
sudo sed -i 's#8#8.8#' /etc/yum.repos.d/aws-fsx.repo
```

4. Gunakan perintah berikut untuk menghapus cache yum.

```
sudo yum clean all
```

Untuk menginstal klien Lustre

- Instal paket dari repositori menggunakan perintah berikut.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Informasi tambahan (CentOS, Rocky Linux, dan Red Hat 8.2 dan yang lebih baru)

Perintah sebelumnya menginstal dua paket yang diperlukan untuk pemasangan dan interaksi dengan sistem file Amazon FSx Anda. Repositori mencakup paket Lustre tambahan, seperti paket berisi kode sumber dan paket yang berisi tes, dan Anda dapat menginstalnya secara opsional. Untuk membuat daftar semua paket yang tersedia di repositori, gunakan perintah berikut.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Untuk mengunduh rpm sumber, yang berisi tarball dari kode sumber hulu dan kumpulan patch yang telah kami terapkan, gunakan perintah berikut.

```
sudo yumdownloader --source kmod-lustre-client
```

Ketika Anda menjalankan yum update, versi yang lebih baru dari modul tersebut diinstal jika tersedia, dan menggantikan versi yang ada. Untuk mencegah versi yang sudah terpasang saat ini dihapus saat pembaruan, tambahkan baris seperti berikut pada file `/etc/yum.conf` Anda.

```
installonlypkgs=kernel, kernel-PAE, installonlypkg(kernel), installonlypkg(kernel-  
module),  
installonlypkg(vm), multiversion(kernel), kmod-lustre-client
```

Daftar ini mencakup paket hanya install default, yang disebutkan dalam halaman `man yum.conf`, dan paket `kmod-lustre-client`.

Untuk menginstal klien Lustre pada CentOS dan Red Hat 7.7, 7.8, atau 7.9 (instans `x86_64`)

Anda dapat menginstal dan memperbarui paket klien Lustre yang kompatibel dengan Red Hat Enterprise Linux (RHEL) dan CentOS dari repositori paket yum klien Lustre Amazon FSx. Paket-paket ini ditandatangani untuk membantu memastikan belum diotak-atik sebelum atau selama pengunduhan. Instalasi repositori gagal jika Anda tidak menginstal kunci publik yang sesuai pada sistem Anda.

Untuk menambahkan repositori paket yum klien Lustre Amazon FSx

1. Buka terminal pada klien Anda.
2. Instal kunci publik rpm Amazon FSx menggunakan perintah berikut.

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
```

3. Impor kunci menggunakan perintah berikut.

```
sudo rpm --import /tmp/fsx-rpm-public-key.asc
```

4. Tambahkan repositori dan perbarui pengelola paket menggunakan perintah berikut.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/el/7/fsx-lustre-client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Untuk mengkonfigurasi repositori yum klien Lustre Amazon FSx

Repositori paket yum klien Lustre Amazon FSx dikonfigurasi secara default untuk menginstal klien Lustre yang kompatibel dengan versi kernel yang awalnya dikirimkan dengan CentOS terbaru dan RHEL rilis 7 yang didukung. Untuk menginstal klien Lustre yang kompatibel dengan versi kernel yang Anda gunakan, Anda dapat mengedit file konfigurasi repositori.

Bagian ini menjelaskan cara menentukan kernel mana yang sedang Anda jalankan, apakah Anda perlu mengedit konfigurasi repositori atau tidak, dan cara mengedit file konfigurasi.

1. Tentukan kernel mana yang sedang berjalan pada instans komputasi Anda dengan menjalankan perintah berikut.

```
uname -r
```

2. Lakukan salah satu hal berikut ini:

- Jika perintah mengembalikan 3.10.0-1160*, Anda tidak perlu mengubah konfigurasi repositori. Lanjutkan ke prosedur Untuk menginstal klien Lustre.
- Jika perintah mengembalikan 3.10.0-1127*, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk CentOS dan RHEL rilis 7.8.
- Jika perintah mengembalikan 3.10.0-1062*, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk CentOS dan RHEL rilis 7.7.

3. Mengedit file konfigurasi repositori untuk menunjuk ke versi tertentu dari RHEL menggunakan perintah berikut.

```
sudo sed -i 's#7#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
```

Untuk menunjuk ke rilis 7.8, ganti *specific_RHEL_version* dengan 7.8 dalam perintah.

```
sudo sed -i 's#7#7.8#' /etc/yum.repos.d/aws-fsx.repo
```

Untuk menunjuk ke rilis 7.7, ganti *specific_RHEL_version* dengan 7.7 dalam perintah.

```
sudo sed -i 's#7#7.7#' /etc/yum.repos.d/aws-fsx.repo
```

4. Gunakan perintah berikut untuk menghapus cache yum.

```
sudo yum clean all
```

Untuk menginstal klien Lustre

- Instal paket klien Lustre dari repositori menggunakan perintah berikut.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Informasi tambahan (CentOS dan Red Hat 7.7 dan rilis yang lebih baru)

Perintah sebelumnya menginstal dua paket yang diperlukan untuk pemasangan dan interaksi dengan sistem file Amazon FSx Anda. Repositori mencakup paket Lustre tambahan, seperti paket berisi kode sumber dan paket yang berisi tes, dan Anda dapat menginstalnya secara opsional. Untuk membuat daftar semua paket yang tersedia di repositori, gunakan perintah berikut.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Untuk mengunduh rpm sumber yang berisi tarball dari kode sumber hulu dan kumpulan patch yang telah kami terapkan, gunakan perintah berikut.

```
sudo yumdownloader --source kmod-lustre-client
```

Ketika Anda menjalankan yum update, versi yang lebih baru dari modul tersebut diinstal jika tersedia, dan menggantikan versi yang ada. Untuk mencegah versi yang sudah terpasang saat ini dihapus saat pembaruan, tambahkan baris seperti berikut pada file `/etc/yum.conf` Anda.

```
installonlypkgs=kernel, kernel-big-mem, kernel-enterprise, kernel-smp,  
                kernel-debug, kernel-unsupported, kernel-source, kernel-devel, kernel-  
PAE,  
                kernel-PAE-debug, kmod-lustre-client
```

Daftar ini mencakup paket hanya install default, yang disebutkan dalam halaman `man yum.conf`, dan paket `kmod-lustre-client`.

Untuk menginstal klien Lustre pada CentOS 7.8 atau 7.9 (instance bertenaga Graviton berbasis ARM) AWS

Anda dapat menginstal dan memperbarui paket klien Lustre dari repositori paket yum klien Amazon FSx Lustre yang kompatibel dengan CentOS 7 untuk instans EC2 berbasis Graviton berbasis ARM. AWS Paket-paket ini ditandatangani untuk membantu memastikan belum diotak-atik sebelum atau selama pengunduhan. Instalasi repositori gagal jika Anda tidak menginstal kunci publik yang sesuai pada sistem Anda.

Untuk menambahkan repositori paket yum klien Lustre Amazon FSx

1. Buka terminal pada klien Anda.
2. Instal kunci publik rpm Amazon FSx menggunakan perintah berikut.

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
```

```
curl https://fsx-lustre-client-repo-public-keys.s3.amazonaws.cn/fsx-rpm-public-key.asc -o /tmp/fsx-rpm-public-key.asc
```

3. Impor kunci menggunakan perintah berikut.

```
sudo rpm --import /tmp/fsx-rpm-public-key.asc
```

4. Tambahkan repositori dan perbarui pengelola paket menggunakan perintah berikut.

```
sudo curl https://fsx-lustre-client-repo.s3.amazonaws.com/centos/7/fsx-lustre-client.repo -o /etc/yum.repos.d/aws-fsx.repo
```

Untuk mengkonfigurasi repositori yum klien Lustre Amazon FSx

Repositori paket yum klien Lustre Amazon FSx dikonfigurasi secara default untuk menginstal klien Lustre yang kompatibel dengan versi kernel yang awalnya dikirimkan dengan CentOS rilis 7 terbaru yang didukung. Untuk menginstal klien Lustre yang kompatibel dengan versi kernel yang Anda gunakan, Anda dapat mengedit file konfigurasi repositori.

Bagian ini menjelaskan cara menentukan kernel mana yang sedang Anda jalankan, apakah Anda perlu mengedit konfigurasi repositori atau tidak, dan cara mengedit file konfigurasi.

1. Tentukan kernel mana yang sedang berjalan pada instans komputasi Anda dengan menjalankan perintah berikut.

```
uname -r
```

2. Lakukan salah satu hal berikut ini:

- Jika perintah mengembalikan `4.18.0-193*`, Anda tidak perlu mengubah konfigurasi repositori. Lanjutkan ke prosedur Untuk menginstal klien Lustre.
- Jika perintah mengembalikan `4.18.0-147*`, Anda harus mengedit konfigurasi repositori sehingga menunjuk ke klien Lustre untuk CentOS rilis 7.8.

3. Mengedit file konfigurasi repositori untuk menunjuk ke CentOS rilis 7.8 menggunakan perintah berikut.

```
sudo sed -i 's#7#7.8#' /etc/yum.repos.d/aws-fsx.repo
```

4. Gunakan perintah berikut untuk menghapus cache yum.

```
sudo yum clean all
```

Untuk menginstal klien Lustre

- Instal paket dari repositori menggunakan perintah berikut.

```
sudo yum install -y kmod-lustre-client lustre-client
```

Informasi tambahan (CentOS 7.8 atau 7.9 untuk instans EC2 bertenaga Graviton berbasis ARM AWS)

Perintah sebelumnya menginstal dua paket yang diperlukan untuk pemasangan dan interaksi dengan sistem file Amazon FSx Anda. Repositori mencakup paket Lustre tambahan, seperti paket berisi kode sumber dan paket yang berisi tes, dan Anda dapat menginstalnya secara opsional. Untuk membuat daftar semua paket yang tersedia di repositori, gunakan perintah berikut.

```
yum --disablerepo="*" --enablerepo="aws-fsx" list available
```

Untuk mengunduh rpm sumber, yang berisi tarball dari kode sumber hulu dan kumpulan patch yang telah kami terapkan, gunakan perintah berikut.

```
sudo yumdownloader --source kmod-lustre-client
```

Ketika Anda menjalankan yum update, versi yang lebih baru dari modul tersebut diinstal jika tersedia, dan menggantikan versi yang ada. Untuk mencegah versi yang sudah terpasang saat ini dihapus saat pembaruan, tambahkan baris seperti berikut pada file `/etc/yum.conf` Anda.

```
installonlypkgs=kernel, kernel-big-mem, kernel-enterprise, kernel-smp,  
                kernel-debug, kernel-unsupported, kernel-source, kernel-devel, kernel-  
PAE,  
                kernel-PAE-debug, kmod-lustre-client
```

Daftar ini mencakup paket hanya install default, yang disebutkan dalam halaman `man yum.conf`, dan paket `kmod-lustre-client`.

Ubuntu

Untuk menginstal klien Lustre di Ubuntu 22.04

Anda bisa mendapatkan paket Lustre dari repositori Amazon FSx Ubuntu 22.04. Untuk memvalidasi bahwa isi repositori belum diotak-atik sebelum atau selama pengunduhan, tanda tangan GNU Privacy Guard (GPG) diterapkan ke metadata repositori. Instalasi repositori gagal kecuali Anda telah menginstal kunci GPG publik yang sesuai pada sistem Anda.

1. Buka terminal pada klien Anda.
2. Ikuti langkah-langkah berikut untuk menambahkan repositori Amazon FSx Ubuntu:
 - a. Jika sebelumnya Anda belum mendaftarkan repositori Amazon FSx Ubuntu pada instans klien Anda, unduh dan instal kunci publik yang diperlukan. Gunakan perintah berikut ini.

```
wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-key.gpg >/dev/null
```

- b. Tambahkan repositori paket Amazon FSx ke pengelola paket lokal Anda menggunakan perintah berikut.

```
sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu jammy main" > /etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
```

3. Tentukan kernel mana yang sedang berjalan pada instans klien Anda, dan perbarui sesuai kebutuhan. Klien Lustre di Ubuntu 22.04 memerlukan kernel `5.15.0-1015-aws` atau yang lebih baru untuk kedua instans EC2 berbasis x86 dan instans EC2 berbasis ARM yang didukung oleh prosesor Graviton. AWS

- a. Jalankan perintah berikut untuk menentukan kernel mana yang sedang berjalan.

```
uname -r
```

- b. Jalankan perintah berikut untuk memperbarui ke kernel Ubuntu dan Lustre versi terbaru dan kemudian reboot.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
```

Jika versi kernel Anda lebih besar daripada 5.15.0-1015-aws instans EC2 berbasis x86 dan instans EC2 berbasis Graviton, dan Anda tidak ingin memperbarui ke versi kernel terbaru, Anda dapat menginstal Lustre untuk kernel saat ini dengan perintah berikut.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Dua paket Lustre yang diperlukan untuk pemasangan dan interaksi dengan sistem file FSx for Lustre Anda diinstal. Anda dapat memilih menginstal paket terkait tambahan, seperti paket berisi kode sumber dan paket yang berisi tes yang termasuk dalam repositori.

- c. Buat daftar semua paket yang tersedia di repositori dengan menggunakan perintah berikut.

```
sudo apt-cache search ^lustre
```

- d. (Opsional) Jika Anda ingin upgrade sistem Anda juga selalu meng-upgrade modul klien Lustre, pastikan bahwa paket `lustre-client-modules-aws` diinstal menggunakan perintah berikut.

```
sudo apt install -y lustre-client-modules-aws
```

Note

Jika Anda mendapatkan `Module Not Found` kesalahan, lihat [Untuk memecahkan masalah kesalahan modul yang hilang](#).

Untuk menginstal klien Lustre pada Ubuntu 20.04

Klien Lustre 2.12 didukung di Ubuntu 20.04 dengan kernel 5.15.0-1015-aws atau yang lebih baru. Klien Lustre 2.10 didukung di Ubuntu 20.04 dengan kernel 5.4.0-1011-aws atau yang lebih baru pada instans EC2 berbasis x86 dan kernel 5.4.0-1015-aws atau yang lebih baru pada instans EC2 berbasis ARM yang didukung oleh prosesor Graviton. AWS

Anda bisa mendapatkan paket Lustre dari repositori Ubuntu 20.04 Amazon FSx. Untuk memvalidasi bahwa isi repositori belum diotak-atik sebelum atau selama pengunduhan, tanda tangan GNU

Privacy Guard (GPG) diterapkan ke metadata repositori. Instalasi repositori gagal kecuali Anda telah menginstal kunci GPG publik yang sesuai pada sistem Anda.

1. Buka terminal pada klien Anda.
2. Ikuti langkah-langkah berikut untuk menambahkan repositori Amazon FSx Ubuntu:
 - a. Jika sebelumnya Anda belum mendaftarkan repositori Amazon FSx Ubuntu pada instans klien Anda, unduh dan instal kunci publik yang diperlukan. Gunakan perintah berikut ini.

```
wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-key.gpg >/dev/null
```

- b. Tambahkan repositori paket Amazon FSx ke pengelola paket lokal Anda menggunakan perintah berikut.

```
sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu focal main" > /etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
```

3. Tentukan kernel mana yang sedang berjalan pada instans klien Anda, dan perbarui sesuai kebutuhan.
 - a. Jalankan perintah berikut untuk menentukan kernel mana yang sedang berjalan.

```
uname -r
```

- b. Jalankan perintah berikut untuk memperbarui ke kernel Ubuntu dan Lustre versi terbaru dan kemudian reboot.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
```

Jika versi kernel Anda lebih besar daripada 5.4.0-1011-aws instans EC2 berbasis x86, atau lebih besar dari 5.4.0-1015-aws instans EC2 berbasis Graviton, dan Anda tidak ingin memperbarui ke versi kernel terbaru, Anda dapat menginstal Lustre untuk kernel saat ini dengan perintah berikut.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Dua paket Lustre yang diperlukan untuk pemasangan dan interaksi dengan sistem file FSx for Lustre Anda diinstal. Anda dapat memilih menginstal paket terkait tambahan, seperti paket berisi kode sumber dan paket yang berisi tes yang termasuk dalam repositori.

- c. Buat daftar semua paket yang tersedia di repositori dengan menggunakan perintah berikut.

```
sudo apt-cache search ^lustre
```

- d. (Opsional) Jika Anda ingin upgrade sistem Anda juga selalu meng-upgrade modul klien Lustre, pastikan bahwa paket `lustre-client-modules-aws` diinstal menggunakan perintah berikut.

```
sudo apt install -y lustre-client-modules-aws
```

Note

Jika Anda mendapatkan `Module Not Found` kesalahan, lihat [Untuk memecahkan masalah kesalahan modul yang hilang](#).

Untuk menginstal klien Lustre di Ubuntu 18.04

Note

Versi kernel Ubuntu 18 yang terakhir didukung adalah `5.4.0.1103.aws`.

Anda bisa mendapatkan paket Lustre dari repositori Ubuntu 18.04 Amazon FSx. Untuk memvalidasi bahwa isi repositori belum diotak-atik sebelum atau selama pengunduhan, tanda tangan GNU Privacy Guard (GPG) diterapkan ke metadata repositori. Instalasi repositori gagal kecuali Anda telah menginstal kunci GPG publik yang sesuai pada sistem Anda.

1. Buka terminal pada klien Anda.
2. Ikuti langkah-langkah berikut untuk menambahkan repositori Amazon FSx Ubuntu:
 - a. Jika sebelumnya Anda belum mendaftarkan repositori Amazon FSx Ubuntu pada instans klien Anda, unduh dan instal kunci publik yang diperlukan. Gunakan perintah berikut ini.

```
wget -O - https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-ubuntu-public-key.asc | gpg --dearmor | sudo tee /usr/share/keyrings/fsx-ubuntu-public-key.gpg >/dev/null
```

- b. Tambahkan repositori paket Amazon FSx ke pengelola paket lokal Anda menggunakan perintah berikut.

```
sudo bash -c 'echo "deb [signed-by=/usr/share/keyrings/fsx-ubuntu-public-key.gpg] https://fsx-lustre-client-repo.s3.amazonaws.com/ubuntu bionic main" > /etc/apt/sources.list.d/fsxlustreclientrepo.list && apt-get update'
```

3. Tentukan kernel mana yang sedang berjalan pada instans klien Anda, dan perbarui sesuai kebutuhan. Klien Lustre di Ubuntu 18.04 memerlukan kernel 4.15.0-1054-aws atau yang lebih baru untuk instans EC2 berbasis x86 dan kernel 5.3.0-1023-aws atau yang lebih baru untuk instans EC2 berbasis ARM yang didukung oleh prosesor Graviton. AWS

- a. Jalankan perintah berikut untuk menentukan kernel mana yang sedang berjalan.

```
uname -r
```

- b. Jalankan perintah berikut untuk memperbarui ke kernel Ubuntu dan Lustre versi terbaru dan kemudian reboot.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
```

Jika versi kernel Anda lebih besar daripada 4.15.0-1054-aws instans EC2 berbasis x86, atau lebih besar dari 5.3.0-1023-aws instans EC2 berbasis Graviton, dan Anda tidak ingin memperbarui ke versi kernel terbaru, Anda dapat menginstal Lustre untuk kernel saat ini dengan perintah berikut.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Dua paket Lustre yang diperlukan untuk pemasangan dan interaksi dengan sistem file FSx for Lustre Anda diinstal. Anda dapat memilih menginstal paket terkait tambahan, seperti paket berisi kode sumber dan paket yang berisi tes yang termasuk dalam repository.

- c. Buat daftar semua paket yang tersedia di repositori dengan menggunakan perintah berikut.

```
sudo apt-cache search ^lustre
```

- d. (Opsional) Jika Anda ingin upgrade sistem Anda juga selalu meng-upgrade modul klien Lustre, pastikan bahwa paket `lustre-client-modules-aws` diinstal menggunakan perintah berikut.

```
sudo apt install -y lustre-client-modules-aws
```

Note

Jika Anda mendapatkan `Module Not Found` kesalahan, lihat [Untuk memecahkan masalah kesalahan modul yang hilang](#).

Untuk memecahkan masalah kesalahan modul yang hilang

Jika Anda mendapatkan `Module Not Found` kesalahan saat menginstal pada versi Ubuntu apa pun, lakukan hal berikut:

Turunkan kelas kernel Anda ke versi terakhir yang didukung. Buat daftar semua versi `lustre-client-modules` paket yang tersedia dan instal kernel yang sesuai. Untuk melakukannya, gunakan perintah berikut.

```
sudo apt-cache search lustre-client-modules
```

Misalnya, jika versi terbaru yang disertakan dalam repositori adalah `lustre-client-modules-5.4.0-1011-aws`, lakukan hal berikut:

1. Instal kernel yang menjadi tujuan dibuatnya paket ini untuk menggunakan perintah berikut.

```
sudo apt-get install -y linux-image-5.4.0-1011-aws
```

```
sudo sed -i 's/GRUB_DEFAULT=.\/+\/GRUB\_DEFAULT="Advanced options for Ubuntu>Ubuntu,  
with Linux 5.4.0-1011-aws"/' /etc/default/grub
```

```
sudo update-grub
```

2. Mulai ulang instans Anda menggunakan perintah berikut.

```
sudo reboot
```

3. Instal klien Lustre menggunakan perintah berikut.

```
sudo apt-get install -y lustre-client-modules-$(uname -r)
```

SUSE Linux

Untuk menginstal klien Lustre pada SUSE Linux 12 SP3, SP4, atau SP5

Untuk menginstal klien Lustre di SUSE Linux 12 SP3

1. Buka terminal pada klien Anda.
2. Instal kunci publik rpm Amazon FSx dengan menggunakan perintah berikut.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Impor kunci dengan menggunakan perintah berikut.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Tambahkan repositori untuk klien Lustre menggunakan perintah berikut.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Unduh dan Instal klien Lustre menggunakan perintah berikut.

```
sudo zypper ar --pgpcheck-strict fsx-lustre-client.repo
sudo sed -i 's#SLES-12#SP3#' /etc/zypp/repos.d/aws-fsx.repo
sudo zypper refresh
sudo zypper in lustre-client
```

Untuk menginstal klien Lustre di SUSE Linux 12 SP4

1. Buka terminal pada klien Anda.

2. Instal kunci publik rpm Amazon FSx dengan menggunakan perintah berikut.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Impor kunci dengan menggunakan perintah berikut.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Tambahkan repositori untuk klien Lustre menggunakan perintah berikut.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Lakukan salah satu hal berikut ini:

- Jika Anda menginstal SP4 secara langsung, unduh dan instal klien Lustre dengan perintah berikut.

```
sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo  
sudo sed -i 's#SLES-12#SP4#' /etc/zypp/repos.d/aws-fsx.repo  
sudo zypper refresh  
sudo zypper in lustre-client
```

- Jika Anda bermigrasi dari SP3 ke SP4 dan sebelumnya menambahkan repositori Amazon FSx untuk SP3, unduh dan instal klien Lustre dengan perintah berikut.

```
sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo  
sudo sed -i 's#SP3#SP4#' /etc/zypp/repos.d/aws-fsx.repo  
sudo zypper ref  
sudo zypper up --force-resolution lustre-client-kmp-default
```

Untuk menginstal klien Lustre di SUSE Linux 12 SP5

1. Buka terminal pada klien Anda.
2. Instal kunci publik rpm Amazon FSx dengan menggunakan perintah berikut.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Impor kunci dengan menggunakan perintah berikut.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Tambahkan repositori untuk klien Lustre menggunakan perintah berikut.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Lakukan salah satu hal berikut ini:

- Jika Anda menginstal SP5 secara langsung, unduh dan instal klien Lustre dengan perintah berikut.

```
sudo zypper ar --gpcheck-strict fsx-lustre-client.repo
sudo zypper refresh
sudo zypper in lustre-client
```

- Jika Anda bermigrasi dari SP4 ke SP5 dan sebelumnya menambahkan repositori Amazon FSx untuk SP4, unduh dan instal klien Lustre dengan perintah berikut.

```
sudo sed -i 's#SP4#SLES-12' /etc/zypp/repos.d/aws-fsx.repo
sudo zypper ref
sudo zypper up --force-resolution lustre-client-kmp-default
```

Note

Anda mungkin perlu mereboot instans komputasi Anda untuk klien untuk menyelesaikan penginstalan.

Pemasangan dari instans Amazon Elastic Compute Cloud

Anda dapat memasang sistem file Anda dari instans Amazon EC2.

Untuk memasang sistem file Anda dari Amazon EC2

1. Connect ke instans Amazon EC2 Anda.

2. Buat direktori pada sistem file FSx for Lustre Anda untuk titik pemasangan dengan perintah berikut.

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

3. Pasang sistem file Amazon FSx for Lustre ke direktori yang Anda buat. Gunakan perintah berikut dan ganti item berikut:

- Ganti *file_system_dns_name* dengan nama DNS sistem file yang sebenarnya.
- Ganti *mountname* dengan nama pemasangan sistem file. Nama pemasangan ini dikembalikan dalam respon operasi API `CreateFileSystem`. Itu juga dikembalikan sebagai respons `describe-file-systems` AWS CLI perintah, dan operasi API [DescribeFileSystem](#).

```
sudo mount -t lustre -o relatime,flock file_system_dns_name@tcp:/mountname /fsx
```

Perintah ini memasang sistem file Anda dengan dua pilihan, `-o relatime` dan `flock`:

- `relatime`— Sementara `atime` opsi mempertahankan `atime` (waktu akses inode) data untuk setiap kali file diakses, `relatime` opsi ini juga mempertahankan `atime` data, tetapi tidak untuk setiap kali file diakses. Dengan `relatime` opsi diaktifkan, `atime` data ditulis ke disk hanya jika file telah dimodifikasi sejak `atime` data terakhir diperbarui (`mtime`), atau jika file terakhir diakses lebih dari jumlah waktu tertentu yang lalu (6 jam secara default). Menggunakan salah satu `atime` opsi `relatime` or akan mengoptimalkan proses [rilis file](#).

Note

Jika beban kerja Anda memerlukan akurasi waktu akses yang tepat, Anda dapat memasang dengan opsi `atime` pemasangan. Namun, hal itu dapat memengaruhi kinerja beban kerja dengan meningkatkan lalu lintas jaringan yang diperlukan untuk mempertahankan nilai waktu akses yang tepat.

Jika beban kerja Anda tidak memerlukan waktu akses metadata, menggunakan opsi `noatime` pemasangan untuk menonaktifkan pembaruan untuk mengakses waktu dapat memberikan peningkatan kinerja. Ketahuilah bahwa proses `atime` terfokus seperti `rilis file` atau `rilis validitas data` akan menjadi tidak akurat dalam rilisnya.

- `flock` — Memungkinkan penguncian file untuk sistem file Anda. Jika Anda tidak ingin penguncian file diaktifkan, gunakan perintah `mount` tanpa `flock`.

4. Verifikasi bahwa perintah pemasangan berhasil dengan mencantumkan isi direktori yang Anda menjadi tempat pemasangan sistem file, `/mnt/fsx` dengan menggunakan perintah berikut.

```
$ ls /fsx
import-path lustre
$
```

Anda dapat juga menggunakan perintah `df` berikut.

```
$ df
Filesystem                1K-blocks    Used   Available Use% Mounted on
devtmpfs                   1001808         0    1001808  0% /dev
tmpfs                      1019760         0    1019760  0% /dev/shm
tmpfs                      1019760        392    1019368  1% /run
tmpfs                      1019760         0    1019760  0% /sys/fs/cgroup
/dev/xvda1                 8376300 1263180   7113120 16% /
123.456.789.0@tcp://mountname 3547698816  13824 3547678848  1% /fsx
tmpfs                      203956         0     203956  0% /run/user/1000
```

Hasilnya menunjukkan sistem file Amazon FSx yang dipasang pada `/fsx`.

Pemasangan dari Amazon Elastic Container Service

Anda dapat mengakses sistem file FSx for Lustre dari wadah Amazon Elastic Container Service (Amazon ECS) Service Elastic Container Docker pada instans Amazon EC2. Anda dapat melakukannya dengan menggunakan salah satu opsi berikut:

1. Dengan memasang sistem file FSx for Lustre Anda dari instans Amazon EC2 yang menghosting tugas Amazon ECS Anda, dan mengeksport titik pemasangan ini ke container Anda.
2. Dengan memasang sistem file langsung di dalam kontainer tugas Anda.

Untuk informasi selengkapnya tentang Amazon ECS, lihat [Apa Itu Amazon Elastic Container Service?](#) di Panduan Developer Amazon Elastic Container Service.

Kami merekomendasikan penggunaan opsi 1 ([Pemasangan dari instans Amazon EC2 yang menghosting tugas Amazon ECS](#)) karena menyediakan penggunaan sumber daya yang lebih baik, terutama jika Anda mulai banyak kontainer (lebih dari lima) pada instans EC2 yang sama atau jika tugas Anda berumur pendek (kurang dari 5 menit).

Gunakan opsi 2 ([Pemasangan dari wadah Docker](#)), jika Anda tidak dapat mengkonfigurasi instans EC2, atau jika aplikasi Anda memerlukan fleksibilitas kontainer.

 Note

Memasang FSx for Lustre AWS pada jenis peluncuran Fargate tidak didukung.

Bagian berikut menjelaskan prosedur untuk masing-masing opsi untuk memasang sistem file FSx for Lustre Anda dari wadah Amazon ECS.

Topik

- [Pemasangan dari instans Amazon EC2 yang menghosting tugas Amazon ECS](#)
- [Pemasangan dari wadah Docker](#)

Pemasangan dari instans Amazon EC2 yang menghosting tugas Amazon ECS

Prosedur ini menunjukkan bagaimana Anda dapat mengonfigurasi Amazon ECS pada instans EC2 untuk memasang sistem file FSx for Lustre secara lokal. Prosedur ini menggunakan properti kontainer `volumes` dan `mountPoints` untuk membagikan sumber daya dan membuat sistem file ini dapat diakses untuk menjalankan tugas secara lokal. Untuk informasi selengkapnya, lihat [Meluncurkan Instans Kontainer Amazon ECS?](#) di Panduan Developer Amazon Elastic Container Service.

Prosedur ini adalah untuk Amazon Linux 2 AMI yang Dioptimalkan Amazon ECS. Jika Anda menggunakan distribusi Linux lain, lihat [Menginstal klien Lustre](#).

Untuk memasang sistem file Anda dari Amazon ECS pada instans EC2

1. Ketika meluncurkan instans Amazon ECS, baik secara manual atau menggunakan grup Auto Scaling, tambahkan baris dalam contoh kode berikut pada akhir bidang Data pengguna. Mengganti item berikut dalam contoh:
 - Ganti `file_system_dns_name` dengan nama DNS sistem file yang sebenarnya.
 - Ganti `mountname` dengan nama pemasangan sistem file.
 - Ganti `mountpoint` dengan titik pasang sistem file, yang perlu Anda buat.

```
#!/bin/bash

...<existing user data>...

fsx_dnsname=file_system_dns_name
fsx_mountname=mountname
fsx_mountpoint=mountpoint
amazon-linux-extras install -y lustre
mkdir -p "$fsx_mountpoint"
mount -t lustre ${fsx_dnsname}@tcp:/${fsx_mountname} ${fsx_mountpoint} -o
    relatime,flock
```

2. Saat membuat tugas Amazon ECS Anda, tambahkan properti kontainer volumes dan mountPoints berikut dalam definisi JSON. Ganti *mountpoint* dengan titik pasang sistem file (seperti /mnt/fsx).

```
{
  "volumes": [
    {
      "host": {
        "sourcePath": "mountpoint"
      },
      "name": "Lustre"
    }
  ],
  "mountPoints": [
    {
      "containerPath": "mountpoint",
      "sourceVolume": "Lustre"
    }
  ],
}
```

Pemasangan dari wadah Docker

Prosedur berikut menunjukkan bagaimana Anda dapat mengonfigurasi wadah tugas Amazon ECS untuk menginstal `lustre-client` paket dan memasang sistem file FSx for Lustre Anda di dalamnya. Prosedur ini menggunakan Amazon Linux (`amazonlinux`) Docker image, tetapi pendekatan serupa dapat bekerja untuk distribusi lain.

Untuk memasang sistem file Anda dari kontainer Docker

1. Pada wadah Docker Anda, instal `lustre-client` paket dan pasang sistem file FSx for Lustre Anda dengan properti. `command` Mengganti item berikut dalam contoh:
 - Ganti `file_system_dns_name` dengan nama DNS sistem file yang sebenarnya.
 - Ganti `mountname` dengan nama pemasangan sistem file.
 - Ganti `mountpoint` dengan titik pasang sistem file.

```
"command": [
  "/bin/sh -c \"amazon-linux-extras install -y lustre; mount -t
  lustre file_system_dns_name@tcp:/mountname mountpoint -o relatime,flock;\""
],
```

2. Tambahkan `SYS_ADMIN` kemampuan ke wadah Anda untuk mengotorisasi untuk me-mount sistem file FSx for Lustre Anda, menggunakan properti. `linuxParameters`

```
"linuxParameters": {
  "capabilities": {
    "add": [
      "SYS_ADMIN"
    ]
  }
}
```

Memasang sistem file Amazon FSx dari on-premise atau Amazon VPC hasil peering

Anda dapat mengakses sistem file Amazon FSx Anda dengan dua cara. Cara pertama adalah dari instans Amazon EC2 yang terletak di Amazon VPC yang di-peering-kan ke VPC sistem file. Yang lainnya adalah dari klien lokal yang terhubung ke VPC sistem file Anda AWS Direct Connect menggunakan atau VPN.

Anda menghubungkan VPC klien dan VPC sistem file Amazon FSx Anda menggunakan koneksi peering VPC atau VPC transit gateway. Ketika Anda menggunakan koneksi peering VPC atau transit gateway untuk menghubungkan VPC, instans Amazon EC2 yang dalam satu VPC dapat mengakses sistem file Amazon FSx di VPC lain, bahkan jika kedua VPC milik akun yang berbeda.

Sebelum menggunakan prosedur berikut ini, Anda perlu mengatur koneksi peering VPC atau VPC transit gateway.

Transit gateway adalah hub transit jaringan yang dapat Anda gunakan untuk saling menghubungkan VPC Anda dan jaringan on-premise. Untuk informasi selengkapnya tentang menggunakan VPC transit gateway, lihat [Memulai dengan Transit Gateway](#) dalam Panduan Transit Gateway Amazon VPC.

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

Anda dapat memasang sistem file Anda dari luar VPC-nya menggunakan alamat IP dari antarmuka jaringan utamanya. Antarmuka jaringan utama adalah antarmuka jaringan pertama yang dikembalikan ketika Anda menjalankan `aws fsx describe-file-systems` AWS CLI perintah. Anda juga bisa mendapatkan alamat IP ini dari Konsol Manajemen Amazon Web Services.

Tabel berikut menggambarkan persyaratan alamat IP untuk mengakses sistem file Amazon FSx menggunakan klien yang berada di luar VPC sistem file.

Untuk klien yang berlokasi di...	Akses ke sistem file yang dibuat sebelum 17 Desember 2020	Akses ke sistem file yang dibuat pada atau setelah 17 Desember 2020
VPC yang di-peering-kan menggunakan peering VPC atau AWS Transit Gateway	Klien dengan alamat IP di rentang alamat IP privat RFC 1918 :	✓
Jaringan peered menggunakan AWS Direct Connect atau AWS VPN	<ul style="list-style-type: none"> • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16 	✓

Jika Anda perlu mengakses sistem file Amazon FSx yang dibuat sebelum 17 Desember 2020 menggunakan rentang alamat IP non-privat, Anda dapat membuat sistem file baru dengan memulihkan backup sistem file. Untuk informasi selengkapnya, lihat [Bekerja dengan backup](#).

Untuk mengambil alamat IP dari antarmuka jaringan utama untuk sistem file

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi, pilih Sistem file.
3. Pilih sistem file Anda dari dasbor.
4. Dari halaman rincian sistem file, pilih Jaringan & keamanan.
5. Untuk Antarmuka jaringan, pilih ID untuk antarmuka jaringan elastis utama Anda. Melakukan hal ini akan membawa Anda ke konsol Amazon EC2.
6. Pada tab Rincian, temukan IP IPv4 privat utama. Ini adalah alamat IP untuk antarmuka jaringan utama Anda.

Note

Anda tidak dapat menggunakan resolusi nama Sistem Nama Domain (DNS) saat memasang sistem file Amazon FSx dari luar VPC yang terkait dengannya.

Memasang sistem file Amazon FSx Anda secara otomatis

Anda dapat memperbarui file `/etc/fstab` dalam instans Amazon EC2 Anda setelah Anda menghubungkan instans tersebut untuk pertama kalinya sehingga akan memasang sistem file Amazon FSx Anda setiap kali reboot.

Menggunakan `/etc/fstab` untuk me-mount FSx for Lustre secara otomatis

Untuk secara otomatis memasang direktori sistem file Amazon FSx Anda ketika instans Amazon EC2 reboot, Anda dapat menggunakan file `fstab`. File `fstab` berisi informasi tentang sistem file. Perintah `mount -a`, yang berjalan selama startup instans, memasang sistem file yang tercantum dalam file `fstab`.

Note

Sebelum Anda dapat memperbarui file `/etc/fstab` instans EC2 Anda, pastikan bahwa Anda telah membuat sistem file Amazon FSx Anda. Untuk informasi selengkapnya, lihat [Buat sistem file FSx for Lustre Anda](#) dalam latihan Memulai.

Untuk memperbarui file `/etc/fstab` di instans EC2 Anda

1. Connect ke instans EC2 Anda, dan buka file `/etc/fstab` dalam editor.
2. Tambahkan baris berikut ke file `/etc/fstab`.

Pasang sistem file Amazon FSx for Lustre ke direktori yang Anda buat. Gunakan perintah berikut dan ganti yang berikut:

- Ganti `/fsx` dengan direktori yang Anda inginkan menjadi tempat untuk memasang sistem file Amazon FSx Anda.
- Ganti `file_system_dns_name` dengan nama DNS sistem file yang sebenarnya.
- Ganti `mounname` dengan nama pemasangan sistem file. Nama pemasangan ini dikembalikan dalam respon operasi API `CreateFileSystem`. Itu juga dikembalikan sebagai respons `describe-file-systems` AWS CLI perintah, dan operasi [DescribeFileSystems](#) API.

```
file_system_dns_name@tcp:/mounname /fsx lustre defaults,relatime,flock,_netdev,x-systemd.automount,x-systemd.requires=network.service 0 0
```

Warning

Gunakan opsi `_netdev`, yang digunakan untuk mengidentifikasi sistem file jaringan, ketika memasang sistem file Anda secara otomatis. Jika `_netdev` hilang, instans EC2 Anda mungkin berhenti merespons. Hasil ini didapatkan karena sistem file jaringan perlu diinisialisasi setelah instans komputasi memulai jaringannya. Untuk informasi selengkapnya, lihat [Pemasangan otomatis gagal dan instans tidak responsif](#).

3. Simpan perubahan pada file.

Instans EC2 Anda sekarang dikonfigurasi untuk memasang sistem file Amazon FSx setiap kali sistem dinyalakan ulang.

Note

Dalam beberapa kasus, instans Amazon EC2 Anda mungkin perlu memulai terlepas dari status sistem file Amazon FSx yang terpasang. Dalam kasus ini, tambahkan opsi `nofail` ke entri sistem file Anda di file `/etc/fstab`.

Bidang-bidang di baris kode yang Anda tambahkan ke file `/etc/fstab` melakukan hal berikut.

Bidang	Deskripsi
<code>file_system_dns_name</code>	Nama DNS untuk sistem file Amazon FSx Anda, yang mengidentifikasi sistem file. Anda bisa mendapatkan nama ini dari konsol atau secara terprogram dari AWS CLI atau SDK. AWS
<code>mountname</code>	Nama pemasangan untuk sistem file. Anda bisa mendapatkan nama ini dari konsol atau secara terprogram dari AWS CLI menggunakan <code>describe-file-systems</code> perintah atau AWS API atau SDK menggunakan operasi. DescribeFileSystems
<code>/fsx</code>	Titik pemasangan untuk sistem file Amazon FSx pada instans EC2 Anda.
<code>lustre</code>	Jenis sistem file, Amazon FSx.
<code>mount options</code>	<p>Opsi pemasangan untuk sistem file, yang disajikan sebagai daftar yang dipisahkan koma dari opsi berikut:</p> <ul style="list-style-type: none"> <code>defaults</code> — Nilai ini memberitahu sistem operasi untuk menggunakan opsi pemasangan default. Anda dapat mencantumkan opsi pemasangan default setelah sistem file telah dipasang dengan menampilkan output perintah <code>mount</code>. <code>relatime</code>— Opsi ini mempertahankan <code>atime</code> (waktu akses inode) data, tetapi tidak untuk setiap kali file diakses. Dengan opsi ini diaktifkan, <code>atime</code> data ditulis ke disk hanya jika file telah dimodifikasi sejak <code>atime</code> data terakhir diperbarui (<code>mtime</code>), atau jika file terakhir diakses lebih dari jumlah waktu tertentu yang lalu (satu hari secara default). Jika Anda ingin mematikan pembaruan waktu akses inode, gunakan opsi <code>noatime</code> mount sebagai gantinya. <code>lock</code> — memasang sistem file Anda dengan penguncian file yang diaktifkan. Jika Anda tidak ingin penguncian file diaktifkan, gunakan opsi <code>noatime</code> mount sebagai gantinya. <code>_netdev</code> — Nilai ini memberitahu sistem operasi bahwa sistem file berada di perangkat yang memerlukan akses jaringan. Opsi

Bidang	Deskripsi
	ini mencegah instans memasang sistem file sampai jaringan telah diaktifkan pada klien.
<code>x-systemd .automount,x- systemd.requires=network.service</code>	<p>Opsi ini memastikan bahwa auto mounter tidak berjalan sampai konektivitas jaringan online.</p> <div data-bbox="505 464 1507 779" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note</p> <p>Untuk Amazon Linux 2023 dan Ubuntu 22.04, gunakan <code>x-systemd.requires=systemd-networkd-wait-online.service</code> opsi alih-alih opsi. <code>x-systemd.requires=network.service</code></p> </div>
0	Nilai yang menunjukkan apakah sistem file harus didukung oleh dump. Untuk Amazon FSx, nilai ini seharusnya 0.
0	Sebuah nilai yang menunjukkan urutan <code>fsck</code> memeriksa sistem file pada boot. Untuk sistem file Amazon FSx, nilai ini harus 0 untuk menunjukkan bahwa <code>fsck</code> seharusnya tidak berjalan saat startup.

Memasang fileset spesifik

Dengan menggunakan fitur fileset Lustre, Anda dapat memasang hanya subset dari namespace sistem file, yang disebut fileset. Untuk memasang fileset dari sistem file, pada klien Anda menyebutkan path subdirektori setelah nama sistem file. Pemasangan fileset (juga disebut pemasangan subdirektori) membatasi visibilitas namespace sistem file pada klien tertentu.

Contoh - Pasang fileset Lustre

1. Asumsikan Anda memiliki sistem file FSx for Lustre dengan direktori berikut:

```
team1/dataset1/  
team2/dataset2/
```

2. Anda hanya memasang fileset `team1/dataset1`, membuat hanya bagian ini dari sistem file yang terlihat secara lokal pada klien. Gunakan perintah berikut dan ganti item berikut:

- Ganti *file_system_dns_name* dengan nama DNS sistem file yang sebenarnya.
- Ganti *mountname* dengan nama pemasangan sistem file. Nama pemasangan ini dikembalikan dalam respon operasi API CreateFileSystem. Itu juga dikembalikan sebagai respons describe-file-systems AWS CLI perintah, dan operasi API [DescribeFileSistem](#).

```
mount -t lustre file_system_dns_name@tcp://mountname/team1/dataset1 /fsx
```

Saat menggunakan fitur fileset Lustre, perhatikan hal berikut:

- Tidak ada kendala yang mencegah klien dari memasang kembali sistem file menggunakan fileset yang berbeda, atau tidak ada fileset sama sekali.
- Ketika menggunakan fileset, beberapa perintah administratif Lustre yang memerlukan akses ke `.lustre/` mungkin tidak bekerja, seperti perintah `lfs fid2path`.
- Jika Anda berencana untuk memasang beberapa subdirektori dari sistem file yang sama pada host yang sama, perhatikan bahwa ini membutuhkan lebih banyak sumber daya daripada satu titik pemasangan, dan bisa lebih efisien untuk memasang direktori root sistem file hanya sekali.

Untuk informasi selengkapnya tentang fitur fileset Lustre, lihat Operasi Manual Lustre di [Situs web dokumentasi Lustre](#).

Melepaskan sistem file

Sebelum Anda menghapus sistem file, kami sarankan Anda melepaskannya dari setiap instans Amazon EC2 yang terhubung dengannya. Anda dapat melepaskan sistem file pada instans Amazon EC2 Anda dengan menjalankan perintah `umount` pada instans itu sendiri. Anda tidak dapat melepas sistem file Amazon FSx melalui AWS CLI, file, AWS Management Console atau melalui SDK mana pun. AWS Untuk melepaskan sistem file Amazon FSx yang terhubung ke instans Amazon EC2 yang menjalankan Linux, gunakan perintah `umount` sebagai berikut:

```
umount /mnt/fsx
```

Kami menyarankan Anda untuk tidak menentukan pilihan `umount` lainnya. Hindari pengaturan pilihan `umount` lainnya yang berbeda dari default.

Anda dapat memverifikasi bahwa sistem file Amazon FSx Anda telah dilepas dengan menjalankan perintah `df`. Perintah ini menampilkan statistik penggunaan disk untuk sistem file yang saat ini dipasang pada instans Amazon EC2 berbasis Linux Anda. Jika sistem file Amazon FSx yang ingin Anda lepaskan tidak tercantum dalam output perintah `df`, ini berarti bahwa sistem file sudah dilepaskan.

Example — Identifikasi status pemasangan dari sistem file Amazon FSx dan lepaskan

```
$ df -T
Filesystem Type 1K-blocks Used Available Use% Mounted on
file-system-id.fsx.aws-region.amazonaws.com@tcp:/mountname /fsx 3547708416 61440
3547622400 1% /fsx
/dev/sda1 ext4 8123812 1138920 6884644 15% /
```

```
$ umount /fsx
```

```
$ df -T
```

```
Filesystem Type 1K-blocks Used Available Use% Mounted on
/dev/sda1 ext4 8123812 1138920 6884644 15% /
```

Mengerjakan Instans Spot Amazon EC2

FSx for Lustre dapat digunakan dengan Instans Spot EC2 untuk menurunkan biaya Amazon EC2 Anda secara signifikan. Instans Spot adalah instans EC2 yang tidak digunakan yang tersedia dengan harga lebih rendah dari harga Sesuai Permintaan. Amazon EC2 dapat menginterupsi Instans Spot Anda saat harga Spot melebihi harga maksimum Anda, saat permintaan Instans Spot naik, atau saat pasokan Instans Spot menurun.

Saat menginterupsi Instans Spot, Amazon EC2 memberikan pemberitahuan interupsi Instans Spot, yang memberi instans peringatan dua menit sebelum Amazon EC2 menginterupsi. Untuk informasi selengkapnya, lihat [Instans Spot](#) di Panduan Pengguna Amazon EC2.

Untuk memastikan bahwa sistem file Amazon FSx tidak terpengaruh oleh Interupsi Instans Spot EC2, kami sarankan untuk melepaskan sistem file Amazon FSx sebelum mengakhiri atau menidurkan Instans Spot EC2. Untuk informasi selengkapnya, lihat [Melepaskan sistem file](#).

Menangani Interupsi Instans Spot Amazon EC2

FSx for Lustre adalah sistem file terdistribusi di mana server dan instance klien bekerja sama untuk menyediakan sistem file yang berkinerja dan andal. Instans-instans ini mempertahankan keadaan terdistribusi dan koheren baik di instans klien maupun server. Server FSx for Lustre mendelegasikan izin akses sementara ke klien saat mereka secara aktif melakukan I/O dan caching data sistem file. Klien diharapkan untuk membalas dalam waktu singkat ketika server meminta mereka untuk mencabut izin akses sementara mereka. Untuk melindungi sistem file dari klien yang berperilaku buruk, server dapat mengusir klien Lustre yang tidak merespons setelah beberapa menit. Agar tidak harus menunggu beberapa menit untuk klien yang tidak merespons untuk membalas permintaan server, penting untuk melepaskan klien Lustre, terutama sebelum mengakhiri Instans Spot EC2.

EC2 Spot mengirimkan pemberitahuan penghentian 2 menit sebelum mematikan sebuah instans. Kami merekomendasikan Anda mengotomatisasi proses pelepasan total klien Lustre sebelum mengakhiri Instans Spot EC2.

Example — Skrip untuk melepaskan total Instans Spot EC2 yang mengakhiri

Contoh skrip ini secara total melepaskan Instans Spot EC2 yang mengakhiri dengan melakukan hal berikut:

- Melihat pemberitahuan Spot pengakhiran.
- Ketika menerima pemberitahuan pengakhiran:
 - Hentikan aplikasi yang mengakses sistem file.
 - Lepaskan sistem file sebelum instans diakhiri.

Anda dapat menyesuaikan skrip sesuai kebutuhan, terutama untuk mematikan aplikasi Anda dengan benar. Untuk informasi lebih lanjut tentang praktik terbaik untuk menangani interupsi Spot Instans, lihat [Praktik terbaik untuk menangani interupsi Instans Spot EC2](#).

```
#!/bin/bash

# TODO: Specify below the FSx mount point you are using
*FSXPATH=/fsx*

cd /

TOKEN=$(curl -s -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 21600")
```

```
if [ "$?" -ne 0 ]; then
    echo "Error running 'curl' command" >&2
    exit 1
fi

# Periodically check for termination
while sleep 5
do

    HTTP_CODE=$(curl -H "X-aws-ec2-metadata-token: $TOKEN" -s -w %{http_code} -o /dev/
null http://169.254.169.254/latest/meta-data/instance-action)

    if [[ "$HTTP_CODE" -eq 401 ]] ; then
        # Refreshing Authentication Token
        TOKEN=$(curl -s -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-
metadata-token-ttl-seconds: 30")
        continue
    elif [[ "$HTTP_CODE" -ne 200 ]] ; then
        # If the return code is not 200, the instance is not going to be interrupted
        continue
    fi

    echo "Instance is getting terminated. Clean and unmount '$FSXPATH' ..."
    curl -H "X-aws-ec2-metadata-token: $TOKEN" -s http://169.254.169.254/latest/meta-
data/instance-action
    echo

    # Gracefully stop applications accessing the filesystem
    #
    # TODO*: Replace with the proper command to stop your application if possible*

    # Kill every process still accessing Lustre filesystem
    echo "Kill every process still accessing Lustre filesystem..."
    fuser -kMm -TERM "${FSXPATH}"; sleep 2
    fuser -kMm -KILL "${FSXPATH}"; sleep 2

    # Unmount FSx For Lustre filesystem
    if ! umount -c "${FSXPATH}"; then
        echo "Error unmounting '$FSXPATH'. Processes accessing it:" >&2
        lsof "${FSXPATH}"

        echo "Retrying..."
        continue
    fi
fi
```

```
# Start a graceful shutdown of the host  
shutdown now
```

```
done
```

Mengelola sistem file

FSx for Lustre menyediakan serangkaian fitur yang menyederhanakan kinerja tugas administratif Anda. Ini termasuk kemampuan untuk mengambil point-in-time cadangan, untuk mengelola kuota penyimpanan sistem file, untuk mengelola kapasitas penyimpanan dan throughput Anda, untuk mengelola kompresi data, dan untuk mengatur jendela pemeliharaan untuk melakukan patching perangkat lunak rutin sistem.

Anda dapat mengelola sistem file FSx for Lustre menggunakan Amazon FSx Management AWS Command Line Interface Console, (), Amazon FSx API AWS CLI, atau SDK. AWS

Topik

- [Bekerja dengan backup](#)
- [Kuota penyimpanan](#)
- [Mengelola kapasitas penyimpanan](#)
- [Mengelola kinerja metadata](#)
- [Mengelola kapasitas throughput](#)
- [Kompresi data Lustre](#)
- [Labu akar kilau](#)
- [FSx for Lustre status sistem berkas](#)
- [Tandai sumber daya Amazon FSx Anda](#)
- [Jendela pemeliharaan Amazon FSx for Lustre](#)
- [Menghapus sistem file](#)

Bekerja dengan backup

Dengan Amazon FSx for Lustre, Anda dapat melakukan backup harian otomatis dan backup yang diinisiasi pengguna dari sistem file persisten yang tidak tertaut dengan repositori data tahan lama Amazon S3. Cadangan Amazon FSx, sangat tahan lama file-system-consistent, dan inkremental. Untuk memastikan daya tahan tinggi, Amazon FSx for Lustre menyimpan backup di Amazon Simple Storage Service (Amazon S3) dengan daya tahan 99,999999999% (11 9's).

Pencadangan sistem file FSx for Lustre adalah pencadangan inkremental berbasis blok, baik yang dihasilkan menggunakan pencadangan harian otomatis atau fitur pencadangan yang

diprakersai pengguna. Hal ini berarti bahwa ketika Anda membuka sebuah backup, Amazon FSx membandingkan data pada sistem file Anda dengan backup sebelumnya di tingkat blok. Kemudian Amazon FSx menyimpan salinan semua perubahan tingkat blok di backup yang baru. Data tingkat-blok yang tidak mengalami perubahan dibandingkan dengan backup sebelumnya maka tidak disimpan di backup yang baru. Durasi proses backup tergantung pada seberapa banyak data telah berubah sejak backup yang terakhir diambil dan pada ketidaktergantungan kapasitas penyimpanan sistem file. Daftar berikut menggambarkan waktu backup dalam situasi yang berbeda-beda:

- Backup awal sebuah sistem file yang sangat baru dengan data yang sangat sedikit memakan waktu beberapa menit saja untuk menyelesaikan.
- Backup awal dari sistem file yang benar-benar baru baru yang diambil setelah memuat data berukuran TB akan membutuhkan waktu berjam-jam untuk menyelesaikan.
- Backup kedua yang diambil dari sistem file dengan data berukuran TB dengan perubahan yang sangat sedikit pada data tingkat blok (pembuatan/modifikasi data yang relatif sedikit) hanya membutuhkan waktu beberapa detik untuk menyelesaikannya.
- Backup ketiga dari sistem file yang sama setelah terdapat sejumlah besar data yang ditambahkan dan dimodifikasi akan membutuhkan waktu berjam-jam untuk menyelesaikannya.

Saat Anda menghapus sebuah backup, hanya data yang unik dari backup tersebut yang dihapus. Setiap cadangan FSx for Lustre berisi semua informasi yang diperlukan untuk membuat sistem file baru dari cadangan, secara efektif point-in-time memulihkan snapshot dari sistem file.

Membuat backup reguler untuk sistem file Anda adalah praktik terbaik yang melengkapi replikasi yang Amazon FSx for Lustre lakukan untuk sistem file Anda. Backup Amazon FSx membantu mendukung penyimpanan backup dan keperluan kepatuhan Anda. Bekerja dengan backup Amazon FSx for Lustre sangatlah mudah, apakah Anda mau membuat backup, menyalin backup, memulihkan sistem file dari backup, atau menghapus backup.

Backup tidak di-support pada sistem file scratch karena sistem file ini dirancang untuk penyimpanan sementara dan pemrosesan data jangka pendek. Backup tidak di-support di sistem file yang tertaut ke bucket Amazon S3 karena bucket S3 berfungsi sebagai repositori data utama, dan sistem file Lustre tidak selalu berisikan set data yang lengkap setiap saat.

Topik

- [Dukungan Backup di FSx for Lustre](#)
- [Bekerja dengan backup harian otomatis](#)
- [Bekerja dengan backup yang diinisiasi pengguna](#)

- [Menggunakan AWS Backup dengan Amazon FSx](#)
- [Menyalin cadangan](#)
- [Menyalin cadangan dalam hal yang sama Akun AWS](#)
- [Memulihkan cadangan](#)
- [Menghapus cadangan](#)

Dukungan Backup di FSx for Lustre

Cadangan hanya didukung pada sistem file persisten FSx for Lustre yang tidak ditautkan ke repositori data Amazon S3.

Amazon FSx tidak men-support backup pada sistem file scratch karena sistem file scratch dirancang untuk penyimpanan sementara dan pemrosesan data jangka pendek. Amazon FSx tidak men-support backup pada sistem file yang tertaut ke bucket Amazon S3 karena bucket S3 berfungsi sebagai repositori data utama dan sistem file tidak selalu berisikan set data yang lengkap setiap saat. Untuk informasi selengkapnya, lihat [Ops deployment sistem file](#) dan [Menggunakan repositori data](#).

Bekerja dengan backup harian otomatis

Amazon FSx for Lustre dapat mengambil backup harian otomatis dari sistem file Anda. Backup harian otomatis ini terjadi selama jendela backup harian yang diberlakukan saat Anda membuat sistem file. Beberapa kali selama jendela backup otomatis, I/O penyimpanan dapat ditangguhkan sebentar sementara proses backup dimulai (biasanya kurang dari beberapa detik). Ketika Anda memilih jendela backup harian Anda, sebaiknya Anda memilih waktu yang tepat dalam sehari. Waktu backup harian idealnya berada di luar jam operasi biasa untuk aplikasi yang menggunakan sistem file.

Backup harian otomatis disimpan untuk satu jangka waktu tertentu, yang dikenal sebagai periode penyimpanan. Anda dapat mengatur periode penyimpanan backup menjadi antara 0–90 hari. Pengaturan periode penyimpanan ke 0 (nol) hari akan mematikan backup harian otomatis. Periode penyimpanan default untuk backup harian otomatis adalah 0 hari. Backup harian otomatis dihapus saat sistem file dihapus.

Note

Pengaturan periode penyimpanan ke 0 hari berarti sistem file Anda tidak pernah dicadangkan secara otomatis. Kami sangat menyarankan Anda menggunakan backup harian otomatis

untuk sistem file yang memiliki fungsionalitas dengan tingkat kepentingan apa saja yang ter-associate dengan sistem file.

Anda dapat menggunakan salah satu AWS SDK untuk mengubah jendela cadangan dan periode penyimpanan cadangan untuk sistem file Anda. AWS CLI Gunakan operasi API [UpdateFileSystem](#) atau perintah CLI [update-file-system](#).

Bekerja dengan backup yang diinisiasi pengguna

Amazon FSx for Lustre memungkinkan Anda untuk secara manual mengambil backup dari sistem file Anda kapan saja. Anda dapat melakukannya menggunakan konsol Amazon FSx for Lustre, API, atau AWS Command Line Interface (CLI). Backup Anda yang diinisiasi pengguna dari sistem file Amazon FSx tidak pernah kedaluwarsa, dan backup tersedia selama Anda ingin menyimpannya. Backup yang diinisiasi pengguna dipertahankan bahkan setelah Anda menghapus sistem file yang di-backup. Anda dapat menghapus backup yang diinisiasi pengguna hanya dengan menggunakan konsol, API atau CLI Amazon FSx for Lustre, dan backup tersebut tidak pernah dihapus secara otomatis oleh Amazon FSx. Untuk informasi selengkapnya, lihat [Menghapus cadangan](#).

Membuat backup yang diinisiasi pengguna

Prosedur berikut memandu Anda melakukan cara untuk membuat backup yang diinisiasi pengguna di konsol Amazon FSx untuk sistem file yang sudah ada.

Untuk membuat backup sistem file yang diinisiasi pengguna

1. Buka konsol Amazon FSx for Lustre di <https://console.aws.amazon.com/fsx/>.
2. Dari dasbor konsol tersebut, pilih nama sistem file yang ingin Anda backup.
3. Dari Tindakan, pilih Buat backup.
4. Di kotak dialog Buat backup yang terbuka, berikan nama untuk backup Anda. Nama Backup dapat terdiri dari maksimal 256 karakter Unicode, termasuk huruf, spasi, angka, dan karakter khusus . + - = _ : /
5. Pilih Buat cadangan.

Anda sekarang telah membuat backup sistem file Anda. Anda dapat menemukan tabel berisi semua backup Anda di konsol Amazon FSx for Lustre dengan memilih backup di navigasi sebelah kiri. Anda

dapat mencari nama yang Anda berikan untuk backup Anda, dan tabel tersebut mem-filter hanya menunjukkan hasil yang sesuai saja.

Ketika Anda membuat backup yang diinisiasi pengguna sebagaimana yang prosedur ini jelaskan, yang berjenis `USER_INITIATED`, dan memiliki status Membuat saat Amazon FSx melakukan backup. Status berubah menjadi Mentransfer sementara backup ditransfer ke Amazon S3, sampai sepenuhnya siap.

Menggunakan AWS Backup dengan Amazon FSx

AWS Backup adalah cara sederhana dan hemat biaya untuk melindungi data Anda dengan mencadangkan sistem file Amazon FSx Anda. AWS Backup adalah layanan cadangan terpadu yang dirancang untuk menyederhanakan pembuatan, penyalinan, pemulihan, dan penghapusan cadangan, sambil memberikan pelaporan dan audit yang lebih baik. AWS Backup membuatnya lebih mudah untuk mengembangkan strategi cadangan terpusat untuk kepatuhan hukum, peraturan, dan profesional. AWS Backup juga membuat melindungi volume AWS penyimpanan, database, dan sistem file Anda lebih sederhana dengan menyediakan tempat sentral di mana Anda dapat melakukan hal berikut:

- Konfigurasi dan audit AWS sumber daya yang ingin Anda cadangkan.
- Otomatiskan penjadwalan cadangan.
- Tetapkan kebijakan penyimpanan.
- Salin cadangan di seluruh AWS Wilayah dan di seluruh AWS akun.
- Pantau semua aktivitas backup dan pemulihan terbaru.

AWS Backup menggunakan fungsionalitas cadangan bawaan Amazon FSx. Cadangan yang diambil dari AWS Backup konsol memiliki tingkat konsistensi dan kinerja sistem file yang sama, dan opsi pemulihan yang sama dengan cadangan yang diambil melalui konsol Amazon FSx. Jika Anda menggunakannya AWS Backup untuk mengelola cadangan ini, Anda mendapatkan fungsionalitas tambahan, seperti opsi retensi tak terbatas dan kemampuan untuk membuat cadangan terjadwal sesering setiap jam. Selain itu, AWS Backup pertahankan cadangan Anda yang tidak dapat diubah bahkan setelah sistem file sumber dihapus. Hal ini membantu melindungi dari penghapusan yang tidak disengaja atau berbahaya.

Pencadangan yang diambil oleh dianggap sebagai cadangan AWS Backup yang diprakarsai pengguna, dan mereka dihitung terhadap kuota cadangan yang diprakarsai pengguna untuk Amazon FSx. Anda dapat melihat dan memulihkan cadangan yang diambil oleh AWS Backup di konsol

Amazon FSx, CLI, dan API. Cadangan yang dibuat oleh AWS Backup memiliki jenis cadangan. `AWS_BACKUP` Namun, Anda tidak dapat menghapus cadangan yang diambil AWS Backup di konsol Amazon FSx, CLI, atau API. Untuk informasi selengkapnya tentang cara menggunakan AWS Backup untuk mencadangkan sistem file Amazon FSx Anda, lihat [Bekerja dengan Sistem File Amazon FSx di Panduan Pengembang](#). AWS Backup

Menyalin cadangan

Anda dapat menggunakan Amazon FSx untuk menyalin cadangan secara manual dalam AWS akun yang sama ke AWS Wilayah lain (Salinan lintas wilayah) atau dalam Wilayah yang sama (Salinan dalam AWS wilayah). Anda dapat membuat salinan lintas wilayah hanya dalam AWS partisi yang sama. Anda dapat membuat salinan cadangan yang dimulai pengguna menggunakan konsol Amazon FSx, atau API. AWS CLI Saat Anda membuat salinan backup yang diinisiasi pengguna, salinan tersebut memiliki jenis `USER_INITIATED`.

Anda juga dapat menggunakan AWS Backup untuk menyalin cadangan di seluruh AWS Wilayah dan di seluruh akun. AWS Backup adalah layanan manajemen cadangan yang dikelola sepenuhnya yang menyediakan antarmuka pusat untuk rencana pencadangan berbasis kebijakan. Dengan pengelolaan lintas akun, Anda dapat secara otomatis menggunakan kebijakan backup untuk menerapkan rencana pencadangan di seluruh akun dalam organisasi Anda.

Salinan backup lintas wilayah Sangat berharga untuk pemulihan bencana lintas-Wilayah. Anda mengambil cadangan dan menyalinnya ke AWS Wilayah lain sehingga jika terjadi bencana di AWS Wilayah utama, Anda dapat memulihkan dari cadangan dan memulihkan ketersediaan dengan cepat di Wilayah lain AWS . Anda juga dapat menggunakan salinan cadangan untuk mengkloning kumpulan data file Anda ke AWS Wilayah lain atau dalam Wilayah yang sama AWS . Anda membuat salinan cadangan dalam AWS akun yang sama (Lintas wilayah atau Dalam wilayah) dengan menggunakan konsol Amazon FSx, AWS CLI, atau Amazon FSx for Lustre API. Anda juga dapat menggunakan [AWS Backup](#) untuk melakukan salinan backup, baik sesuai permintaan atau berbasis kebijakan.

Salinan backup lintas akun sangat berharga untuk memenuhi persyaratan kepatuhan terhadap peraturan Anda untuk menyalin backup ke akun yang terisolasi. Mereka juga menyediakan lapisan perlindungan data tambahan untuk membantu mencegah penghapusan cadangan yang tidak disengaja atau berbahaya, kehilangan kredensial, atau kompromi kunci. AWS KMS Support backup lintas akun fan-in (penyalinan backup dari beberapa akun utama ke satu akun salinan backup yang terisolasi) dan fan-out (penyalinan backup dari satu akun utama ke beberapa akun salinan backup yang terisolasi).

Anda dapat membuat salinan cadangan lintas akun AWS Backup dengan menggunakan AWS Organizations dukungan. Batasan akun untuk salinan lintas akun ditentukan oleh AWS Organizations kebijakan. Untuk informasi selengkapnya tentang penggunaan AWS Backup untuk membuat salinan cadangan lintas akun, lihat [Membuat salinan cadangan Akun AWS di](#) Panduan AWS Backup Pengembang.

Batasan salinan Backup

Berikut ini adalah beberapa batasan saat Anda menyalin cadangan:

- Salinan cadangan Lintas Wilayah hanya didukung antara dua komersial Wilayah AWS, antara Wilayah China (Beijing) dan China (Ningxia), dan antara Wilayah AWS GovCloud (AS-Timur) dan AWS GovCloud (AS-Barat), tetapi tidak di seluruh wilayah tersebut.
- Salinan backup Lintas-Wilayah tidak di-support di Wilayah-wilayah opt-in.
- Anda dapat membuat salinan cadangan In-region dalam AWS Wilayah mana pun.
- Backup sumber harus memiliki status AVAILABLE sebelum Anda dapat menyalinnya.
- Anda tidak dapat menghapus backup sumber jika sedang disalin. Mungkin ada jeda singkat antara saat backup tujuan menjadi tersedia dan ketika Anda diizinkan untuk menghapus backup sumber. Anda harus mengingat bahwa terdapat jeda jika Anda mencoba lagi menghapus backup sumber.
- Anda dapat memiliki hingga lima permintaan salinan cadangan yang sedang berlangsung ke satu AWS Wilayah tujuan per akun.

Izin untuk penyalinan backup lintas Wilayah

Anda menggunakan pernyataan kebijakan IAM untuk memberikan izin untuk melakukan operasi penyalinan backup. Untuk berkomunikasi dengan AWS Wilayah sumber untuk meminta salinan cadangan Lintas wilayah, pemohon (peran IAM atau pengguna IAM) harus memiliki akses ke cadangan sumber dan Wilayah sumber. AWS

Anda menggunakan kebijakan untuk memberikan izin melakukan tindakan CopyBackup untuk operasi penyalinan backup. Tentukan tindakan dalam bidang Action kebijakan, dan tentukan nilai sumber daya dalam bidang Resource kebijakan, sebagaimana contoh berikut ini.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```
        "Effect": "Allow",
        "Action": "fsx:CopyBackup",
        "Resource": "arn:aws:fsx:*:111122223333:backup/*"
    }
]
}
```

Untuk informasi selengkapnya tentang kebijakan IAM, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.

Salinan penuh dan bersifat tambahan

Ketika Anda menyalin cadangan ke yang berbeda Wilayah AWS dari cadangan sumber, salinan pertama adalah salinan cadangan lengkap. Setelah salinan cadangan pertama, semua salinan cadangan berikutnya ke Wilayah tujuan yang sama dalam AWS akun yang sama bersifat inkremental, asalkan Anda belum menghapus semua cadangan yang disalin sebelumnya di Wilayah tersebut dan telah menggunakan kunci yang sama. AWS KMS Jika kedua kondisi tidak terpenuhi, operasi penyalinan menghasilkan salinan backup penuh (bukan yang bersifat tambahan).

Menyalin cadangan dalam hal yang sama Akun AWS

Anda dapat menyalin cadangan sistem file FSx for Lustre menggunakan, CLI, dan API, seperti AWS Management Console yang dijelaskan dalam prosedur berikut.

Untuk menyalin sebuah backup dalam akun yang sama (Lintas-Wilayah atau Dalam-Wilayah) menggunakan konsol

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Pada panel navigasi, pilih Backup.
3. Di tabel Backup, pilih backup yang ingin Anda salin, dan kemudian pilih Salin backup.
4. Di bagian Pengaturan, lakukan hal berikut:
 - Dalam daftar Wilayah Tujuan, pilih AWS Wilayah tujuan untuk menyalin cadangan. Tujuan dapat berada di AWS Wilayah lain (salinan Lintas wilayah) atau dalam Wilayah yang sama AWS (Salinan dalam wilayah).
 - (Opsional) Pilih Salin Tag untuk menyalin tag dari backup sumber untuk backup tujuan. Jika Anda memilih Salin Tag dan juga menambahkan tag pada langkah 6, semua tag digabung.
5. Untuk Enkripsi, pilih kunci AWS KMS enkripsi untuk mengenkripsi cadangan yang disalin.

6. Untuk Tag - opsional, masukkan kunci dan nilai untuk menambahkan tag untuk backup yang disalin. Jika Anda menambahkan tag di sini dan juga Salin tag terpilih pada langkah 4, semua tag tergabung.
7. Pilih Salin cadangan.

Cadangan Anda disalin dalam hal yang sama Akun AWS ke yang dipilih Wilayah AWS.

Untuk menyalin backup dalam akun yang sama (lintas-Wilayah atau dalam-Wilayah) menggunakan CLI

- Gunakan perintah `copy-backup` CLI atau operasi [CopyBackup](#) API untuk menyalin cadangan dalam AWS akun yang sama, baik di seluruh AWS Wilayah atau di dalam Wilayah. AWS

Perintah berikut menyalin backup dengan sebuah ID backup-0abc123456789cba7 dari Wilayah us-east-1.

```
aws fsx copy-backup \  
  --source-backup-id backup-0abc123456789cba7 \  
  --source-region us-east-1
```

Respoons menunjukkan deskripsi backup yang disalin.

Anda dapat melihat cadangan Anda di konsol Amazon FSx atau secara terprogram menggunakan perintah `describe-backups` CLI atau operasi API. [DescribeBackups](#)

Memulihkan cadangan

Anda dapat menggunakan cadangan yang tersedia untuk membuat sistem file baru, secara efektif memulihkan point-in-time snapshot dari sistem file lain. Anda dapat memulihkan cadangan menggunakan konsol, AWS CLI, atau salah satu AWS SDK. Memulihkan backup ke sistem file yang baru menghabiskan waktu yang sama dengan membuat sistem file baru. Data yang dipulihkan dari backup di-lazy-load ke sistem file, pada waktu lazy-load Anda akan mengalami latensi yang sedikit lebih tinggi.

Prosedur berikut memandu Anda melakukan cara untuk memulihkan backup menggunakan konsol untuk membuat sistem file yang baru.

Note

Anda hanya dapat memulihkan cadangan Anda ke sistem file dari jenis versi Lustre yang sama, jenis penyebaran, throughput per unit penyimpanan, kapasitas penyimpanan, jenis kompresi data, dan AWS Wilayah seperti aslinya. Anda dapat meningkatkan kapasitas penyimpanan sistem file yang dipulihkan setelah tersedia. Untuk informasi selengkapnya, lihat [Mengelola kapasitas penyimpanan](#).

Untuk memulihkan sistem file dari backup

1. Buka konsol Amazon FSx for Lustre di <https://console.aws.amazon.com/fsx/>.
2. Dari dasbor konsol, pilih Backup dari navigasi sebelah kiri.
3. Pilih backup yang ingin Anda pulihkan dari tabel Backup, dan kemudian pilih Pulihkan backup.

Dengan melakukannya maka akan membuka wizard pembuatan sistem file. Wizard ini identik dengan wizard pembuatan sistem file standar, kecuali konfigurasi sistem file (misalnya, Jenis Deployment, throughput per unit penyimpanan). Namun, Anda dapat mengubah VPC yang ter-associate, dan pengaturan backup.

4. Selesaikan wizard seperti yang Anda lakukan ketika Anda membuat sistem file baru.
5. Pilih Periksa dan buat.
6. Tinjau pengaturan yang Anda pilih untuk sistem file Amazon FSx for Lustre, lalu pilih Membuat sistem file.

Anda telah memulihkan data dari backup, dan sistem file yang baru sekarang sedang dibuat. Ketika statusnya berubah menjadi AVAILABLE, Anda bisa menggunakan sistem file seperti biasa.

Menghapus cadangan

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 yang diambil oleh AWS Backup di konsol Amazon FSx, CLI, atau API.

Untuk menghapus backup

1. Buka konsol Amazon FSx for Lustre 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, konfirmasi bahwa ID cadangan tersebut mengidentifikasi cadangan yang ingin Anda hapus.
5. Konfirmasikan bahwa kotak centang dicentang untuk cadangan yang ingin Anda hapus.
6. Pilih Hapus backup.

Cadangan Anda dan semua data yang termasuk kini dihapus secara permanen dan tidak dapat dipulihkan.

Kuota penyimpanan

Anda dapat membuat kuota penyimpanan untuk pengguna, grup, dan proyek pada sistem file FSx for Lustre. Dengan kuota penyimpanan, Anda dapat membatasi jumlah ruang disk dan jumlah file yang dapat dikonsumsi pengguna, grup, atau proyek. Kuota penyimpanan secara otomatis melacak penggunaan tingkat pengguna, tingkat grup, dan tingkat proyek sehingga Anda dapat memantau konsumsi apakah Anda memilih untuk menetapkan batas penyimpanan atau tidak.

Amazon FSx memberlakukan kuota dan mencegah pengguna yang telah melampaui kuota dari menulis ke ruang penyimpanan. Ketika pengguna melebihi kuota mereka, mereka harus menghapus beberapa file yang cukup untuk sampai di bawah batas kuota sehingga mereka dapat menulis ke sistem file lagi.

Topik

- [Pemberlakuan kuota](#)
- [Jenis kuota](#)
- [Batas kuota dan masa tenggang](#)
- [Mengatur dan melihat kuota](#)
- [Kuota dan bucket terkait Amazon S3](#)
- [Kuota dan memulihkan backup](#)

Pemberlakuan kuota

Penegakan kuota pengguna, grup, dan proyek diaktifkan secara otomatis di semua sistem file FSx for Lustre. Anda tidak dapat menonaktifkan pemberlakuan kuota.

Jenis kuota

Administrator sistem dengan kredensi pengguna root AWS akun dapat membuat jenis kuota berikut:

- Kuota pengguna berlaku untuk pengguna individu. Kuota pengguna untuk pengguna tertentu dapat berbeda dengan kuota pengguna lain.
- Kuota grup berlaku untuk semua pengguna yang merupakan anggota kelompok tertentu.
- Kuota proyek berlaku untuk semua file atau direktori yang terkait dengan proyek. Sebuah proyek dapat mencakup beberapa direktori atau file individual yang terletak di direktori yang berbeda dalam sistem file.

Note

Kuota proyek hanya didukung pada Lustre versi 2.15 pada FSx for Lustre file system.

- Kuota blok membatasi jumlah ruang disk yang dapat dikonsumsi pengguna, grup, atau proyek. Anda mengkonfigurasi ukuran penyimpanan dalam kilobyte.
- Kuota inode membatasi jumlah file atau direktori yang dapat dibuat oleh pengguna, grup, atau proyek. Anda mengkonfigurasi jumlah maksimum inodes sebagai integer.

Note

Kuota default tidak didukung.

Jika Anda menetapkan kuota untuk pengguna dan grup tertentu, dan pengguna adalah anggota grup tersebut, penggunaan data pengguna berlaku untuk kedua kuota. Ini juga dibatasi oleh kedua kuota. Jika batas kuota tercapai, pengguna diblokir dari menulis ke sistem file.

Note

Kuota yang ditetapkan untuk pengguna root tidak diberlakukan. Demikian pula, menulis data sebagai pengguna akar menggunakan pemberlakuan pintasan perintah `sudo` kuota.

Batas kuota dan masa tenggang

Amazon FSx memberlakukan kuota pengguna, grup, dan proyek sebagai batas keras atau sebagai batas lunak dengan masa tenggang yang dapat dikonfigurasi.

Batas keras adalah batas mutlak. Jika pengguna melebihi batas keras mereka, alokasi blok atau inode gagal dengan pesan Kuota disk terlampaui. Pengguna yang telah mencapai batas keras kuota mereka harus menghapus cukup file atau direktori agar dapat berada di bawah batas kuota sebelum mereka dapat menulis ke sistem file lagi. Ketika masa tenggang diatur, pengguna dapat melampaui batas lunak dalam masa tenggang jika berada di bawah batas keras.

Untuk batas lunak, Anda mengkonfigurasi masa tenggang dalam hitungan detik. Batas lunak harus lebih kecil dari batas keras.

Anda dapat mengatur masa tenggang yang berbeda untuk kuota inode dan blok. Anda juga dapat mengatur masa tenggang yang berbeda untuk kuota pengguna, kuota grup, dan kuota proyek. Ketika kuota pengguna, grup, dan proyek memiliki masa tenggang yang berbeda, batas lunak berubah menjadi batas keras setelah masa tenggang salah satu kuota ini berlalu.

Ketika pengguna melebihi batas lunak, Amazon FSx mengizinkan mereka untuk terus melampaui kuota mereka sampai masa tenggang telah berlalu atau sampai batas keras tercapai. Setelah masa tenggang berakhir, batas lunak berubah menjadi batas keras, dan pengguna diblokir dari operasi penulisan lebih lanjut sampai penggunaan penyimpanan mereka kembali di bawah batas kuota blok atau kuota inode yang ditetapkan. Pengguna tidak menerima notifikasi atau peringatan ketika masa tenggang dimulai.

Mengatur dan melihat kuota

Anda mengatur kuota penyimpanan menggunakan perintah sistem file Lustre `lfs` di terminal Linux Anda. Perintah `lfs setquota` mengatur batas kuota, dan perintah `lfs quota` menampilkan informasi kuota.

Untuk informasi lebih lanjut tentang perintah kuota Lustre, lihat Operasi Manual Lustre di [Situs web dokumentasi Lustre](#).

Mengatur kuota pengguna, grup, dan proyek

Sintaks `setquota` perintah untuk mengatur kuota pengguna, grup, atau proyek adalah sebagai berikut.

```
lfs setquota {-u|--user|-g|--group|-p|--project} username|groupname|projectid
```

```
[-b block_softlimit] [-B block_hardlimit]  
[-i inode_softlimit] [-I inode_hardlimit]  
/mount_point
```

Di mana:

- -u atau --user menentukan pengguna yang akan diatur kuotanya.
- -g atau --group menentukan pengguna yang akan diatur kuotanya.
- -p atau --project menentukan proyek untuk menetapkan kuota untuk.
- -b mengatur kuota blok dengan batas lunak. -B mengatur kuota blok dengan batas keras. Baik *block_softlimit* maupun *block_hardlimit* dinyatakan dalam kilobyte, dan nilai minimumnya adalah 1024 KB.
- -i mengatur kuota inode dengan batas lunak. -I mengatur kuota inode dengan batas keras. Baik *inode_softlimit* maupun *inode_hardlimit* dinyatakan dalam jumlah inodes, dan nilai minimumnya adalah 1024 inodes.
- *mount_point* adalah direktori yang dipasang pada sistem file.

Contoh kuota pengguna: Perintah berikut menetapkan batas blok lunak 5.000 KB, batas hard block 8.000 KB, batas inode lunak 2.000, dan kuota batas inode keras 3.000 untuk sistem file yang user1 dipasang. /mnt/fsx

```
sudo lfs setquota -u user1 -b 5000 -B 8000 -i 2000 -I 3000 /mnt/fsx
```

Contoh kuota grup: Perintah berikut menetapkan batas hard block 100.000 KB untuk grup bernama group1 pada sistem file yang dipasang. /mnt/fsx

```
sudo lfs setquota -g group1 -B 100000 /mnt/fsx
```

Contoh kuota proyek: Pertama pastikan bahwa Anda telah menggunakan project perintah untuk mengaitkan file dan direktori yang diinginkan dengan proyek. Misalnya, perintah berikut mengaitkan semua file dan sub-direktori /mnt/fsxfs/dir1 direktori dengan proyek yang ID proyeknya. 100

```
sudo lfs project -p 100 -r -s /mnt/fsxfs/dir1
```

Kemudian gunakan setquota perintah untuk mengatur kuota proyek. Perintah berikut menetapkan batas soft block 307.200 KB, batas hard block 309.200 KB, batas inode lunak 10.000, dan kuota batas inode keras 11.000 untuk proyek pada sistem file yang dipasang. 250 /mnt/fsx

```
sudo lfs setquota -p 250 -b 307200 -B 309200 -i 10000 -I 11000 /mnt/fsx
```

Mengatur masa tenggang

Masa tenggang default adalah satu minggu. Anda dapat menyesuaikan masa tenggang default untuk pengguna, grup, atau proyek, menggunakan sintaks berikut.

```
lfs setquota -t {-u|-g|-p}
               [-b block_grace]
               [-i inode_grace]
               /mount_point
```

Di mana:

- `-t` menunjukkan bahwa masa tenggang akan diatur.
- `-u` mengatur masa tenggang untuk semua pengguna.
- `-g` mengatur masa tenggang untuk semua grup.
- `-p` menetapkan masa tenggang untuk semua proyek.
- `-b` mengatur masa tenggang untuk kuota blok. `-i` mengatur masa tenggang untuk kuota inode. Baik *block_grace* maupun *inode_grace* dinyatakan dalam detik integer atau dalam format XXwXXdXXhXXmXXs.
- *mount_point* adalah direktori yang dipasang pada sistem file.

Perintah berikut mengatur masa tenggang 1.000 detik untuk kuota blok pengguna dan 1 minggu dan 4 hari untuk kuota inode pengguna.

```
sudo lfs setquota -t -u -b 1000 -i 1w4d /mnt/fsx
```

Melihat kuota

Perintah `lfs quota` menampilkan informasi tentang kuota pengguna, kuota grup, kuota proyek, dan masa tenggang.

Lihat perintah kuota	Informasi kuota yang ditampilkan
<pre>lfs quota /<i>mount_point</i></pre>	Informasi kuota umum (penggunaan disk dan batas) untuk pengguna yang menjalankan perintah dan grup utama pengguna.
<pre>lfs quota -u <i>username</i> /<i>mount_point</i></pre>	Informasi kuota umum untuk pengguna tertentu. Pengguna dengan kredensi pengguna root AWS akun dapat menjalankan perintah ini untuk setiap pengguna, tetapi pengguna non-root tidak dapat menjalankan perintah ini untuk mendapatkan informasi kuota tentang pengguna lain.
<pre>lfs quota -u <i>username</i> -v /<i>mount_point</i></pre>	Informasi kuota umum untuk pengguna tertentu dan statistik kuota terperinci untuk setiap target penyimpanan objek (OST) dan target metadata (MDT). Pengguna dengan kredensi pengguna root AWS akun dapat menjalankan perintah ini untuk setiap pengguna, tetapi pengguna non-root tidak dapat menjalankan perintah ini untuk mendapatkan informasi kuota tentang pengguna lain.
<pre>lfs quota -g <i>groupname</i> /<i>mount_point</i></pre>	Informasi kuota umum untuk grup tertentu.

Lihat perintah kuota	Informasi kuota yang ditampilkan
<code>lfs quota -p <i>projectid</i> /<i>mount_point</i></code>	Informasi kuota umum untuk proyek tertentu.
<code>lfs quota -t -u /<i>mount_point</i></code>	Waktu tenggang blok dan inode untuk kuota pengguna.
<code>lfs quota -t -g /<i>mount_point</i></code>	Waktu tenggang blok dan inode untuk kuota grup.
<code>lfs quota -t -p /<i>mount_point</i></code>	Blokir dan inode waktu tenggang untuk kuota proyek.

Kuota dan bucket terkait Amazon S3

Anda dapat menautkan sistem file FSx for Lustre ke repositori data Amazon S3. Untuk informasi selengkapnya, lihat [Menautkan sistem file Anda ke bucket S3](#).

Anda dapat memilih folder tertentu atau prefiks dalam bucket S3 terkait sebagai jalur impor ke sistem file Anda. Ketika folder di Amazon S3 ditentukan dan diimpor ke sistem file Anda dari S3, hanya data dari folder tersebut yang diterapkan terhadap kuota. Data seluruh bucket tidak dihitung terhadap batas kuota.

Metadata file dalam bucket S3 terkait diimpor ke folder dengan struktur yang cocok dengan folder impor dari Amazon S3. File-file ini dihitung terhadap kuota inode dari pengguna dan grup yang memiliki file.

Ketika pengguna melakukan `hsm_restore` atau malas memuat file, ukuran penuh file dihitung terhadap kuota blok yang terkait dengan pemilik file. Sebagai contoh, jika pengguna malas memuat file yang dimiliki oleh pengguna B, jumlah penyimpanan dan penggunaan inode dihitung terhadap kuota pengguna B. Demikian pula, ketika pengguna menggunakan Amazon FSx API untuk merilis file, data dibebaskan dari kuota blok pengguna atau grup yang memiliki file tersebut.

Karena HSM mengembalikan dan pemuatan malas dilakukan dengan akses akar, mereka memotong pemberlakuan kuota. Setelah data diimpor, data tersebut dihitung terhadap pengguna atau grup berdasarkan kepemilikan yang diatur di S3, yang dapat menyebabkan pengguna atau grup

melampaui batas pemblokirannya. Jika ini terjadi, mereka harus membebaskan file untuk dapat menulis ke sistem file lagi.

Demikian pula, sistem file dengan impor otomatis yang diaktifkan akan secara otomatis membuat inodes baru untuk objek yang ditambahkan ke S3. Inodes baru ini dibuat dengan akses akar dan pemberlakuan kuota pintasan ketika dibuat. Inodes baru ini akan dihitung terhadap pengguna dan grup, berdasarkan siapa yang memiliki objek di S3. Jika pengguna dan grup tersebut melampaui kuota inode berdasarkan aktivitas impor otomatis, mereka harus menghapus file untuk membebaskan kapasitas tambahan dan agar berada di bawah batas kuota mereka.

Kuota dan memulihkan backup

Ketika Anda memulihkan backup, pengaturan kuota sistem file asli dilaksanakan dalam sistem file yang dipulihkan. Sebagai contoh, jika kuota diatur dalam sistem file A, dan sistem file B dibuat dari cadangan sistem file A, kuota sistem file A diberlakukan dalam sistem file B.

Mengelola kapasitas penyimpanan

Anda dapat meningkatkan kapasitas penyimpanan yang dikonfigurasi pada sistem file FSx for Lustre Anda karena Anda memerlukan penyimpanan dan throughput tambahan. Karena throughput sistem file FSx for Lustre berskala linier dengan kapasitas penyimpanan, Anda juga mendapatkan peningkatan kapasitas throughput yang sebanding. Untuk meningkatkan kapasitas penyimpanan, Anda dapat menggunakan konsol Amazon FSx, AWS Command Line Interface (AWS CLI), atau Amazon FSx API.

Ketika Anda meminta pembaruan ke kapasitas penyimpanan sistem file Anda, Amazon FSx secara otomatis menambahkan server file jaringan baru dan menskalakan server metadata Anda. Ketika menskalakan kapasitas penyimpanan, sistem file mungkin tidak tersedia selama beberapa menit. Operasi file yang dikeluarkan oleh klien sementara sistem file tidak tersedia akan secara transparan mencoba lagi dan akhirnya berhasil setelah penyekalaan penyimpanan selesai. Selama waktu sistem file tidak tersedia, status sistem file diatur ke UPDATING. Setelah penyekalaan penyimpanan selesai, status sistem file diatur ke AVAILABLE.

Amazon FSx kemudian menjalankan proses optimasi penyimpanan yang secara transparan menyeimbangkan kembali data di server file yang ada dan baru ditambahkan. Penyeimbangan kembali dilakukan di latar belakang tanpa dampak pada ketersediaan sistem file. Selama rebalancing, Anda mungkin melihat penurunan kinerja sistem file karena sumber daya dikonsumsi untuk perpindahan data. Untuk sebagian besar sistem file, pengoptimuman penyimpangan

membutuhkan waktu beberapa jam hingga beberapa hari. Anda dapat mengakses dan menggunakan sistem file Anda selama tahap optimasi.

Anda dapat melacak kemajuan optimasi penyimpanan kapan saja menggunakan konsol Amazon FSx, CLI, dan API. Untuk informasi selengkapnya, lihat [Memantau peningkatan kapasitas penyimpanan](#).

Topik

- [Pertimbangan saat meningkatkan kapasitas penyimpanan](#)
- [Kapan harus meningkatkan kapasitas penyimpanan](#)
- [Bagaimana penyekalaan penyimpanan dan permintaan backup secara bersamaan ditangani](#)
- [Bagaimana meningkatkan kapasitas penyimpanan](#)
- [Memantau peningkatan kapasitas penyimpanan](#)

Pertimbangan saat meningkatkan kapasitas penyimpanan

Berikut adalah beberapa item penting yang perlu dipertimbangkan saat meningkatkan kapasitas penyimpanan:

- Meningkatkan hanya — Anda hanya dapat meningkatkan jumlah kapasitas penyimpanan untuk sistem file; Anda tidak dapat mengurangi kapasitas penyimpanan.
- Meningkatkan kenaikan — Ketika Anda meningkatkan kapasitas penyimpanan, gunakan kenaikan yang tercantum dalam kotak dialog Meningkatkan kapasitas penyimpanan.
- Waktu antara kenaikan — Anda tidak dapat meningkatkan kapasitas penyimpanan lebih lanjut pada sistem file hingga 6 jam setelah peningkatan terakhir diminta, atau hingga proses optimasi penyimpanan selesai, mana saja yang lebih lama.
- Kapasitas throughput — Anda secara otomatis meningkatkan kapasitas throughput saat Anda meningkatkan kapasitas penyimpanan. Untuk sistem file HDD persisten dengan cache SSD, kapasitas penyimpanan cache baca juga ditingkatkan untuk mempertahankan cache SSD yang berukuran hingga 20 persen dari kapasitas penyimpanan HDD. Amazon FSx menghitung nilai baru untuk unit kapasitas penyimpanan dan throughput dan mencantumkannya di kotak dialog Meningkatkan kapasitas penyimpanan.

Note

Anda dapat secara mandiri memodifikasi kapasitas throughput dari sistem file berbasis SSD persisten tanpa harus memperbarui kapasitas penyimpanan sistem file. Untuk informasi selengkapnya, lihat [Mengelola kapasitas throughput](#).

- Jenis Deployment — Anda dapat meningkatkan kapasitas penyimpanan semua jenis deployment kecuali untuk sistem file scratch 1. Jika Anda memiliki sistem file scratch 1, Anda dapat membuat yang baru dengan kapasitas penyimpanan yang lebih besar.

Kapan harus meningkatkan kapasitas penyimpanan

Tingkatkan kapasitas penyimpanan sistem file saat kapasitas penyimpanan gratis Anda sudah hampir habis terpakai. Gunakan `FreeStorageCapacity` CloudWatch metrik untuk memantau jumlah penyimpanan gratis yang tersedia pada sistem file. Anda dapat membuat CloudWatch alarm Amazon pada metrik ini dan mendapatkan pemberitahuan saat turun di bawah ambang batas tertentu. Untuk informasi selengkapnya, lihat [Pemantauan CloudWatch dengan Amazon](#).

Anda dapat menggunakan CloudWatch metrik untuk memantau tingkat penggunaan throughput sistem file yang sedang berlangsung. Jika Anda menentukan bahwa sistem file Anda memerlukan kapasitas throughput yang lebih tinggi, Anda dapat menggunakan informasi metrik untuk membantu Anda memutuskan seberapa banyak untuk meningkatkan kapasitas penyimpanan. Untuk informasi tentang cara menentukan throughput sistem file Anda saat ini, lihat [Cara menggunakan Amazon FSx for Lustre](#). Untuk informasi tentang bagaimana kapasitas penyimpanan mempengaruhi kapasitas throughput, lihat [Performa Amazon FSx for Lustre](#).

Anda juga dapat melihat kapasitas penyimpanan sistem file dan total throughput pada panel Ringkasan dari laman detail sistem file.

Bagaimana penyekalaan penyimpanan dan permintaan backup secara bersamaan ditangani

Anda dapat meminta backup sebelum alur kerja penyekalaan penyimpanan dimulai atau saat sedang berlangsung. Urutan bagaimana Amazon FSx menangani dua permintaan adalah sebagai berikut:

- Jika alur kerja penyekalaan penyimpanan sedang berlangsung (status penyimpanan penyimpanan `IN_PROGRESS` dan status sistem file adalah `UPDATING`) dan Anda meminta backup, permintaan

backup antri. Tugas cadangan dimulai ketika penyekalaan penyimpanan dalam tahap optimasi penyimpanan (status penyekalaan penyimpanan UPDATED_OPTIMIZING dan status sistem file adalah AVAILABLE).

- Jika backup sedang berlangsung (status backup CREATING) dan Anda meminta penyekalaan penyimpanan, permintaan penyekalaan penyimpanan antri. Alur kerja penyekalaan penyimpanan dimulai ketika Amazon FSx mentransfer backup ke Amazon S3 (status backup TRANSFERRING).

Jika permintaan penyekalaan penyimpanan tertunda dan permintaan backup sistem file juga tertunda, tugas backup memiliki prioritas yang lebih tinggi. Tugas penyekalaan penyimpanan tidak dimulai sampai tugas backup selesai.

Bagaimana meningkatkan kapasitas penyimpanan

Anda dapat meningkatkan kapasitas penyimpanan sistem file menggunakan konsol Amazon FSx, API AWS CLI, atau Amazon FSx.

Untuk meningkatkan kapasitas penyimpanan untuk sistem file (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Arahkan ke Sistem file, dan pilih sistem file Lustre yang ingin Anda tingkatkan kapasitas penyimpanannya.
3. Untuk Tindakan pilih Memperbarui kapasitas penyimpanan. Atau, di panel Ringkasan, pilih Perbarui di samping Kapasitas penyimpanan sistem file untuk menampilkan kotak dialog Meningkatkan kapasitas penyimpanan.

Increase storage capacity ✕

File system ID
fs-0dc01f485f15851b4

Current storage capacity
2400 GiB

Desired storage capacity
 GiB
Minimum 4,800 GiB; Increments of 2,400 GiB

Current throughput capacity
120 MB/s

Updated throughput capacity
240 MB/s

While scaling storage capacity, the file system may be unavailable for a few minutes. File operations issued by clients while the file system is unavailable will transparently retry and eventually succeed after scaling is complete.

Cancel
Update

4. Untuk Kapasitas penyimpanan yang diinginkan, sediakan kapasitas penyimpanan baru di GiB yang lebih besar dari kapasitas penyimpanan sistem file saat ini:
 - Untuk sistem file SSD atau scratch 2 persisten, nilai ini harus kelipatan 2400 GiB.
 - Untuk sistem file HDD persisten, nilai ini harus kelipatan 6000 GiB untuk sistem file 12 MB/S/TIB dan kelipatan 1800 GiB untuk sistem file 40 MB/S/TIB.

Note

Anda tidak dapat meningkatkan kapasitas penyimpanan sistem file scratch 1.

5. Pilih Perbarui untuk memulai pembaruan kapasitas penyimpanan.
6. Anda dapat memantau kemajuan pembaruan pada laman detail sistem file di tab Pembaruan.

Untuk meningkatkan kapasitas penyimpanan untuk sistem file (CLI)

1. Untuk meningkatkan kapasitas penyimpanan untuk sistem file FSx for Lustre, gunakan perintah. AWS CLI [update-file-system](#) Atur parameter berikut:

Atur `--file-system-id` ke ID dari sistem file yang Anda perbarui.

Atur `--storage-capacity` ke nilai integer yaitu jumlah, di GiB, dari peningkatan kapasitas penyimpanan. Untuk sistem file SSD atau scratch 2 persisten, nilai ini harus kelipatan 2400. Untuk sistem file HDD persisten, nilai ini harus kelipatan 6000 untuk sistem file 12 MB/s/TiB dan kelipatan 1800 GiB untuk sistem file 40 MB/s/TiB. Nilai target baru harus lebih besar dari kapasitas penyimpanan sistem file saat ini.

Perintah ini menentukan nilai target kapasitas penyimpanan 9600 GiB untuk SSD persisten atau sistem file scratch 2.

```
$ aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --storage-capacity 9600
```

2. Anda dapat memantau kemajuan pembaruan dengan menggunakan AWS CLI perintah [describe-file-systems](#). Cari `administrative-actions` di output.

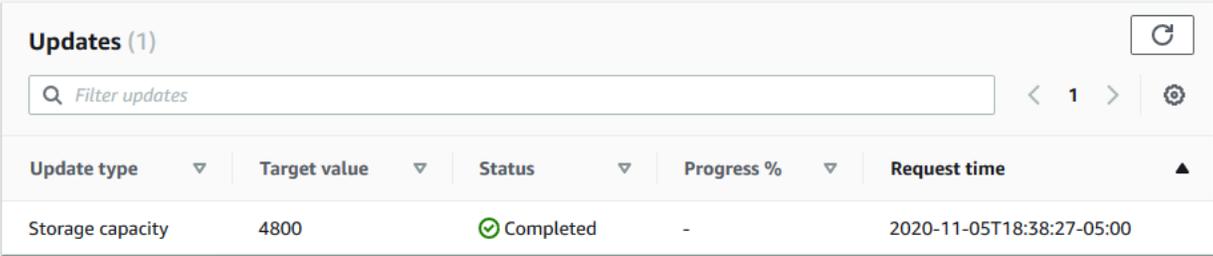
Untuk informasi lebih lanjut, lihat [AdministrativeAction](#).

Memantau peningkatan kapasitas penyimpanan

Anda dapat memantau kemajuan peningkatan kapasitas penyimpanan menggunakan konsol Amazon FSx, API, atau AWS CLI.

Memantau peningkatan dalam konsol

Di tab Pembaruan di laman detail sistem file, Anda dapat melihat 10 pembaruan terbaru untuk setiap jenis pembaruan.



Update type	Target value	Status	Progress %	Request time
Storage capacity	4800	Completed	-	2020-11-05T18:38:27-05:00

Anda dapat melihat informasi berikut:

Jenis pembaruan

Jenis yang didukung adalah Kapasitas penyimpanan dan Pengoptimalan penyimpanan.

Nilai target

Nilai yang diinginkan untuk memperbarui kapasitas penyimpanan sistem file ke.

Status

Status pembaruan kapasitas penyimpanan saat ini. Kemungkinan nilainya adalah sebagai berikut:

- Menunggu – Amazon FSx telah menerima permintaan pembaruan, namun belum mulai memprosesnya.
- Dalam proses – Amazon FSx sedang memproses permintaan pembaruan.
- Diperbarui; Mengoptimalkan — Amazon FSx telah meningkatkan kapasitas penyimpanan sistem file. Proses optimasi penyimpanan sekarang menyeimbangkan kembali data di server file.
- Selesai — Peningkatan kapasitas penyimpanan berhasil diselesaikan.
- Gagal — Peningkatan kapasitas penyimpanan gagal. Pilih tanda tanya (?) untuk melihat detail mengapa pembaruan penyimpanan gagal.

Kemajuan%

Menampilkan kemajuan proses optimasi penyimpanan sebagai persen selesai.

Waktu permintaan

Waktu Amazon FSx menerima permintaan tindakan pembaruan.

Pemantauan meningkat dengan API AWS CLI dan

Anda dapat melihat dan memantau permintaan peningkatan kapasitas penyimpanan sistem file menggunakan [describe-file-systems](#) AWS CLI perintah dan tindakan [DescribeFileSystems](#) API. Array `AdministrativeActions` mendaftarkan 10 tindakan pembaruan terbaru untuk setiap jenis tindakan administratif. Saat Anda meningkatkan kapasitas penyimpanan sistem file, dua `AdministrativeActions` dihasilkan: tindakan `FILE_SYSTEM_UPDATE` dan `STORAGE_OPTIMIZATION`.

Contoh berikut menunjukkan kutipan respons perintah CLI `describe-file-systems`. Sistem file memiliki kapasitas penyimpanan 4800 GB, dan ada tindakan administratif yang tertunda untuk meningkatkan kapasitas penyimpanan menjadi 9600 GB.

```
{
  "FileSystems": [
    {
```

```

    "OwnerId": "111122223333",
    .
    .
    .
    "StorageCapacity": 4800,
    "AdministrativeActions": [
      {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "StorageCapacity": 9600
        }
      },
      {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
      }
    ]
  ]

```

Amazon FSx memproses proses tindakan FILE_SYSTEM_UPDATE terlebih dahulu, dengan menambahkan server file baru 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 administratif STORAGE_OPTIMIZATION. Ini ditunjukkan dalam kutipan tanggapan perintah CLI describe-file-systems berikut.

Properti ProgressPercent menampilkan kemajuan proses optimasi penyimpanan. Setelah proses optimasi penyimpanan berhasil diselesaikan, status tindakan FILE_SYSTEM_UPDATE berubah menjadi COMPLETED, dan tindakan STORAGE_OPTIMIZATION tidak lagi muncul.

```

{
  "FileSystems": [
    {
      "OwnerId": "111122223333",
      .
      .
      .
      "StorageCapacity": 9600,
      "AdministrativeActions": [
        {

```

```

        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 9600
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1581694764.757,
        "Status": "IN_PROGRESS",
        "ProgressPercent": 50,
    }
]

```

Jika peningkatan kapasitas penyimpanan gagal, status tindakan FILE_SYSTEM_UPDATE berubah menjadi FAILED. Properti FailureDetails menyediakan informasi tentang kegagalan, yang ditunjukkan dalam contoh berikut.

```

{
  "FileSystems": [
    {
      "OwnerId": "111122223333",
      .
      .
      .
      "StorageCapacity": 4800,
      "AdministrativeActions": [
        {
          "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
          "FailureDetails": {
            "Message": "string"
          },
          "RequestTime": 1581694764.757,
          "Status": "FAILED",
          "TargetFileSystemValues":
            "StorageCapacity": 9600
        }
      ]
    }
  ]
}

```

Mengelola kinerja metadata

Anda dapat memperbarui konfigurasi metadata sistem file FSx for Lustre Anda tanpa gangguan pada pengguna akhir atau aplikasi Anda dengan menggunakan konsol Amazon FSx, Amazon FSx API, atau (). AWS Command Line Interface AWS CLI Prosedur pembaruan meningkatkan jumlah IOPS Metadata yang disediakan untuk sistem file Anda.

Note

Anda dapat meningkatkan kinerja metadata hanya pada sistem file FSx for Lustre yang dibuat dengan jenis penyebaran Persistent_2 dan konfigurasi metadata yang ditentukan.

Peningkatan kinerja metadata sistem file Anda tersedia untuk digunakan dalam beberapa menit. Anda dapat memperbarui kinerja metadata kapan saja, selama permintaan peningkatan kinerja metadata setidaknya berjarak 6 jam. Saat menskalakan kinerja metadata, sistem file mungkin tidak tersedia selama beberapa menit. Operasi file yang dikeluarkan oleh klien saat sistem file tidak tersedia akan dicoba lagi secara transparan dan akhirnya berhasil setelah penskalaan kinerja metadata selesai. Anda akan ditagih untuk peningkatan kinerja metadata baru setelah tersedia untuk Anda.

Anda dapat melacak kemajuan peningkatan kinerja metadata kapan saja dengan menggunakan konsol Amazon FSx, CLI, dan API. Untuk informasi selengkapnya, lihat [Memantau pembaruan konfigurasi metadata](#).

Topik

- [Konfigurasi kinerja metadata kilau](#)
- [Pertimbangan saat meningkatkan kinerja metadata](#)
- [Kapan harus meningkatkan kinerja metadata](#)
- [Cara meningkatkan kinerja metadata](#)
- [Mengubah mode konfigurasi metadata](#)
- [Memantau pembaruan konfigurasi metadata](#)

Konfigurasi kinerja metadata kilau

Jumlah IOPS Metadata yang disediakan menentukan tingkat maksimum operasi metadata yang dapat didukung oleh sistem file.

Saat Anda membuat sistem file, Anda memilih salah satu dari dua mode konfigurasi metadata, Otomatis atau yang disediakan pengguna:

- Dalam mode Otomatis, Amazon FSx secara otomatis menyediakan dan menskalakan jumlah Metadata IOPS pada sistem file Anda berdasarkan kapasitas penyimpanan sistem file Anda.
- Dalam mode yang disediakan pengguna, Anda menentukan jumlah Metadata IOPS yang akan disediakan untuk sistem file Anda.

Anda dapat beralih dari mode Otomatis ke mode yang disediakan Pengguna kapan saja. Anda juga dapat beralih dari mode yang disediakan pengguna ke mode Otomatis jika jumlah Metadata IOPS yang disediakan pada sistem file Anda cocok dengan nomor default Metadata IOPS yang disediakan dalam mode Otomatis.

Nilai IOPS Metadata yang valid adalah 1500, 3000, 6000, 12000, dan kelipatan 12000 hingga maksimum 192000. Setiap nilai 12000 Metadata IOPS memerlukan satu alamat IP dalam subnet tempat sistem file Anda berada.

Jumlah default Metadata IOPS yang disediakan dalam mode Otomatis tergantung pada kapasitas sistem file Anda. Lihat [tabel ini](#) untuk informasi tentang jumlah default Metadata IOPS yang disediakan berdasarkan kapasitas penyimpanan sistem file.

Jika kinerja metadata beban kerja Anda melebihi jumlah IOPS Metadata yang disediakan dalam mode Otomatis, Anda dapat menggunakan mode yang disediakan pengguna untuk meningkatkan nilai IOPS Metadata untuk sistem file Anda.

Anda dapat melihat nilai saat ini dari konfigurasi server metadata sistem file sebagai berikut:

- Menggunakan konsol — Pada panel Ringkasan halaman detail sistem file, bidang Metadata IOPS menunjukkan nilai terkini dari IOPS Metadata yang disediakan dan mode konfigurasi metadata saat ini (baik Otomatis atau yang disediakan pengguna) dari sistem file.
- Menggunakan CLI atau API — Gunakan perintah CLI [deskripsi-file-sistem](#) atau operasi API Sistem, dan cari [DescribeFilepropertinya](#). MetadataConfiguration

Pertimbangan saat meningkatkan kinerja metadata

Berikut adalah beberapa pertimbangan penting saat meningkatkan kinerja metadata Anda:

- Kinerja metadata hanya meningkat — Anda hanya dapat meningkatkan jumlah IOPS Metadata untuk sistem file; Anda tidak dapat mengurangi jumlah IOPS Metadata.
- Menentukan Metadata IOPS dalam mode Otomatis tidak didukung - Anda tidak dapat menentukan jumlah IOPS Metadata pada sistem file yang berada dalam mode Otomatis. Anda harus beralih ke mode yang disediakan pengguna dan kemudian membuat permintaan. Untuk informasi selengkapnya, lihat [Mengubah mode konfigurasi metadata](#).
- Waktu antara peningkatan — Anda tidak dapat membuat peningkatan kinerja metadata lebih lanjut pada sistem file hingga 6 jam setelah peningkatan terakhir diminta.
- Kinerja metadata bersamaan dan penyimpanan SSD meningkat — Anda tidak dapat menskalakan kinerja metadata dan kapasitas penyimpanan sistem file secara bersamaan.

Kapan harus meningkatkan kinerja metadata

Tingkatkan jumlah IOPS Metadata saat Anda perlu menjalankan beban kerja yang memerlukan tingkat kinerja metadata yang lebih tinggi daripada yang disediakan secara default di sistem file Anda. Anda dapat memantau kinerja metadata Anda AWS Management Console dengan menggunakan Metadata IOPS Utilization grafik yang memberikan persentase kinerja server metadata yang disediakan yang Anda konsumsi di sistem file Anda.

Anda juga dapat memantau kinerja metadata Anda menggunakan metrik yang lebih terperinci CloudWatch . CloudWatch metrik termasuk `DiskReadOperations` dan `DiskWriteOperations`, yang menyediakan volume operasi server metadata yang memerlukan disk IO, serta metrik granular untuk operasi metadata termasuk pembuatan file dan direktori, statistik, pembacaan, dan penghapusan. Untuk informasi selengkapnya, lihat [Metrik metadata sistem file](#).

Cara meningkatkan kinerja metadata

Anda dapat meningkatkan kinerja metadata sistem file dengan menggunakan konsol Amazon FSx, API, AWS CLI atau Amazon FSx.

Untuk meningkatkan kinerja metadata untuk sistem file (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.

2. Di panel navigasi kiri, pilih Sistem file. Dalam daftar sistem File, pilih sistem file FSx for Lustre yang ingin Anda tingkatkan kinerja metadata.
3. Untuk Tindakan, pilih Perbarui Metadata IOPS. Atau, di panel Ringkasan, pilih Perbarui di sebelah bidang IOPS Metadata sistem file.

Kotak dialog Update Metadata IOPS muncul.

4. Pilih User-provisioned.
5. Untuk IOPS Metadata yang Diinginkan, pilih nilai IOPS Metadata baru. Nilai yang valid adalah 1500 3000 6000, 12000,, dan kelipatan 12000 hingga maksimum. 192000 Nilai yang Anda masukkan harus lebih besar dari atau sama dengan nilai IOPS Metadata saat ini.
6. Pilih Perbarui.

Untuk meningkatkan kinerja metadata untuk sistem file (CLI)

Untuk meningkatkan kinerja metadata untuk sistem file FSx for Lustre, gunakan [perintah UpdateFileSystem update-file-system](#) (adalah aksi API AWS CLI yang setara). Atur parameter berikut:

- Atur `--file-system-id` ke ID dari sistem file yang Anda perbarui.
- Untuk meningkatkan kinerja metadata Anda, gunakan properti. `--lustre-configuration MetadataConfiguration` Properti ini memiliki dua parameter, Mode dan Iops.
 1. Jika sistem file Anda dalam mode `USER_PROVISIONED`, penggunaan Mode adalah opsional (jika digunakan, atur ke). Mode `USER_PROVISIONED`

Jika sistem file Anda dalam mode OTOMATIS, atur Mode ke `USER_PROVISIONED` (yang mengalihkan mode sistem file ke `USER_PROVISIONED` selain meningkatkan nilai IOPS Metadata).

2. Setel Iops ke nilai 1500 3000, 6000, 12000,, atau kelipatan 12000 hingga maksimum. 192000 Nilai yang Anda masukkan harus lebih besar dari atau sama dengan nilai IOPS Metadata saat ini.

Contoh berikut memperbarui IOPS Metadata yang disediakan ke 96000.

```
aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --lustre-configuration 'MetadataConfiguration={Mode=USER_PROVISIONED,Iops=96000}'
```

Mengubah mode konfigurasi metadata

Anda dapat mengubah mode konfigurasi metadata dari sistem file yang ada menggunakan AWS konsol dan CLI, seperti yang dijelaskan dalam prosedur berikut.

Saat beralih dari mode Otomatis ke mode yang disediakan pengguna, Anda harus memberikan nilai IOPS Metadata yang lebih besar dari atau sama dengan nilai IOPS Metadata sistem file saat ini.

Jika Anda meminta untuk beralih dari mode yang disediakan pengguna ke mode Otomatis dan nilai IOPS Metadata saat ini lebih besar dari default otomatis, Amazon FSx menolak permintaan tersebut, karena downscaling Metadata IOPS tidak didukung. Untuk membuka blokir sakelar mode, Anda harus meningkatkan kapasitas penyimpanan agar sesuai dengan Metadata IOPS Anda saat ini dalam mode Otomatis untuk mengaktifkan sakelar mode lagi.

Anda dapat mengubah mode konfigurasi metadata sistem file dengan menggunakan konsol Amazon FSx, API, AWS CLI atau Amazon FSx.

Untuk mengubah mode konfigurasi metadata untuk sistem file (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi kiri, pilih Sistem file. Dalam daftar sistem File, pilih sistem file FSx for Lustre yang ingin Anda ubah mode konfigurasi metadata.
3. Untuk Tindakan, pilih Perbarui Metadata IOPS. Atau, di panel Ringkasan, pilih Perbarui di sebelah bidang IOPS Metadata sistem file.

Kotak dialog Update Metadata IOPS muncul.

4. Lakukan salah satu dari berikut ini.
 - Untuk beralih dari mode yang disediakan pengguna ke mode Otomatis, pilih Otomatis.
 - Untuk beralih dari mode Otomatis ke mode yang disediakan pengguna, pilih User-provisioned. Kemudian, untuk IOPS Metadata yang Diinginkan, berikan nilai IOPS Metadata yang lebih besar dari atau sama dengan nilai IOPS Metadata sistem file saat ini.
5. Pilih Perbarui.

Untuk mengubah mode konfigurasi metadata untuk sistem file (CLI)

Untuk mengubah mode konfigurasi metadata untuk sistem file FSx for Lustre, gunakan [perintah](#) UpdateFileSystem update-file-system (adalah aksi API AWS CLI yang setara). Atur parameter berikut:

- Atur `--file-system-id` ke ID dari sistem file yang Anda perbarui.
- Untuk mengubah mode konfigurasi metadata, gunakan properti. `--lustre-configuration` MetadataConfiguration Properti ini memiliki dua parameter, Mode dan Iops.
- Untuk beralih dari mode OTOMATIS ke mode USER_PROVISIONED, atur Mode ke USER_PROVISIONED dan Iops ke nilai IOPS Metadata yang lebih besar dari atau sama dengan nilai IOPS Metadata sistem file saat ini. Sebagai contoh:

```
aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --lustre-configuration  
  'MetadataConfiguration={Mode=USER_PROVISIONED,Iops=96000}'
```

- Untuk beralih dari mode USER_PROVISIONED ke mode OTOMATIS, atur Mode ke AUTOMATIC dan jangan gunakan parameter. Iops Sebagai contoh:

```
aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --lustre-configuration 'MetadataConfiguration={Mode=AUTOMATIC}'
```

Memantau pembaruan konfigurasi metadata

Anda dapat memantau kemajuan pembaruan konfigurasi metadata dengan menggunakan konsol Amazon FSx, API, atau. AWS CLI

Memantau pembaruan konfigurasi metadata (konsol)

Anda dapat memantau pembaruan konfigurasi metadata di tab Pembaruan pada halaman detail sistem file.

Untuk pembaruan konfigurasi metadata, Anda dapat melihat informasi berikut:

Jenis pembaruan

Tipe yang didukung adalah Metadata IOPS dan mode konfigurasi Metadata.

Nilai target

Nilai yang diperbarui untuk mode konfigurasi Metadata IOPS atau Metadata sistem file.

Status

Status terkini dari pembaruan. Kemungkinan nilainya adalah sebagai berikut:

- Menunggu – Amazon FSx telah menerima permintaan pembaruan, namun belum mulai memprosesnya.
- Dalam proses – Amazon FSx sedang memproses permintaan pembaruan.
- Selesai - Pembaruan selesai dengan sukses.
- Gagal — Permintaan pembaruan gagal. Pilih tanda tanya (?) untuk melihat detail tentang mengapa permintaan gagal.

Waktu permintaan

Waktu Amazon FSx menerima permintaan tindakan pembaruan.

Memantau pembaruan konfigurasi metadata (CLI)

[Anda dapat melihat dan memantau permintaan pembaruan konfigurasi metadata menggunakan perintah `describe-file-systems` dan operasi `Systems API` AWS CLI . `DescribeFile` Array](#)

`AdministrativeActions` mencantumkan 10 tindakan pembaruan terbaru untuk setiap jenis tindakan administratif. Saat Anda memperbarui kinerja metadata sistem file atau mode konfigurasi metadata, akan dihasilkan `FILE_SYSTEM_UPDATE` `AdministrativeActions`

Contoh berikut menunjukkan kutipan respons perintah CLI `describe-file-systems`. Sistem file memiliki tindakan administratif yang tertunda untuk meningkatkan Metadata IOPS menjadi 96000 dan mode konfigurasi metadata ke `USER_PROVISIONED`.

```
"AdministrativeActions": [  
  {  
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",  
    "RequestTime": 1678840205.853,  
    "Status": "PENDING",  
    "TargetFileSystemValues": {  
      "LustreConfiguration": {  
        "MetadataConfiguration": {  
          "Iops": 96000,  
          "Mode": USER_PROVISIONED  
        }  
      }  
    }  
  }  
]
```

Amazon FSx memproses FILE_SYSTEM_UPDATE tindakan, memodifikasi Metadata IOPS sistem file dan mode konfigurasi metadata. Ketika sumber daya metadata baru tersedia untuk sistem file, FILE_SYSTEM_UPDATE status berubah menjadi. COMPLETED

Jika permintaan pembaruan konfigurasi metadata gagal, status FILE_SYSTEM_UPDATE tindakan berubah menjadi FAILED, seperti yang ditunjukkan pada contoh berikut. FailureDetailsProperti memberikan informasi tentang kegagalan.

```
"AdministrativeActions": [
  {
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
    "RequestTime": 1678840205.853,
    "Status": "FAILED",
    "TargetFileSystemValues": {
      "LustreConfiguration": {
        "MetadataConfiguration": {
          "Iops": 96000,
          "Mode": USER_PROVISIONED
        }
      }
    },
    "FailureDetails": {
      "Message": "failure-message"
    }
  }
]
```

Mengelola kapasitas throughput

Setiap sistem file FSx for Lustre memiliki kapasitas throughput yang dikonfigurasi saat Anda membuat sistem file. Throughput sistem file FSx for Lustre diukur dalam megabyte per detik per tebibyte (MB/s/Tib). Kapasitas throughput adalah salah satu faktor yang menentukan kecepatan di mana server file yang meng-hosting sistem file dapat menyediakan data file. Semakin tinggi tingkat kapasitas throughput, semakin tinggi pula tingkat operasi I/O per detik (IOPS) dan memakan lebih banyak memori untuk caching data pada server file. Untuk informasi selengkapnya, lihat [Performa Amazon FSx for Lustre](#).

Anda dapat memodifikasi tingkat throughput dari sistem file berbasis SSD persisten dengan meningkatkan atau mengurangi nilai throughput sistem file per unit penyimpanan. Nilai yang valid tergantung pada jenis penyebaran sistem file, sebagai berikut:

- Untuk jenis penyebaran berbasis SSD Persistent_1, nilai yang valid adalah 50, 100, dan 200 MB/s/Tib.
- Untuk jenis penyebaran berbasis SSD Persistent_2, nilai yang valid adalah 125, 250, 500, dan 1000 MB/s/Tib.

Anda dapat melihat nilai saat ini dari throughput sistem file per unit penyimpanan, sebagai berikut:

- Menggunakan konsol — Pada panel Ringkasan halaman detail sistem file, bidang Throughput per unit penyimpanan menunjukkan nilai saat ini.
- Menggunakan CLI atau API — Gunakan perintah [describe-file-systems](#)CLI atau operasi [DescribeFileSystems](#)API, dan cari properti. `PerUnitStorageThroughput`

Saat Anda memodifikasi kapasitas throughput sistem file Anda, di belakang layar, Amazon FSx mengalihkan server file sistem file. Sistem file Anda tidak akan tersedia selama beberapa menit selama penskalaan kapasitas throughput. Anda akan ditagih atas jumlah baru kapasitas throughput begitu tersedia untuk sistem file Anda.

Topik

- [Pertimbangan saat memperbarui kapasitas throughput](#)
- [Kapan harus mengubah kapasitas throughput](#)
- [Bagaimana cara mengubah kapasitas throughput](#)
- [Memantau perubahan kapasitas throughput pada konsol](#)

Pertimbangan saat memperbarui kapasitas throughput

Berikut adalah beberapa hal penting yang perlu dipertimbangkan saat memperbarui kapasitas throughput:

- Menambah atau mengurangi — Anda dapat menambah atau mengurangi jumlah kapasitas throughput untuk sistem file.
- Update increments — Bila Anda mengubah kapasitas throughput, gunakan kenaikan yang tercantum dalam kotak dialog Update throughput tier.
- Waktu antara peningkatan - Anda tidak dapat membuat perubahan kapasitas throughput lebih lanjut pada sistem file hingga 6 jam setelah permintaan terakhir, atau sampai proses optimasi throughput selesai, waktu mana pun yang lebih lama.

- Jenis Deployment — Anda hanya dapat memperbarui kapasitas throughput tipe penerapan berbasis SSD persisten.

Kapan harus mengubah kapasitas throughput

Amazon FSx terintegrasi dengan Amazon CloudWatch, memungkinkan Anda memantau tingkat penggunaan throughput sistem file yang sedang berlangsung. Kinerja (throughput dan IOPS) yang dapat Anda jalankan melalui sistem file tergantung pada karakteristik beban kerja spesifik Anda, selain kapasitas throughput, kapasitas penyimpanan, dan jenis penyimpanan pada sistem file Anda. Untuk informasi tentang cara menentukan throughput sistem file Anda saat ini, lihat [Cara menggunakan Amazon FSx for Lustre](#). Untuk informasi tentang CloudWatch metrik, lihat [Pemantauan CloudWatch dengan Amazon](#).

Bagaimana cara mengubah kapasitas throughput

Anda dapat mengubah kapasitas throughput pada sistem file dengan menggunakan konsol Amazon FSx, AWS Command Line Interface (AWS CLI), atau API Amazon FSx.

Untuk mengubah kapasitas throughput sistem file (CLI)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Arahkan ke sistem File, dan pilih sistem file FSx for Lustre yang ingin Anda ubah kapasitas throughputnya.
3. Untuk Tindakan, pilih Perbarui tingkat throughput. Atau, di panel Ringkasan, pilih Perbarui di sebelah Throughput sistem file per unit penyimpanan.

Jendela tingkat throughput pembaruan muncul.

4. Pilih nilai baru untuk throughput yang diinginkan per unit penyimpanan dari daftar.

Update throughput tier
✕

File system ID
fs-04be0cb4339a509e8

Current throughput per unit of storage
125 MB/s/TiB

Current total throughput capacity
150 MB/s

Desired throughput per unit of storage
 MB/s/TiB

Updated total throughput capacity
150 MB/s

While scaling throughput capacity, the file system will be unavailable for up to an hour. File operations issued by clients while the file system is unavailable will transparently retry and eventually succeed after scaling is complete.

Cancel
Update

5. Pilih Perbarui untuk memulai pembaruan kapasitas throughput.

i Note

Sistem file Anda mungkin mengalami periode tidak tersedianya yang sangat singkat selama pembaruan.

Untuk mengubah kapasitas throughput sistem file (CLI)

- Untuk memodifikasi kapasitas throughput sistem file, gunakan perintah [update-file-system](#) CLI (atau operasi API yang [UpdateFileSystem](#) setara). Atur parameter berikut:
 - Atur `--file-system-id` ke ID dari sistem file yang Anda perbarui.
 - Setel `--lustre-configuration PerUnitStorageThroughput` ke nilai `50100`, atau `200` MB/s/Tib untuk sistem file SSD Persistent_1, atau ke nilai `250 500 1000`, atau MB/s/Tib untuk sistem file SSD 125 Persistent_2.

Perintah ini menentukan bahwa kapasitas throughput diatur ke 1000 MB/s/Tib untuk sistem file.

```
aws fsx update-file-system \
```

```
--file-system-id fs-0123456789abcdef0 \  
--lustre-configuration PerUnitStorageThroughput=1000
```

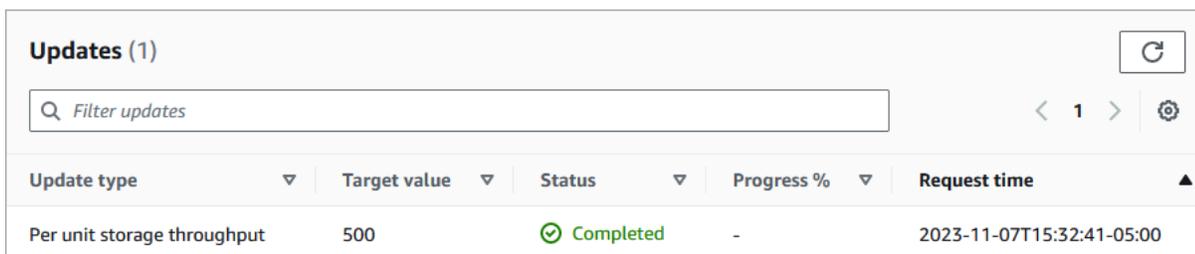
Memantau perubahan kapasitas throughput pada konsol

Anda dapat memantau perkembangan peningkatan kapasitas throughput menggunakan konsol Amazon FSx, API, atau AWS CLI.

Memantau perubahan kapasitas throughput (konsol)

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

- Pada tab Pembaruan di halaman detail sistem file, Anda dapat melihat 10 tindakan pembaruan terbaru untuk setiap jenis tindakan pembaruan.



Update type	Target value	Status	Progress %	Request time
Per unit storage throughput	500	Completed	-	2023-11-07T15:32:41-05:00

Untuk melakukan tindakan pembaruan kapasitas throughput, Anda dapat melihat informasi berikut.

Jenis pembaruan

Tipe yang didukung adalah throughput penyimpanan per unit.

Nilai target

Nilai yang diinginkan untuk mengubah throughput sistem file per unit penyimpanan menjadi.

Status

Status terkini dari pembaruan tersebut. Untuk pembaruan kapasitas throughput, nilai yang mungkin didapat adalah sebagai berikut:

- Tertunda – Amazon FSx telah menerima permintaan pembaruan, namun belum mulai memprosesnya.
- Dalam proses – Amazon FSx sedang memproses permintaan pembaruan.

- Diperbarui; Mengoptimalkan - Amazon FSx telah memperbarui jaringan I/O, CPU, dan sumber daya memori sistem file. Tingkat kinerja I/O disk baru tersedia untuk operasi tulis. Operasi baca Anda akan melihat kinerja I/O disk antara level sebelumnya dan level baru hingga sistem file Anda tidak lagi dalam keadaan ini.
- Selesai – Pembaruan kapasitas throughput berhasil diselesaikan.
- Gagal – Pembaruan kapasitas throughput gagal. Pilih tanda tanya (?) untuk melihat secara terperinci mengapa pembaruan throughput gagal.

Waktu permintaan

Waktu ketika Amazon FSx menerima permintaan pembaruan.

Pemantauan pembaruan sistem file (CLI)

- 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 target throughput per unit penyimpanan 500 MB/s/Tib.

```
.  
. .  
.  
"AdministrativeActions": [  
  {  
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",  
    "RequestTime": 1581694764.757,  
    "Status": "PENDING",  
    "TargetFileSystemValues": {  
      "LustreConfiguration": {  
        "PerUnitStorageThroughput": 500  
      }  
    }  
  }  
]
```

Saat Amazon FSx berhasil memproses tindakan, statusnya berubah menjadi `COMPLETED`. Kapasitas throughput yang baru kemudian tersedia untuk sistem file tersebut, dan tampak dalam properti `PerUnitStorageThroughput`.

Jika perubahan kapasitas throughput gagal, statusnya berubah menjadi `FAILED`, dan properti `FailureDetails` memberikan informasi tentang kegagalan tersebut.

Kompresi data Lustre

Anda dapat menggunakan fitur kompresi data Lustre untuk mencapai penghematan biaya pada sistem file Amazon FSx for Lustre yang ber-performa tinggi dan penyimpanan backup. Ketika kompresi data diaktifkan, Amazon FSx for Lustre secara otomatis memampatkan file yang baru ditulis sebelum ditulis ke disk dan secara otomatis melepaskannya ketika mereka terbaca.

Kompresi data menggunakan algoritme LZ4, yang dioptimalkan untuk memberikan tingkat kompresi yang tinggi tanpa memberikan dampak pada performa sistem file. LZ4 adalah algoritme Lustre yang dipercaya oleh komunitas dan berorientasi pada performa yang memberikan keseimbangan antara kecepatan kompresi dan ukuran file yang dikompresi. Mengaktifkan kompresi data biasanya tidak memiliki dampak terukur pada latensi.

Kompresi data meredam jumlah data yang ditransfer antara server file Amazon FSx for Lustre dan penyimpanannya. Jika Anda belum menggunakan format file yang terkompresi, Anda akan melihat peningkatan sistem file kapasitas throughput saat menggunakan kompresi data. Peningkatan kapasitas throughput yang terkait dengan kompresi data akan dibatasi setelah Anda telah memenuhi kartu antarmuka jaringan front-end Anda.

Sebagai contoh, jika sistem file Anda adalah tipe deployment PERSISTENT-50 SSD, jaringan throughput Anda memiliki dasar penyimpanan 250 MB/s per TiB. Disk throughput Anda memiliki dasar 50 MB/s per TiB. Dengan kompresi data, disk throughput Anda dapat meningkat dari 50 MB/s per TiB hingga maksimum 250 MB/s per TiB, yang merupakan batas dasar jaringan throughput. Untuk informasi selengkapnya tentang batas jaringan dan batas disk throughput, lihat tabel performa sistem file di [Performa kumpulan sistem file](#). Untuk informasi selengkapnya tentang performa kompresi data, [lihat postingan kompresi data Amazon FSx for Lustre](#) di Blog Penyimpanan.AWS

Topik

- [Mengelola kompresi data](#)

- [Mengompresi file yang sebelumnya ditulis](#)
- [Melihat ukuran file](#)
- [Menggunakan CloudWatch metrik](#)

Mengelola kompresi data

Anda dapat mengaktifkan atau menonaktifkan kompresi data saat membuat sistem file Amazon FSx for Lustre yang baru. Kompresi data dimatikan secara default saat Anda membuat sistem file Amazon FSx for Lustre dari konsol,, atau API. AWS CLI

Untuk mengaktifkan kompresi data saat membuat sistem file (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Ikuti prosedur untuk membuat sistem file baru yang dijelaskan di [Buat sistem file FSx for Lustre Anda](#) pada bagian Mulai.
3. Pada bagian Detail sistem file untuk Tipe kompresi data, pilih LZ4.
4. Menyelesaikan wizard seperti yang Anda lakukan ketika Anda membuat sistem file baru.
5. Pilih Periksa dan buat.
6. Tinjau pengaturan yang Anda pilih untuk sistem file Amazon FSx for Lustre, lalu pilih Buat sistem file.

Ketika sistem file Tersedia, kompresi data diaktifkan.

Untuk mengaktifkan kompresi data saat membuat sistem file (CLI)

- Untuk membuat sistem file FSx for Lustre dengan kompresi data dihidupkan, gunakan perintah Amazon FSx [create-file-system](#) CLI dengan parameter, seperti yang ditunjukkan berikut. DataCompressionType Operasi API yang sesuai adalah [CreateFileSystem](#).

```
$ aws fsx create-file-system \
  --client-request-token CRT1234 \
  --file-system-type LUSTRE \
  --file-system-type-version 2.12 \
  --lustre-configuration
DeploymentType=PERSISTENT_1,PerUnitStorageThroughput=50,DataCompressionType=LZ4 \
  --storage-capacity 3600 \
  --subnet-ids subnet-123456 \
```

```
--tags Key=Name,Value=Lustre-TEST-1 \  
--region us-east-2
```

Setelah berhasil membuat sistem file, Amazon FSx mengembalikan deskripsi sistem file sebagai JSON, seperti yang ditunjukkan dalam contoh berikut.

```
{  
  "FileSystems": [  
    {  
      "OwnerId": "111122223333",  
      "CreationTime": 1549310341.483,  
      "FileSystemId": "fs-0123456789abcdef0",  
      "FileSystemType": "LUSTRE",  
      "FileSystemTypeVersion": "2.12",  
      "Lifecycle": "CREATING",  
      "StorageCapacity": 3600,  
      "VpcId": "vpc-123456",  
      "SubnetIds": [  
        "subnet-123456"  
      ],  
      "NetworkInterfaceIds": [  
        "eni-039fcf55123456789"  
      ],  
      "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",  
      "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/  
fs-0123456789abcdef0",  
      "Tags": [  
        {  
          "Key": "Name",  
          "Value": "Lustre-TEST-1"  
        }  
      ],  
      "LustreConfiguration": {  
        "DeploymentType": "PERSISTENT_1",  
        "DataCompressionType": "LZ4",  
        "PerUnitStorageThroughput": 50  
      }  
    }  
  ]  
}
```

Anda juga dapat mengubah konfigurasi kompresi data Anda dari sistem file yang sudah ada. Ketika Anda mengaktifkan kompresi data untuk sistem file yang ada, hanya file yang baru ditulis yang akan dikompresi, dan file yang ada tidak dikompresi. Untuk informasi selengkapnya, lihat [Mengompresi file yang sebelumnya ditulis](#).

Untuk memperbaharui kompresi data pada sistem file yang ada (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Arahkan ke Sistem file, dan pilih sistem file Lustre yang ingin Anda kelola untuk kompresi data.
3. Untuk Tindakan, pilih Memperbarui tipe kompresi data.
4. Pada Memperbarui tipe data kompresi kotak dialog, pilih LZ4 untuk mengaktifkan kompresi data, atau memilih TIDAK ADA untuk memmatikannya.
5. Pilih Perbarui.
6. Anda dapat memantau kemajuan pembaruan pada halaman detail sistem file di tab Pembaruan .

Untuk memperbarui kompresi data pada sistem file yang ada (CLI)

Untuk memperbarui konfigurasi kompresi data untuk sistem file FSx for Lustre yang ada, gunakan perintah. AWS CLI [update-file-system](#) Atur parameter berikut:

- Atur `--file-system-id` ke ID dari sistem file yang Anda perbarui.
- Atur `--lustre-configuration DataCompressionType` ke `NONE` untuk mematikan kompresi data atau `LZ4` untuk mengaktifkan kompresi data dengan algoritme LZ4.

Perintah ini menentukan bahwa kompresi data diaktifkan dengan algoritme LZ4.

```
$ aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --lustre-configuration DataCompressionType=LZ4
```

Konfigurasi kompresi data saat membuat sistem file dari backup

Anda dapat menggunakan backup yang tersedia untuk membuat Amazon FSx for Lustre baru untuk sistem file Lustre. Ketika Anda membuat sistem file baru dari backup, tidak perlu untuk menentukan `DataCompressionType`; pengaturan akan diterapkan menggunakan pengaturan `DataCompressionType` backup. Jika Anda memilih untuk menentukan `DataCompressionType`

saat membuatnya dari backup, nilainya harus sesuai dengan pengaturan `DataCompressionType` backup.

Untuk melihat pengaturan pada backup, pilih pengaturan dari tab Backup pada konsol Amazon FSx. Detail backup akan tercantum pada halaman Ringkasan untuk backup. Anda juga dapat menjalankan [describe-backups](#) AWS CLI perintah (tindakan API yang setara adalah [DescribeBackups](#)).

Mengompresi file yang sebelumnya ditulis

File tidak dikompresi jika mereka dibuat ketika kompresi data dimatikan pada sistem file Amazon FSx for Lustre. Mengaktifkan kompresi data tidak akan secara otomatis mengompresi data yang belum terkompresi.

Anda dapat menggunakan perintah `lfs_migrate` yang diinstal sebagai bagian dari instalasi klien Lustre untuk mengompres file yang sudah ada. Sebagai contoh, lihat [Kompresi FSXL yang tersedia](#) di GitHub

Melihat ukuran file

Anda dapat menggunakan perintah berikut untuk melihat ukuran data yang sudah dan belum terkompresi dan direktori Anda.

- `du -sh` menampilkan ukuran yang sudah terkompresi.
- `du --apparent-size` menampilkan ukuran yang belum terkompresi.
- `ls -lh` menampilkan ukuran yang belum terkompresi.

Contoh berikut menunjukkan output dari setiap perintah dengan file yang sama.

```
$ du -sh samplefile
272M samplefile
$ du -sh --apparent-size samplefile
1.0G samplefile
$ ls -lh samplefile
-rw-r--r-- 1 root root 1.0G May 10 21:16 samplefile
```

Pilihan `-h` berguna untuk perintah ini karena dapat mencetak ukuran dalam format yang dapat dibaca manusia.

Menggunakan CloudWatch metrik

Anda dapat menggunakan metrik Amazon CloudWatch Logs untuk melihat penggunaan sistem file Anda. Metrik `LogicalDiskUsage` menunjukkan total penggunaan diska logis (tanpa kompresi), dan metrik `PhysicalDiskUsage` menunjukkan total penggunaan disk fisik (dengan kompresi). Dua metrik ini hanya tersedia jika sistem file Anda meminta kompresi data diaktifkan atau sebelumnya telah diaktifkan.

Anda dapat menentukan rasio kompresi sistem file Anda dengan membagi Sum dari statistik `LogicalDiskUsage` berdasarkan Sum dari statistik `PhysicalDiskUsage`. Untuk informasi tentang penggunaan metrik matematika untuk menghitung rasio ini, lihat [Matematika metrik: Rasio kompresi data](#).

Untuk informasi selengkapnya tentang cara memantau performa sistem file Anda, lihat [Memantau Amazon FSx for Lustre](#).

Labu akar kilau

Root squash adalah fitur administratif yang menambahkan lapisan tambahan kontrol akses file di atas kontrol akses berbasis jaringan saat ini dan izin file POSIX. Menggunakan fitur root squash, Anda dapat membatasi akses tingkat root dari klien yang mencoba mengakses sistem file FSx for Lustre Anda sebagai root.

Izin pengguna root diperlukan untuk melakukan tindakan administratif, seperti mengelola izin pada sistem file FSx for Lustre. Namun, akses root menyediakan akses tidak terbatas kepada pengguna, memungkinkan mereka untuk melewati pemeriksaan izin untuk mengakses, memodifikasi, atau menghapus objek sistem file. Dengan menggunakan fitur root squash, Anda dapat mencegah akses atau penghapusan data yang tidak sah dengan menentukan ID pengguna non-root (UID) dan ID grup (GID) untuk sistem file Anda. Pengguna root yang mengakses sistem file akan secara otomatis dikonversi ke pengguna/grup yang kurang istimewa yang ditentukan dengan izin terbatas yang ditetapkan oleh administrator penyimpanan.

Fitur root squash juga secara opsional memungkinkan Anda untuk memberikan daftar klien yang tidak terpengaruh oleh pengaturan root squash. Klien ini dapat mengakses sistem file sebagai root, dengan hak istimewa yang tidak terbatas.

Topik

- [Cara kerja root squash](#)
- [Mengelola root squash](#)

Cara kerja root squash

Fitur root squash bekerja dengan memetakan ulang ID pengguna (UID) dan ID grup (GID) pengguna root ke UID dan GID yang ditentukan oleh administrator sistem Lustre. Fitur root squash juga memungkinkan Anda secara opsional menentukan satu set klien yang pemetaan ulang UID/GID tidak berlaku.

Saat Anda membuat sistem file FSx for Lustre baru, root squash dinonaktifkan secara default. Anda mengaktifkan root squash dengan mengonfigurasi pengaturan root squash UID dan GID untuk sistem file FSx for Lustre Anda. Nilai UID dan GID adalah bilangan bulat yang dapat berkisar dari 0 hingga: 4294967294

- Nilai bukan nol untuk UID dan GID memungkinkan root squash. Nilai UID dan GID bisa berbeda, tetapi masing-masing harus berupa nilai bukan nol.
- Nilai 0 (nol) untuk UID dan GID menunjukkan root, dan karenanya menonaktifkan root squash.

Selama pembuatan sistem file, Anda dapat menggunakan konsol Amazon FSx untuk memberikan nilai UID dan GID root squash di properti Root Squash, seperti yang ditunjukkan pada [Untuk mengaktifkan root squash saat membuat sistem file \(konsol\)](#) Anda juga dapat menggunakan RootSquash parameter dengan API AWS CLI atau untuk memberikan nilai UID dan GID, seperti yang ditunjukkan pada [Untuk mengaktifkan root squash saat membuat sistem file \(CLI\)](#).

Secara opsional, Anda juga dapat menentukan daftar NID klien yang tidak berlaku root squash. NID klien adalah Identifier Jaringan Lustre yang digunakan untuk mengidentifikasi klien secara unik. Anda dapat menentukan NID sebagai satu alamat atau rentang alamat:

- Satu alamat dijelaskan dalam format NID Lustre standar dengan menentukan alamat IP klien diikuti oleh ID jaringan Lustre (misalnya,). `10.0.1.6@tcp`
- Rentang alamat dijelaskan menggunakan tanda hubung untuk memisahkan rentang (misalnya, `10.0.[2-10].[1-255]@tcp`).
- Jika Anda tidak menentukan NID klien apa pun, tidak akan ada pengecualian untuk melakukan root squash.

Saat membuat atau memperbarui sistem file, Anda dapat menggunakan properti Exceptions to Root Squash di konsol Amazon FSx untuk menyediakan daftar NID klien. Di API AWS CLI atau, gunakan NoSquashNids parameter. Untuk informasi lebih lanjut, lihat prosedur di [Mengelola root squash](#).

Note

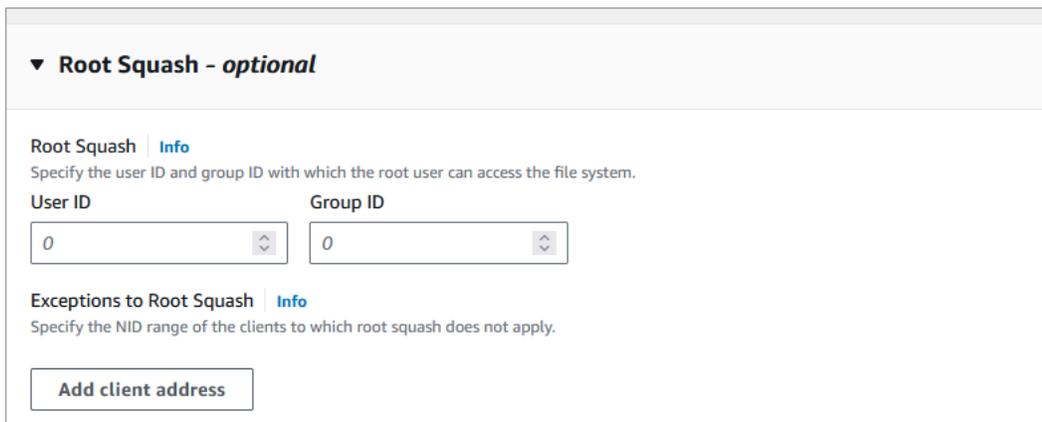
Root squash tidak didukung untuk pencadangan dan pemulihan. Untuk menggunakan backup dan restores, Anda harus menonaktifkan root squash dengan mengatur RootSquash parameter ke `0:0` dan parameter dengan API AWS CLI atau, atau `[]` dengan memilih Nonaktifkan di kotak dialog Update Root Squash Settings di konsol Amazon FSx. NoSquashNids

Mengelola root squash

Selama pembuatan sistem file, root squash dinonaktifkan secara default. Anda dapat mengaktifkan root squash saat membuat sistem file Amazon fsX for Lustre baru dari konsol Amazon AWS CLI FSx,, atau API.

Untuk mengaktifkan root squash saat membuat sistem file (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Ikuti prosedur untuk membuat sistem file baru yang dijelaskan di [Buat sistem file FSx for Lustre Anda](#) pada bagian Mulai.
3. Buka bagian Root Squash - opsional.



4. Untuk Root Squash, berikan ID pengguna dan grup yang dengannya pengguna root dapat mengakses sistem file. Anda dapat menentukan bilangan bulat apa pun dalam kisaran 1 -4294967294:
 1. Untuk ID Pengguna, tentukan ID pengguna untuk pengguna root yang akan digunakan.
 2. Untuk ID Grup, tentukan ID grup untuk pengguna root yang akan digunakan.

5. (Opsional) Untuk Pengecualian Root Squash, lakukan hal berikut:
 1. Pilih Tambahkan alamat klien.
 2. Di bidang Alamat klien, tentukan alamat IP klien yang tidak diterapkan root squash, Untuk informasi tentang format alamat IP, lihat [Cara kerja root squash](#).
 3. Ulangi sesuai kebutuhan untuk menambahkan lebih banyak alamat IP klien.
6. Menyelesaikan wizard seperti yang Anda lakukan ketika Anda membuat sistem file baru.
7. Pilih Periksa dan buat.
8. Tinjau pengaturan yang Anda pilih untuk sistem file Amazon FSx for Lustre, lalu pilih Buat sistem file.

Ketika sistem file Tersedia, root squash diaktifkan.

Untuk mengaktifkan root squash saat membuat sistem file (CLI)

- Untuk membuat sistem file FSx for Lustre dengan root squash diaktifkan, gunakan perintah Amazon FSx CLI dengan parameter. [create-file-system](#)RootSquashConfiguration Operasi API yang sesuai adalah [CreateFileSystem](#).

Untuk RootSquashConfiguration parameter, atur opsi berikut:

- RootSquash— Nilai UID: GID yang dipisahkan kolon yang menentukan ID pengguna dan ID grup untuk digunakan pengguna root. Anda dapat menentukan bilangan bulat dalam kisaran 0 — 4294967294 (0 adalah root) untuk setiap ID (misalnya,65534 : 65534).
- NoSquashNids— Tentukan Lustre Network Identifiers (NID) klien yang root squash tidak berlaku. Untuk informasi tentang format NID klien, lihat [Cara kerja root squash](#).

Contoh berikut membuat sistem file FSx for Lustre dengan root squash diaktifkan:

```
$ aws fsx create-file-system \
  --client-request-token CRT1234 \
  --file-system-type LUSTRE \
  --file-system-type-version 2.15 \
  --lustre-configuration
  "DeploymentType=PERSISTENT_2,PerUnitStorageThroughput=250,DataCompressionType=LZ4,
  \
  RootSquashConfiguration={RootSquash="65534:65534",\
  NoSquashNids=["10.216.123.47@tcp", "10.216.12.176@tcp"]} " \
```

```
--storage-capacity 2400 \  
--subnet-ids subnet-123456 \  
--tags Key=Name,Value=Lustre-TEST-1 \  
--region us-east-2
```

Setelah berhasil membuat sistem file, Amazon FSx mengembalikan deskripsi sistem file sebagai JSON, seperti yang ditunjukkan dalam contoh berikut.

```
{  
  
  "FileSystems": [  
    {  
      "OwnerId": "111122223333",  
      "CreationTime": 1549310341.483,  
      "FileSystemId": "fs-0123456789abcdef0",  
      "FileSystemType": "LUSTRE",  
      "FileSystemTypeVersion": "2.15",  
      "Lifecycle": "CREATING",  
      "StorageCapacity": 2400,  
      "VpcId": "vpc-123456",  
      "SubnetIds": [  
        "subnet-123456"  
      ],  
      "NetworkInterfaceIds": [  
        "eni-039fcf55123456789"  
      ],  
      "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",  
      "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/  
fs-0123456789abcdef0",  
      "Tags": [  
        {  
          "Key": "Name",  
          "Value": "Lustre-TEST-1"  
        }  
      ],  
      "LustreConfiguration": {  
        "DeploymentType": "PERSISTENT_2",  
        "DataCompressionType": "LZ4",  
        "PerUnitStorageThroughput": 250,  
        "RootSquashConfiguration": {  
          "RootSquash": "65534:65534",  
          "NoSquashNids": "10.216.123.47@tcp 10.216.29.176@tcp"  
        }  
      }  
    }  
  ]  
}
```

```

    }
  }
]
}

```

Anda juga dapat memperbarui pengaturan root squash dari sistem file yang ada menggunakan konsol Amazon FSx AWS CLI, atau API. Misalnya, Anda dapat mengubah nilai UID dan GID root squash, menambah atau menghapus NID klien, atau menonaktifkan root squash.

Untuk memperbarui pengaturan root squash pada sistem file yang ada (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Arahkan ke sistem File, dan pilih sistem file Lustre yang ingin Anda kelola root squash.
3. Untuk Tindakan, pilih Perbarui root squash. Atau, di panel Ringkasan, pilih Perbarui di sebelah bidang Root Squash sistem file untuk menampilkan kotak dialog Update Root Squash Settings.

Update Root Squash Settings [X]

File system ID
fs-04be0cb4339a509e8

Root Squash - optional
Specify the user ID and group ID with which the root user can access the file system.

User ID: 65534 [v]

Group ID: 65534 [v]

Exceptions to Root Squash
Specify the NID range of the clients to which root squash does not apply.

Client addresses

10.0.1.105@tcp [Remove]

[Add client address]

Cancel [Disable] [Update]

4. Untuk Root Squash, perbarui ID pengguna dan grup yang dengannya pengguna root dapat mengakses sistem file. Anda dapat menentukan bilangan bulat apa pun dalam kisaran 0 —4294967294. Untuk menonaktifkan root squash, tentukan 0 (nol) untuk kedua ID.

1. Untuk ID Pengguna, tentukan ID pengguna untuk pengguna root yang akan digunakan.

2. Untuk ID Grup, tentukan ID grup untuk pengguna root yang akan digunakan.
5. Untuk Pengecualian terhadap Root Squash, lakukan hal berikut:
 1. Pilih Tambahkan alamat klien.
 2. Di bidang Alamat klien, tentukan alamat IP klien yang tidak diterapkan root squash,
 3. Ulangi sesuai kebutuhan untuk menambahkan lebih banyak alamat IP klien.
6. Pilih Perbarui.

 Note

Jika root squash diaktifkan dan Anda ingin menonaktifkannya, pilih Nonaktifkan alih-alih melakukan langkah 4-6.

Anda dapat memantau kemajuan pembaruan pada laman detail sistem file di tab Pembaruan.

Untuk memperbarui pengaturan root squash pada sistem file yang ada (CLI)

Untuk memperbarui pengaturan root squash untuk sistem file FSx for Lustre yang ada, gunakan perintah. AWS CLI [update-file-system](#) Operasi API yang sesuai adalah [UpdateFileSystem](#).

Atur parameter berikut:

- Atur `--file-system-id` ke ID dari sistem file yang Anda perbarui.
- Atur `--lustre-configuration RootSquashConfiguration` opsi sebagai berikut:
 - RootSquash— Tetapkan nilai UID: GID yang dipisahkan kolon yang menentukan ID pengguna dan ID grup untuk digunakan pengguna root. Anda dapat menentukan bilangan bulat apa pun dalam kisaran 0 - 4294967294 (0 adalah root) untuk setiap ID. Untuk menonaktifkan root squash, tentukan nilai 0:0 UID:GID.
 - NoSquashNids— Tentukan Lustre Network Identifiers (NID) klien yang root squash tidak berlaku. Gunakan [] untuk menghapus semua NID klien, yang berarti tidak akan ada pengecualian untuk melakukan root squash.

Perintah ini menentukan bahwa root squash diaktifkan menggunakan 65534 sebagai nilai untuk ID pengguna root dan ID grup.

```
$ aws fsx update-file-system \
```

```
--file-system-id fs-0123456789abcdef0 \
--lustre-configuration RootSquashConfiguration={RootSquash="65534:65534", \
  NoSquashNids=["10.216.123.47@tcp", "10.216.12.176@tcp"]}
```

Jika perintah berhasil, Amazon FSx for Lustre mengembalikan respons dalam format JSON.

Anda dapat melihat pengaturan root squash sistem file Anda di panel Ringkasan halaman detail sistem file di konsol Amazon FSx atau dalam respons perintah [describe-file-systems](#) CLI (tindakan API yang setara adalah) [DescribeFileSystems](#)

FSx for Lustre status sistem berkas

[Anda dapat melihat status sistem file Amazon FSx dengan menggunakan konsol Amazon FSx, AWS CLI perintah describe-file-systems, atau Sistem operasi API. DescribeFile](#)

Status sistem file	Deskripsi
TERSEDIA	Sistem file dalam keadaan sehat, dan dapat dijangkau dan tersedia untuk digunakan.
MEMBUAT	Amazon FSx sedang membuat sistem file yang baru.
MENGHAPUS	Amazon FSx sedang menghapus sistem file yang ada.
MEMPERBARUI	Sistem file sedang mengalami pembaruan yang dikerjakan pelanggan.
SALAH KONFIGURASI	Sistem file sedang dalam keadaan gagal tetapi dapat dipulihkan.
GAGAL	Status ini dapat berarti salah satu dari berikut ini: <ul style="list-style-type: none"> Sistem file telah gagal dan Amazon FSx tidak dapat memulihkannya. Saat membuat sistem file yang baru, Amazon FSx tidak dapat membuat sistem file.

Tandai sumber daya Amazon FSx Anda

Untuk membantu mengelola sistem file dan sumber daya Amazon FSx for Lustre lainnya, Anda dapat menetapkan metadata Anda sendiri ke setiap sumber daya dalam bentuk tag. Tag memungkinkan Anda untuk mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Hal ini berguna ketika Anda memiliki banyak sumber daya dengan jenis yang sama—Anda dapat dengan cepat mengidentifikasi sumber daya tertentu berdasarkan tag yang telah Anda tetapkan. Topik ini menjelaskan tag dan menunjukkan cara membuatnya.

Topik

- [Dasar-dasar tag](#)
- [Menandai Sumber Daya Anda](#)
- [Pembatasan tanda](#)
- [Izin dan tag](#)

Dasar-dasar tag

Tag adalah label yang Anda tetapkan ke AWS sumber daya. Setiap tag terdiri dari kunci dan nilai opsional, yang keduanya Anda tentukan.

Tag memungkinkan Anda untuk mengkategorikan AWS sumber daya Anda dengan cara yang berbeda, misalnya, berdasarkan tujuan, pemilik, atau lingkungan. Misalnya, Anda dapat menentukan satu set tag untuk sistem file Amazon fsX for Lustre 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.

Tag tidak memiliki arti semantik untuk Amazon FSx dan ditafsirkan secara ketat sebagai serangkaian karakter. Selain itu, tag tidak secara otomatis ditetapkan ke sumber daya Anda. Anda dapat mengedit kunci dan nilai tanda, dan dapat menghapus tanda dari sumber daya kapan saja. Anda dapat mengatur nilai tanda ke string kosong, tetapi tidak dapat mengatur nilai tanda ke null. Jika Anda menambahkan tanda yang memiliki kunci yang sama dengan tanda yang telah ada pada sumber daya tersebut, nilai yang baru akan menimpa nilai yang lama. Jika sumber daya dihapus, semua tanda untuk sumber daya tersebut juga akan dihapus.

Jika Anda menggunakan Amazon FSx for Lustre API AWS , CLI, atau SDK, Anda `TagResource` dapat menggunakan AWS tindakan API untuk menerapkan tag ke sumber daya yang ada. Selain itu, beberapa tindakan pembuatan sumber daya memungkinkan Anda menentukan tag untuk sumber daya saat sumber daya tersebut dibuat. Jika tag tidak dapat diterapkan selama pembuatan sumber daya, kami akan mengembalikan proses pembuatan sumber daya. Hal ini untuk memastikan bahwa sumber daya dibuat dengan tag atau tidak akan dibuat sama sekali, dan tidak akan ada sumber daya yang dibiarkan tidak bertanda. Dengan menandai sumber daya saat pembuatan, Anda dapat menghilangkan kebutuhan untuk menjalankan skrip penandaan kustom setelah pembuatan sumber daya. Untuk informasi selengkapnya tentang memungkinkan pengguna menandai sumber daya saat pembuatan, lihat [Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat](#).

Menandai Sumber Daya Anda

Anda dapat menandai Amazon FSx for Lustre resource yang ada di akun Anda. Jika menggunakan konsol Amazon FSx, Anda dapat menerapkan tag ke sumber daya menggunakan tab Tag di layar sumber daya yang relevan. Saat Anda membuat sumber daya, Anda dapat menerapkan kunci Nama dengan nilai, dan Anda dapat menerapkan tag pilihan Anda saat membuat sistem file baru. Konsol dapat mengatur sumber daya sesuai dengan tag Nama, tetapi tag ini tidak memiliki arti semantik apa pun terhadap layanan Amazon FSx for Lustre.

Anda dapat menerapkan izin tingkat sumber daya berbasis tag dalam kebijakan IAM Anda ke tindakan Amazon FSx for Lustre API yang mendukung penandaan pada pembuatan untuk menerapkan kontrol terperinci atas pengguna dan grup yang dapat menandai sumber daya saat pembuatan. Sumber daya Anda diamankan secara tepat sejak pembuatan—tanda segera diterapkan pada sumber daya Anda, oleh karena itu, izin tingkat sumber daya berbasis tanda yang mengontrol penggunaan sumber daya langsung berlaku. Sumber daya Anda dapat dilacak dan dilaporkan dengan lebih akurat. Anda dapat menerapkan penggunaan pemberian tag pada sumber daya baru serta mengontrol kunci dan nilai tag mana yang ditetapkan pada sumber daya Anda.

Anda juga dapat menerapkan izin tingkat sumber daya ke tindakan Amazon `fsX TagResource for UntagResource` Lustre API dalam kebijakan IAM untuk mengontrol kunci dan nilai tag mana yang disetel pada sumber daya yang ada.

Untuk informasi selengkapnya tentang penandaan sumber daya untuk penagihan, lihat [Menggunakan tanda alokasi biaya](#) dalam Buku Panduan AWS Billing .

Pembatasan tanda

Batasan dasar berikut berlaku untuk tag:

- Jumlah maksimum tag per sumber daya – 50
- Untuk setiap sumber daya, setiap kunci tanda harus unik, dan setiap kunci tanda hanya dapat memuat satu nilai.
- Panjang kunci maksimum – 128 karakter Unicode dalam UTF-8
- Panjang nilai maksimum – 256 karakter Unicode dalam UTF-8
- Karakter yang diizinkan untuk tag Amazon FSx for Lustre adalah: huruf, angka, dan spasi yang dapat direpresentasikan dalam UTF-8, dan karakter berikut: + - =. _:/@.
- Kunci dan nilai tag peka huruf besar dan kecil.
- `aws :` Awalan dicadangkan untuk AWS digunakan. Jika tag memiliki kunci tag dengan awalan ini, Anda tidak dapat mengedit atau menghapus kunci atau nilai tag tersebut. Tag dengan awalan `aws :` tidak dihitung terhadap tag per batas sumber daya.

Anda tidak dapat menghapus sumber daya hanya berdasarkan tagnya; Anda harus menentukan pengenal sumber daya. Misalnya, untuk menghapus sistem file yang Anda tag dengan kunci tag yang disebut `DeleteMe`, Anda harus menggunakan `DeleteFileSystem` tindakan dengan pengenal sumber daya sistem file, seperti `fs-1234567890abcdef0`.

Saat Anda menandai sumber daya publik atau bersama, tag yang Anda tetapkan hanya tersedia untuk Anda Akun AWS; tidak ada orang lain yang Akun AWS akan memiliki akses ke tag tersebut. Untuk kontrol akses berbasis tag ke sumber daya bersama, masing-masing Akun AWS harus menetapkan set tag sendiri untuk mengontrol akses ke sumber daya.

Izin dan tag

Untuk informasi selengkapnya tentang izin yang diperlukan untuk menandai sumber daya Amazon FSx saat pembuatan, [Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat](#) lihat. Untuk informasi selengkapnya tentang penggunaan tag untuk membatasi akses ke sumber daya Amazon FSx dalam kebijakan IAM, lihat. [Menggunakan tanda untuk mengontrol akses ke sumber daya Amazon FSx sumber daya](#)

Jendela pemeliharaan Amazon FSx for Lustre

Amazon FSx for Lustre melakukan patch perangkat lunak rutin untuk perangkat lunak Lustre yang dikelolanya. Window pemeliharaan adalah kesempatan Anda untuk mengontrol hari dan waktu dalam seminggu patch perangkat lunak ini terjadi.

Patching hanya memerlukan sebagian kecil dari window pemeliharaan 30 menit Anda. Selama beberapa menit waktu, sistem file Anda sementara tidak akan tersedia. Anda memilih window pemeliharaan selama pembuatan sistem file. Jika Anda tidak memiliki preferensi waktu, maka jendela default 30 menit ditugaskan.

FSx for Lustre 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 dijadwalkan setidaknya sekali setiap 14 hari. Jika patch dirilis dan Anda belum menjadwalkan jendela pemeliharaan dalam 14 hari, FSx for Lustre akan melanjutkan pemeliharaan pada sistem file untuk memastikan keamanan dan keandalannya.

Anda dapat menggunakan Amazon FSx Management Console AWS CLI, AWS API, atau salah satu AWS SDK untuk mengubah jendela pemeliharaan sistem file Anda.

Untuk mengubah window pemeliharaan yang diinginkan menggunakan konsol

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Di panel navigasi, pilih Sistem file.
3. Pilih sistem file yang ingin Anda ubah jendela pemeliharaannya. Laman detail sistem file muncul.
4. Pilih tab Pemeliharaan. Panel Pengaturan window pemeliharaan muncul.
5. Pilih Edit dan masukkan hari dan waktu baru yang Anda inginkan agar window pemeliharaan dimulai.
6. Pilih Simpan untuk menyimpan perubahan Anda. Waktu mulai pemeliharaan baru ditampilkan di panel Pengaturan.

Anda dapat mengubah jendela pemeliharaan untuk sistem file Anda menggunakan perintah [update-file-system](#) CLI. Jalankan perintah berikut, ganti ID sistem file dengan ID untuk sistem file Anda, serta tanggal dan waktu dengan kapan Anda ingin memulai window.

```
aws fsx update-file-system --file-system-id fs-01234567890123456 --lustre-configuration  
WeeklyMaintenanceStartTime=1:01:30
```

Menghapus sistem file

Anda dapat menghapus sistem file Amazon FSx for Lustre menggunakan konsol Amazon FSx AWS CLI, API Amazon FSx. Sebelum menghapus sistem file FSx for Lustre, [Anda](#) harus melepaskannya dari setiap instans Amazon EC2 yang terhubung. Pada sistem file terkait S3, untuk memastikan semua data Anda ditulis kembali ke S3 sebelum menghapus sistem file Anda, Anda dapat memantau metrik [AgeOfOldestQueuedPesan](#) menjadi nol (jika menggunakan ekspor otomatis) atau Anda dapat menjalankan tugas repositori data [ekspor](#). Jika Anda mengaktifkan ekspor otomatis dan ingin menggunakan tugas repositori data ekspor, Anda harus menonaktifkan ekspor otomatis sebelum menjalankan tugas repositori data ekspor.

Untuk menghapus sistem file setelah melepas dari setiap instans Amazon EC2:

- Menggunakan konsol — Ikuti prosedur yang dijelaskan di [Pembersihan sumber daya](#).
- Menggunakan API atau CLI - Gunakan operasi API [DeleteFileSistem](#) atau perintah CLI [delete-file-system](#).

Migrasi ke Amazon FSx for Lustre menggunakan AWS DataSync

Anda dapat menggunakan AWS DataSync untuk mentransfer data antara FSx for Lustre sistem file. 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. AWS Direct Connect DataSync dapat mentransfer data dan metadata sistem file Anda, seperti kepemilikan, stempel waktu, dan izin akses.

Cara memigrasi file yang ada ke FSx for Lustre menggunakan AWS DataSync

Anda dapat menggunakan DataSync sistem file FSx for Lustre untuk melakukan migrasi data satu kali, secara berkala menelan data untuk beban kerja terdistribusi, dan menjadwalkan replikasi untuk perlindungan dan pemulihan data. Untuk informasi tentang skenario transfer tertentu, lihat [Di mana saya dapat mentransfer data saya?](#) dalam AWS DataSync User Guide.

Prasyarat

Untuk memigrasikan data ke penyiapan FSx for Lustre, Anda memerlukan server dan jaringan yang memenuhi persyaratan. DataSync Untuk mempelajari lebih lanjut, lihat [Persyaratan untuk DataSync](#) di Panduan AWS DataSync Pengguna.

- Anda telah membuat tujuan FSx untuk sistem file Lustre. Untuk informasi selengkapnya, lihat [Buat sistem file FSx for Lustre Anda](#).
- Sistem file sumber dan tujuan terhubung dalam virtual private cloud (VPC) yang sama. Sistem file sumber dapat ditemukan di lokasi atau di VPC Amazon lain,, Wilayah AWS atau Akun AWS, tetapi harus berada di jaringan yang diintip dengan sistem file tujuan menggunakan Amazon VPC Peering, Transit Gateway, atau. AWS Direct Connect AWS VPN Untuk informasi selengkapnya, lihat [Apa yang dimaksud peering VPC?](#) di Panduan Peering Amazon VPC.

Note

DataSync Hanya dapat mentransfer Akun AWS ke atau dari FSx for Lustre jika lokasi transfer lainnya adalah Amazon S3.

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 AWS DataSync Pengguna:

- [Mentransfer antar penyimpanan lokal dan AWS](#)
- [Mengkonfigurasi AWS DataSync transfer dengan Amazon FSx](#) for AWS DataSync Lustre di Panduan Pengguna.
- [Terapkan agen Anda di Amazon EC2](#)

Memantau Amazon FSx for Lustre

Anda dapat menggunakan alat pemantauan otomatis berikut untuk menonton Amazon FSx for Lustre dan melaporkan ketika ada sesuatu yang salah:

- Pemantauan menggunakan Amazon CloudWatch — CloudWatch mengumpulkan dan memproses data mentah dari Amazon FSx for Lustre menjadi metrik yang dapat dibaca, mendekati waktu nyata. Anda dapat membuat CloudWatch alarm yang mengirimkan pesan Amazon SNS saat alarm berubah status.
- Pemantauan menggunakan pencatatan Lustre - Anda dapat memantau peristiwa logging yang diaktifkan untuk sistem file Anda. Lustre logging menulis peristiwa ini ke Amazon CloudWatch Logs.
- AWS CloudTrail pemantauan log - Bagikan file log antar akun, pantau file CloudTrail log secara real time dengan mengirimkannya ke CloudWatch Log, menulis aplikasi pemrosesan log di Java, dan validasi bahwa file log Anda tidak berubah setelah pengiriman oleh CloudTrail.

Topik

- [Pemantauan CloudWatch dengan Amazon](#)
- [Logging dengan Amazon CloudWatch Logs](#)
- [Logging FSx untuk panggilan API Lustre dengan AWS CloudTrail](#)

Pemantauan CloudWatch dengan Amazon

Anda dapat memantau sistem file menggunakan Amazon CloudWatch, yang mengumpulkan dan memproses data mentah dari Amazon FSx for Lustre menjadi metrik hampir real-time yang dapat dibaca. Statistik ini dipertahankan untuk jangka waktu 15 bulan, sehingga Anda dapat mengakses informasi historis dan mendapatkan perspektif yang lebih baik tentang bagaimana kinerja aplikasi web atau layanan web Anda. Secara default, data metrik Amazon FSx for Lustre dikirim secara otomatis CloudWatch pada periode 1 menit. Untuk informasi selengkapnya CloudWatch, lihat [Apa itu Amazon CloudWatch?](#) di Panduan CloudWatch Pengguna Amazon.

CloudWatch metrik dilaporkan sebagai Byte mentah. Byte tidak dibulatkan baik ke desimal atau biner ganda unit.

Metrik sistem file

FSx for Lustre menerbitkan metrik berikut ke dalam namespace di FSx CloudWatch. Untuk setiap metrik, FSx for Lustre memancarkan titik data per disk per menit. Untuk melihat detail sistem file agregat, Anda dapat menggunakan statistik Sum. Perhatikan bahwa server file di belakang sistem file FSx for Lustre Anda tersebar di beberapa disk.

Metrik	Deskripsi
DataReadBytes	<p>Jumlah byte untuk operasi baca sistem file.</p> <p>Statistik Sum adalah jumlah total byte yang terkait dengan operasi baca selama periode. Statistik Minimum adalah jumlah minimum byte yang terkait dengan operasi baca pada disk tunggal. Statistik Maximum adalah jumlah minimum byte yang terkait dengan operasi baca pada disk. Statistik Average adalah jumlah rata-rata byte yang terkait dengan operasi baca pada disk. Statistik SampleCount adalah jumlah disk.</p> <p>Untuk menghitung throughput rata-rata (byte per detik) untuk suatu periode, bagi statistik Sum dengan jumlah detik dalam periode tersebut.</p> <p>Unit:</p> <ul style="list-style-type: none"> • Byte untuk Sum, Minimum, Maximum, dan Average. • Jumlah untuk SampleCount . <p>Statistik yang valid:Sum,Minimum,Maximum,Average, SampleCount</p>
DataWriteBytes	<p>Jumlah byte untuk operasi tulis sistem file.</p> <p>Statistik Sum adalah jumlah total byte yang terkait dengan operasi tulis. Statistik Minimum adalah jumlah minimum byte yang terkait dengan operasi tulis pada disk tunggal. Statistik Maximum adalah jumlah minimum byte yang terkait dengan operasi tulis pada disk. Statistik Average adalah jumlah rata-rata byte yang terkait dengan operasi tulis per disk. Statistik SampleCount adalah jumlah disk.</p>

Metrik	Deskripsi
	<p>Untuk menghitung throughput rata-rata (byte per detik) untuk suatu periode, bagi statistik Sum dengan jumlah detik dalam periode tersebut.</p> <p>Unit:</p> <ul style="list-style-type: none"> • Byte untuk Sum, Minimum, Maximum, dan Average. • Jumlah untuk SampleCount . <p>Statistik yang valid:Sum,Minimum,Maximum,Average, SampleCount</p>
DataReadOperations	<p>Jumlah operasi baca.</p> <p>Statistik Sum adalah jumlah total operasi baca. Statistik Minimum adalah jumlah minimum operasi baca pada disk tunggal. Statistik Maximum adalah jumlah maksimum byte yang terkait dengan operasi baca pada disk. Statistik Average adalah jumlah rata-rata operasi baca per disk. Statistik SampleCount adalah jumlah disk.</p> <p>Untuk menghitung jumlah rata-rata operasi baca (operasi per detik) selama suatu periode, bagi statistik Sum dengan jumlah detik dalam periode tersebut.</p> <p>Unit:</p> <ul style="list-style-type: none"> • Byte untuk Sum, Minimum, Maximum, dan Average. • Jumlah untuk SampleCount . <p>Statistik yang valid:Sum,Minimum,Maximum,Average, SampleCount</p>

Metrik	Deskripsi
DataWrite Operations	<p>Jumlah operasi tulis.</p> <p>Statistik Sum adalah jumlah total operasi tulis. Statistik Minimum adalah jumlah minimum operasi tulis pada disk tunggal. Maximum Statistik adalah jumlah maksimum operasi tulis pada disk. Statistik Average adalah jumlah rata-rata operasi tulis per disk. Statistik SampleCount adalah jumlah disk.</p> <p>Untuk menghitung jumlah rata-rata operasi tulis (operasi per detik) selama suatu periode, bagi statistik Sum dengan jumlah detik dalam periode tersebut.</p> <p>Unit:</p> <ul style="list-style-type: none">• Byte untuk Sum, Minimum, Maximum, dan Average.• Jumlah untuk SampleCount . <p>Statistik yang valid:Sum,Minimum,Maximum,Average, SampleCount</p>

Metrik	Deskripsi
MetadataOperations	<p>Jumlah operasi metadata.</p> <p>Statistik <code>Sum</code> adalah hitungan operasi metadata. Statistik <code>Minimum</code> adalah jumlah minimum operasi metadata per disk. Statistik <code>Maximum</code> adalah jumlah maksimum operasi metadata per disk. Statistik <code>Average</code> adalah jumlah rata-rata operasi metadata per disk. Statistik <code>SampleCount</code> adalah jumlah disk.</p> <p>Untuk menghitung jumlah rata-rata operasi metadata (operasi per detik) selama suatu periode, bagi statistik <code>Sum</code> dengan jumlah detik dalam periode tersebut.</p> <p>Unit:</p> <ul style="list-style-type: none"> Jumlah untuk <code>Sum</code>, <code>Minimum</code>, <code>Maximum</code>, <code>Average</code>, dan <code>SampleCount</code> . <p>Statistik yang valid: <code>Sum</code>, <code>Minimum</code>, <code>Maximum</code>, <code>Average</code>, <code>SampleCount</code></p>
FreeDataStorageCapacity	<p>Jumlah kapasitas penyimpanan lokal yang tersedia.</p> <p>Statistik <code>Sum</code> adalah jumlah total byte yang tersedia dalam sistem file. Statistik <code>Minimum</code> adalah jumlah total byte yang tersedia dalam disk paling penuh. Statistik <code>Maximum</code> adalah jumlah total byte yang tersedia di disk dengan sisa penyimpanan paling banyak. Statistik <code>Average</code> adalah jumlah rata-rata byte yang tersedia per disk. Statistik <code>SampleCount</code> adalah jumlah disk.</p> <p>Unit:</p> <ul style="list-style-type: none"> Byte untuk <code>Sum</code>, <code>Minimum</code>, <code>Maximum</code>. Jumlah untuk <code>SampleCount</code> . <p>Statistik yang valid: <code>Sum</code>, <code>Minimum</code>, <code>Maximum</code>, <code>Average</code>, <code>SampleCount</code></p>

Metrik	Deskripsi
LogicalDiskUsage	<p>Jumlah data logis yang disimpan (tidak dimampatkan).</p> <p>Statistik Sum adalah jumlah total byte logis yang disimpan dalam sistem file. Statistik Minimum adalah jumlah byte logis minimum yang disimpan dalam sebuah disk dalam sistem file. Statistik Maximum adalah jumlah total byte logis maksimum yang disimpan dalam sebuah disk dalam sistem file. Statistik Average adalah jumlah rata-rata byte logis yang disimpan per disk. Statistik SampleCount adalah jumlah disk.</p> <p>Unit:</p> <ul style="list-style-type: none"> • Byte untuk Sum, Minimum, Maximum. • Jumlah untuk SampleCount . <p>Statistik yang valid:Sum,Minimum,Maximum,Average, SampleCount</p>
PhysicalDiskUsage	<p>Jumlah penyimpanan yang ditempati secara fisik oleh data sistem file (terkompresi).</p> <p>Statistik Sum adalah jumlah total byte yang ditempati di disk dalam sistem file. Statistik Minimum adalah jumlah total byte yang ditempati di disk paling kosong. Statistik Maximum adalah jumlah total byte yang ditempati di disk paling penuh. Statistik Average adalah jumlah rata-rata byte yang ditempati per disk. Statistik SampleCount adalah jumlah disk.</p> <p>Unit:</p> <ul style="list-style-type: none"> • Byte untuk Sum, Minimum, Maximum. • Jumlah untuk SampleCount . <p>Statistik yang valid:Sum,Minimum,Maximum,Average, SampleCount</p>

Metrik metadata sistem file

FSx for Lustre menerbitkan metrik metadata sistem file berikut ke dalam namespace di. FSx CloudWatch Metrik ini menggunakan dimensi untuk memungkinkan pengukuran data metadata Anda yang lebih terperinci. Semua metadata metrik memiliki dimensi dan dimensi. `FileSystemId` `StorageTargetId` Metrik metadata sistem file diekspos hanya jika sistem file Anda memiliki konfigurasi metadata yang ditentukan.

Metrik	Deskripsi
<code>DiskReadOperations</code>	<p>Jumlah operasi baca untuk server file yang mengakses volume penyimpanan. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang. Ada satu metrik yang dipancarkan setiap menit untuk setiap volume penyimpanan sistem file Anda.</p> <p><code>SumStatistik</code> adalah jumlah total operasi baca yang dilakukan oleh volume penyimpanan yang diberikan selama periode yang ditentukan.</p> <p><code>AverageStatistik</code> adalah jumlah rata-rata operasi baca yang dilakukan setiap menit dengan volume penyimpanan yang diberikan selama periode yang ditentukan.</p> <p><code>MinimumStatistik</code> adalah jumlah operasi baca terendah yang dilakukan setiap menit dengan volume penyimpanan yang diberikan selama periode yang ditentukan.</p> <p><code>MaximumStatistik</code> adalah jumlah operasi baca tertinggi yang dilakukan setiap menit dengan volume penyimpanan yang diberikan selama periode yang ditentukan.</p>

Metrik	Deskripsi
	<p>Untuk menghitung rata-rata IOPS disk metadata selama periode tersebut, gunakan <code>Average</code> statistik dan bagi hasilnya dengan 60 (detik).</p> <p>Unit: Hitungan</p> <p>Statistik yang valid: <code>Sum</code>, <code>Average</code>, <code>Minimum</code>, dan <code>Maximum</code></p>

Metrik	Deskripsi
DiskWriteOperations	<p>Jumlah operasi tulis untuk server file yang mengakses volume penyimpanan.</p> <p>Jumlah operasi tulis ke volume penyimpanan ini. Semua lalu lintas dipertimbangkan dalam metrik ini, termasuk tugas latar belakang. Ada satu metrik yang dipancarkan setiap menit untuk setiap volume penyimpanan sistem file Anda.</p> <p>SumStatistik adalah jumlah total operasi penulisan yang dilakukan oleh volume penyimpanan yang diberikan selama periode yang ditentukan.</p> <p>AverageStatistik adalah jumlah rata-rata operasi tulis yang dilakukan setiap menit dengan volume penyimpanan yang diberikan selama periode yang ditentukan.</p> <p>Untuk menghitung rata-rata IOPS disk metadata selama periode tersebut, gunakan Average statistik dan bagi hasilnya dengan 60 (detik).</p> <p>Unit: Hitungan</p> <p>Statistik yang valid: Sum dan Average</p>
FileCreateOperations	<p>Jumlah total operasi pembuatan file.</p> <p>Unit: Jumlah</p>
FileOpenOperations	<p>Jumlah total operasi terbuka file.</p> <p>Unit: Jumlah</p>

Metrik	Deskripsi
FileDeleteOperations	Jumlah total operasi penghapusan file. Unit: Jumlah
StatOperations	Jumlah total operasi stat. Unit: Jumlah
RenameOperations	Jumlah total penggantian nama direktori, apakah penggantian nama direktori di tempat atau penggantian nama lintas direktori. Unit: Jumlah

AutoImport dan AutoExport metrik

FSx for Lustre menerbitkan metrik berikut (impor otomatis `AutoExport`) dan (ekspor otomatis `AutoImport`) ke dalam namespace di `FSx CloudWatch`. Metrik ini menggunakan dimensi untuk memungkinkan pengukuran data Anda yang lebih terperinci. Semua `AutoImport` dan `AutoExport` metrik memiliki `Publisher` dimensi `FileSystemId` dan dimensi.

Metrik	Deskripsi
AgeOfOldestQueuedMessage Dimensi: <code>AutoExport</code>	Usia, dalam hitungan detik, dari pesan tertua yang menunggu untuk diekspor. AverageStatistik adalah usia rata-rata pesan tertua yang menunggu untuk diekspor. MaximumStatistik adalah jumlah maksimum detik pesan yang hidup dalam antrian ekspor. MinimumStatistik adalah jumlah minimum detik pesan yang hidup dalam antrian ekspor. Nilai nol menunjukkan bahwa tidak ada pesan yang menunggu untuk diekspor.

Metrik	Deskripsi
	<p>Unit: detik</p> <p>Statistik yang valid: Average, Minimum, Maximum</p>
<p>RepositoryRenameOperations</p> <p>Dimensi: AutoExport</p>	<p>Jumlah penggantian nama yang diproses oleh sistem file sebagai respons terhadap penggantian nama direktori yang lebih besar.</p> <p>SumStatistik adalah jumlah total operasi ganti nama yang dihasilkan dari penggantian nama direktori. AverageStatistik adalah jumlah rata-rata operasi penggantian nama untuk sistem file. MaximumStatistik adalah jumlah maksimum operasi ganti nama yang terkait dengan penggantian nama direktori pada sistem file. MinimumStatistik adalah jumlah minimum penggantian nama yang terkait dengan penggantian nama direktori pada sistem file.</p> <p>Unit: Hitungan</p> <p>Statistik yang valid: Sum, Minimum, Maximum, Average</p>

Metrik	Deskripsi
AgeOfOldestQueuedMessage Dimensi: AutoImport	<p>Usia, dalam hitungan detik, dari pesan tertua yang menunggu untuk diimpor.</p> <p>AverageStatistik adalah usia rata-rata pesan tertua yang menunggu untuk diimpor. MaximumStatistik adalah jumlah maksimum detik pesan yang hidup dalam antrian impor. MinimumStatistik adalah jumlah minimum detik pesan yang hidup dalam antrian impor. Nilai nol menunjukkan bahwa tidak ada pesan yang menunggu untuk diimpor.</p> <p>Unit: detik</p> <p>Statistik yang valid:Average,Minimum,Maximum</p>

Dimensi Amazon FSx for Lustre

Metrik Amazon FSx for Lustre FSx menggunakan namespace dan menyediakan metrik untuk dimensi. FileSystemId ID sistem file dapat ditemukan menggunakan describe-file-systems AWS CLI perintah, dan mengambil bentuk *fs-01234567890123456*.

StorageTargetIdDimensi tersedia CloudWatch untuk menunjukkan MDT (target metadata) mana yang menerbitkan metrik metadata sistem file. A StorageTargetId mengambil bentuk MDTxxxx (misalnya,MDT0001).

PublisherDimensi tersedia di CloudWatch dan AWS CLI untuk AutoImport metrik AutoImport dan untuk menunjukkan layanan mana yang menerbitkan metrik.

Cara menggunakan Amazon FSx for Lustre

Metrik yang dilaporkan oleh Amazon FSx for Lustre memberikan informasi yang dapat Anda analisis dengan cara yang berbeda-beda. Daftar berikut menunjukkan beberapa kegunaan umum untuk metrik. Ini adalah saran agar Anda dapat mulai, bukan daftar komprehensif.

Bagaimana saya menentukan...	Metrik yang Relevan (Dimensi Metrik)
Throughput sistem file saya?	$SUM (DataReadBytes + DataWriteBytes) / Periode$ (dalam detik)
IOPS sistem file saya?	Total IOPS = $SUM (DataReadOperations + DataWriteOperations + MetadataOperations) / Periode$ (dalam detik)
Rasio kompresi data sistem file saya?	$SUM (LogicalDiskPenggunaan) / SUM (PhysicalDiskPenggunaan)$
Jika pembaruan ke sistem file saya telah disinkronkan dengan bucket S3 saya?	AutoExport AgeOfOldestQueuedMessage
Jika pembaruan ke bucket S3 saya telah disinkronkan dengan sistem file saya?	AutoImport AgeOfOldestQueuedMessage

Matematika metrik: Rasio kompresi data

Menggunakan matematika metrik, Anda dapat menanyakan beberapa CloudWatch metrik dan menggunakan ekspresi matematika untuk membuat deret waktu baru berdasarkan metrik ini. Anda dapat memvisualisasikan deret waktu yang dihasilkan di CloudWatch konsol dan menambahkannya ke dasbor. Untuk informasi selengkapnya tentang matematika [metrik](#), lihat [Menggunakan matematika metrik](#) di Panduan CloudWatch Pengguna Amazon.

Ekspresi matematika metrik ini menghitung rasio kompresi data sistem file Amazon FSx for Lustre Anda. Untuk menghitung rasio ini, pertama dapatkan jumlah statistik dari total penggunaan disk logis (tanpa kompresi), yang disediakan oleh metrik LogicalDiskUsage. Kemudian bagi itu dengan jumlah statistik total penggunaan disk fisik (dengan kompresi), yang disediakan oleh metrik PhysicalDiskUsage.

Jadi jika logika Anda adalah ini: jumlah LogicalDiskUsage ÷ jumlah PhysicalDiskUsage

Maka informasi CloudWatch metrik Anda adalah sebagai berikut.

ID	Metrik yang dapat digunakan	Statistik	Periode
m1	LogicalDiskUsage	Jumlah	1 menit
m2	PhysicalDiskUsage	Jumlah	1 menit

ID dan ekspresi matematika metrik Anda adalah sebagai berikut.

ID	Ekspresi
e1	m1/m2

e1 adalah rasio kompresi data.

Mengakses metrik CloudWatch

Anda dapat melihat metrik Amazon FSx for Lustre CloudWatch dalam banyak hal. Anda dapat melihatnya melalui CloudWatch konsol, atau Anda dapat mengaksesnya menggunakan CloudWatch CLI atau API. CloudWatch Prosedur berikut menunjukkan cara mengakses metrik menggunakan berbagai alat.

Untuk melihat metrik menggunakan konsol CloudWatch

1. Buka [konsol CloudWatch](#).
2. Di panel navigasi, pilih Metrik.
3. Pilih namespace FSx.
4. (Opsional) Untuk melihat metrik, ketik namanya di kolom pencarian.
5. (Opsional) Untuk memfilter berdasarkan dimensi, pilih FileSystemId.

Untuk mengakses metrik dari AWS CLI

- Gunakan perintah [list-metrics](#) dengan perintah namespace `--namespace "AWS/FSx"`. Untuk informasi selengkapnya, lihat [Referensi Perintah AWS CLI](#).

Untuk mengakses metrik dari API CloudWatch

- Panggil [GetMetricStatistics](#). Untuk informasi selengkapnya, lihat [Referensi Amazon CloudWatch API](#).

Membuat CloudWatch alarm untuk memantau Amazon FSx for Lustre

Anda dapat membuat CloudWatch alarm yang mengirimkan pesan Amazon SNS saat alarm berubah status. Alarm mengawasi satu metrik selama jangka waktu yang Anda tentukan, dan melakukan satu atau beberapa tindakan berdasarkan nilai metrik relatif terhadap ambang batas tertentu selama jangka waktu tertentu. Tindakan ini adalah notifikasi yang dikirim ke topik Amazon SNS atau kebijakan Penskalaan Otomatis.

Alarm memanggil tindakan untuk perubahan status berkelanjutan saja. CloudWatch alarm tidak memanggil tindakan hanya karena mereka berada dalam keadaan tertentu; negara harus telah berubah dan dipertahankan untuk sejumlah periode tertentu.

Prosedur berikut menunjukkan cara membuat alarm untuk Amazon FSx for Lustre.

Untuk mengatur alarm menggunakan konsol CloudWatch

1. Masuk ke AWS Management Console dan buka CloudWatch konsol di <https://console.aws.amazon.com/cloudwatch/>.
2. Pilih Buat Alarm. Melakukan ini akan meluncurkan Buat Wizard Alarm.
3. Pilih Metrik FSx dan gulir menggunakan metrik Amazon FSx for Lustre untuk menemukan metrik yang ingin Anda aktifkan alarm-nya. Untuk menampilkan metrik Amazon FSx for Lustre di kotak dialog ini, cari di ID sistem file dari sistem file Anda. Pilih metrik untuk membuat sebuah alarm aktif lalu pilih Selanjutnya.
4. Di bagian Kondisi, pilih kondisi yang Anda inginkan untuk alarm, dan pilih Selanjutnya.

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

5. Jika Anda ingin CloudWatch mengirimkan Anda email ketika status alarm tercapai, untuk Setiap kali alarm ini, pilih Status adalah ALARM. Untuk Mengirim notifikasi ke, pilih topik SNS yang sudah ada. Jika memilih Buat topik, Anda dapat mengatur nama dan alamat email untuk daftar langganan email baru. Daftar ini disimpan dan muncul di kotak ini untuk alarm selanjutnya.

Note

Jika Anda menggunakan Buat topik untuk membuat topik Amazon SNS baru, verifikasi alamat email sebelum menerima notifikasi. Email hanya dikirim saat alarm memasuki keadaan alarm. Jika perubahan keadaan alarm ini terjadi sebelum alamat email diverifikasi, alamat tidak akan menerima pemberitahuan.

6. Lakukan pratinjau alarm yang akan Anda buat di area Pratinjau Alarm. Jika muncul seperti yang diharapkan, pilih Buat Alarm.

Untuk mengatur alarm menggunakan AWS CLI

- Panggil [put-metric-alarm](#). Untuk informasi selengkapnya, lihat [Referensi Perintah AWS CLI](#).

Untuk menyetel alarm menggunakan CloudWatch API

- Panggil [PutMetricAlarm](#). Untuk informasi selengkapnya, lihat [Referensi Amazon CloudWatch API](#).

Logging dengan Amazon CloudWatch Logs

FSx for Lustre mendukung pencatatan kesalahan dan peristiwa peringatan untuk repositori data yang terkait dengan sistem file Anda ke Amazon Logs. CloudWatch

Note

Logging dengan Amazon CloudWatch Logs hanya tersedia di Amazon FSx for Lustre sistem file yang dibuat setelah jam 3 sore PST pada 30 November 2021.

Topik

- [Ikhtisar pencatatan](#)
- [Log tujuan](#)
- [Mengelola logging](#)
- [Melihat log](#)

Ikhtisar pencatatan

Jika Anda memiliki repositori data yang ditautkan ke sistem file FSx for Lustre, Anda dapat mengaktifkan pencatatan peristiwa repositori data ke Amazon Logs. CloudWatch Kesalahan dan peristiwa peringatan dapat dicatat dari operasi repositori data berikut:

- Ekspor otomatis
- Tugas repositori data

Untuk informasi lebih lanjut tentang operasi ini dan tentang menautkan ke repositori data, lihat.

[Menggunakan repositori data dengan Amazon FSx for Lustre](#)

Anda dapat mengonfigurasi level log yang dicatat Amazon FSx; yaitu, apakah Amazon FSx hanya akan mencatat peristiwa kesalahan, hanya peristiwa peringatan, atau peristiwa kesalahan dan peringatan. Anda juga dapat menonaktifkan log acara kapan saja.

Note

Kami sangat menyarankan Anda mengaktifkan log untuk sistem file yang memiliki tingkat fungsionalitas kritis apa pun yang terkait dengannya.

Log tujuan

Saat logging diaktifkan, FSx for Lustre harus dikonfigurasi dengan tujuan Amazon Logs. CloudWatch Tujuan log peristiwa adalah grup CloudWatch log Amazon Logs, dan Amazon FSx membuat aliran log untuk sistem file Anda dalam grup log ini. CloudWatch Log memungkinkan Anda menyimpan, melihat, dan mencari log peristiwa audit di CloudWatch konsol Amazon, menjalankan kueri di CloudWatch log menggunakan Wawasan Log, dan memicu CloudWatch alarm atau fungsi Lambda.

Anda memilih tujuan log saat Anda membuat sistem file FSx for Lustre atau sesudahnya dengan memperbaruinya. Untuk informasi selengkapnya, lihat [Mengelola logging](#).

Secara default, Amazon FSx akan membuat dan menggunakan grup CloudWatch log Log default di akun Anda sebagai tujuan log peristiwa. Jika Anda ingin menggunakan grup CloudWatch log Log kustom sebagai tujuan log peristiwa, berikut adalah persyaratan untuk nama dan lokasi tujuan log peristiwa:

- Nama grup CloudWatch log Log harus dimulai dengan `/aws/fsx/` awalan.
- Jika Anda tidak memiliki grup CloudWatch log Log saat membuat atau memperbarui sistem file di konsol, Amazon FSx for Lustre dapat membuat dan menggunakan aliran CloudWatch log default di grup log Log. `/aws/fsx/lustre` Aliran log akan dibuat dengan format `datarepo_file_system_id` (misalnya, `datarepo_fs-0123456789abcdef0`).
- Jika Anda tidak ingin menggunakan grup log default, UI konfigurasi memungkinkan Anda membuat grup CloudWatch log Log saat membuat atau memperbarui sistem file di konsol.
- Grup CloudWatch log Log tujuan harus berada di AWS partisi yang sama Wilayah AWS, dan Akun AWS sebagai sistem file Amazon FSx for Lustre Anda.

Anda dapat mengubah tujuan log peristiwa kapan saja. Ketika Anda melakukannya, log peristiwa baru dikirim hanya ke tujuan baru.

Mengelola logging

Anda dapat mengaktifkan logging ketika Anda membuat sistem file FSx for Lustre baru atau sesudahnya dengan memperbaruinya. Pencatatan diaktifkan secara default saat Anda membuat sistem file dari konsol Amazon FSx. Namun, logging dimatikan secara default saat Anda membuat sistem file dengan AWS CLI atau Amazon FSx API.

Pada sistem file yang ada yang mengaktifkan logging, Anda dapat mengubah pengaturan pencatatan peristiwa, termasuk tingkat log untuk mencatat peristiwa, dan tujuan log. Anda dapat melakukan tugas-tugas ini menggunakan konsol Amazon FSx, AWS CLI, atau Amazon FSx API.

Untuk mengaktifkan logging saat membuat sistem file (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Ikuti prosedur untuk membuat sistem file baru yang dijelaskan di [Buat sistem file FSx for Lustre Anda](#) pada bagian Mulai.
3. Buka bagian Logging - opsional. Logging diaktifkan secara default.

▼ Logging - optional

Log data repository events [Info](#)
 You can log error and warning events for data repository import/export activity associated with your file system to CloudWatch Logs.

Log errors
 Log warnings

Choose a CloudWatch Logs destination

[Create new](#)

Pricing
 Standard Amazon CloudWatch Logs pricing applies based on your usage. [Learn more](#)

4. Lanjutkan dengan bagian berikutnya dari wizard pembuatan sistem file.

Ketika sistem file menjadi Tersedia, logging akan diaktifkan.

Untuk mengaktifkan logging saat membuat sistem file (CLI)

1. Saat membuat sistem file baru, gunakan `LogConfiguration` properti dengan operasi [CreateFileSistem](#) untuk mengaktifkan logging untuk sistem file baru.

```
create-file-system --file-system-type LUSTRE \
  --storage-capacity 1200 --subnet-id subnet-08b31917a72b548a9 \
  --lustre-configuration "LogConfiguration={Level=WARN_ERROR, \
    Destination="arn:aws:logs:us-east-1:234567890123:log-group:/aws/fsx/
testEventLogging"}"
```

2. Ketika sistem file menjadi Tersedia, fitur logging akan diaktifkan.

Untuk mengubah konfigurasi logging (konsol)

1. Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
2. Arahkan ke sistem File, dan pilih sistem file Lustre yang ingin Anda kelola untuk pencatatan.
3. Pilih tab Pemantauan.
4. Pada panel Logging, pilih Update.
5. Pada dialog Perbarui konfigurasi logging, ubah pengaturan yang diinginkan.
 - a. Pilih Kesalahan log untuk mencatat peristiwa kesalahan saja, atau Log peringatan untuk mencatat peristiwa peringatan saja, atau keduanya. Logging dinonaktifkan jika Anda tidak membuat pilihan.
 - b. Pilih tujuan CloudWatch log Log yang ada atau buat yang baru.
6. Pilih Simpan.

Untuk mengubah konfigurasi logging (CLI)

- Gunakan perintah CLI [update-file-system](#) atau operasi API [UpdateFileSystem](#) yang setara.

```
update-file-system --file-system-id fs-0123456789abcdef0 \  
  --lustre-configuration "LogConfiguration={Level=WARN_ERROR, \  
    Destination="arn:aws:logs:us-east-1:234567890123:log-group:/aws/fsx/  
testEventLogging"}"
```

Melihat log

Anda dapat melihat log setelah Amazon FSx mulai memancarkannya. Anda dapat melihat log sebagai berikut:

- Anda dapat melihat log dengan membuka CloudWatch konsol Amazon dan memilih grup log dan aliran log tempat log peristiwa Anda dikirim. Untuk informasi selengkapnya, lihat [Melihat data log yang dikirim ke CloudWatch Log](#) di Panduan Pengguna CloudWatch Log Amazon.
- Anda dapat menggunakan Wawasan CloudWatch Log untuk mencari dan menganalisis data log secara interaktif. Untuk informasi selengkapnya, lihat [Menganalisis data CloudWatch log dengan Wawasan Log](#), di Panduan Pengguna CloudWatch Log Amazon.

- Anda juga dapat mengekspor log ke Amazon S3. Untuk informasi selengkapnya, lihat [Mengekspor data log ke Amazon S3](#), di Panduan Pengguna CloudWatch Amazon Logs.

Untuk mempelajari tentang alasan kegagalan, lihat [Log peristiwa repositori data](#).

Logging FSx untuk panggilan API Lustre dengan AWS CloudTrail

Amazon FSx for Lustre AWS CloudTrail terintegrasi dengan, layanan yang menyediakan catatan tindakan yang diambil oleh pengguna, peran, AWS atau layanan di Amazon FSx for Lustre. CloudTrail menangkap semua panggilan API untuk Amazon FSx for Lustre sebagai peristiwa. Panggilan yang tertangkap meliputi panggilan dari konsol Amazon FSx for Lustre dan dari panggilan kode ke operasi API Amazon FSx for Lustre.

Jika Anda membuat jejak, Anda dapat mengaktifkan pengiriman CloudTrail acara secara terus menerus ke bucket Amazon S3, termasuk acara untuk Amazon FSx for Lustre. 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 for Lustre. 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](#).

Informasi Amazon FSx for Lustre di CloudTrail

CloudTrail diaktifkan di AWS akun Anda saat Anda membuat akun. Saat aktivitas API terjadi di Amazon FSx for Lustre, aktivitas tersebut direkam CloudTrail dalam suatu peristiwa bersama AWS dengan peristiwa layanan lainnya dalam riwayat Peristiwa. Anda dapat melihat, mencari, dan mengunduh acara terbaru di AWS akun Anda. Untuk informasi selengkapnya, lihat [Melihat Acara dengan Riwayat CloudTrail Acara](#).

Untuk catatan peristiwa yang sedang berlangsung di AWS akun Anda, termasuk acara untuk Amazon FSx for Lustre, 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 :

- [Gambaran Umum untuk Membuat Jejak](#)
- [CloudTrail Layanan dan Integrasi yang Didukung](#)
- [Mengonfigurasi Notifikasi Amazon SNS untuk CloudTrail](#)
- [Menerima File CloudTrail Log dari Beberapa Wilayah](#) dan [Menerima File CloudTrail Log dari Beberapa Akun](#)

Semua panggilan Amazon FSx [for Lustre](#) 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 terfederasi.
- Apakah permintaan itu dibuat oleh AWS layanan lain.

Untuk informasi selengkapnya, lihat [Elemen CloudTrail UserIdentity](#) di AWS CloudTrail Panduan Pengguna.

Memahami entri file berkas log Amazon FSx for Lustre

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

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan `TagResource` operasi ketika tag untuk sistem file dibuat dari konsol.

```
{
```

```

"eventVersion": "1.05",
"userIdentity": {
  "type": "Root",
  "principalId": "111122223333",
  "arn": "arn:aws:sts::111122223333:root",
  "accountId": "111122223333",
  "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
  "sessionContext": {
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "2018-11-14T22:36:07Z"
    }
  }
},
"eventTime": "2018-11-14T22:36:07Z",
"eventSource": "fsx.amazonaws.com",
"eventName": "TagResource",
"awsRegion": "us-east-1",
"sourceIPAddress": "192.0.2.0",
"userAgent": "console.amazonaws.com",
"requestParameters": {
  "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
},
"responseElements": null,
"requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
"eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
"eventType": "AwsApiCall",
"apiVersion": "2018-03-01",
"recipientAccountId": "111122223333"
}

```

Contoh berikut menunjukkan entri CloudTrail log yang menunjukkan UntagResource tindakan ketika tag untuk sistem file dihapus dari konsol.

```

{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:sts::111122223333:root",

```

```
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-14T23:40:54Z"
      }
    }
  },
  "eventTime": "2018-11-14T23:40:54Z",
  "eventSource": "fsx.amazonaws.com",
  "eventName": "UntagResource",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
  },
  "responseElements": null,
  "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
  "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
  "eventType": "AwsApiCall",
  "apiVersion": "2018-03-01",
  "recipientAccountId": "111122223333"
}
```

Keamanan di FSx for Lustre

Keamanan cloud di AWS adalah prioritas tertinggi. Sebagai AWS pelanggan, Anda mendapat manfaat dari pusat data dan arsitektur jaringan yang dibangun untuk memenuhi persyaratan organisasi yang paling sensitif terhadap keamanan.

Keamanan adalah tanggung jawab bersama antara Anda AWS dan Anda. [Model tanggung jawab bersama](#) menjelaskan hal ini sebagai keamanan cloud dan keamanan dalam cloud:

- Keamanan cloud — AWS bertanggung jawab untuk melindungi infrastruktur yang menjalankan AWS layanan di Amazon Web Services Cloud. AWS juga memberi Anda layanan yang dapat Anda gunakan dengan aman. Auditor pihak ketiga secara teratur menguji dan memverifikasi keefektifan keamanan kami sebagai bagian dari [program kepatuhan AWS](#). Untuk mempelajari tentang program kepatuhan yang berlaku di Amazon FSx for Lustre, lihat [Layanan AWS di Ruang Lingkup melalui 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 for Lustre. Topik berikut menunjukkan cara mengonfigurasi Amazon FSx untuk memenuhi tujuan keamanan dan kepatuhan Anda. Anda juga belajar cara menggunakan layanan Amazon lainnya yang dapat membantu Anda memantau dan mengamankan sumber daya Amazon FSx for Lustre Anda.

Setelah itu, Anda dapat menemukan penjelasan pertimbangan keamanan untuk bekerja dengan Amazon FSx.

Topik

- [Perlindungan data di Amazon FSx for Lustre](#)
- [Manajemen identitas dan akses untuk Amazon FSx for Lustre](#)
- [Kontrol akses sistem file dengan Amazon VPC](#)
- [ACL jaringan VPC Amazon](#)
- [Validasi Kepatuhan untuk Amazon FSx for Lustre](#)
- [Amazon FSx for Lustre dan titik akhir VPC antarmuka \(AWS PrivateLink\)](#)

Perlindungan data di Amazon FSx for Lustre

[Model tanggung jawab AWS bersama model](#) berlaku untuk perlindungan data di Amazon FSx for Lustre. 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 sumber daya. AWS Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3.
- Siapkan API dan pencatatan aktivitas pengguna dengan AWS CloudTrail.
- Gunakan solusi AWS enkripsi, bersama dengan semua kontrol keamanan default di dalamnya Layanan AWS.
- Gunakan layanan keamanan terkelola lanjut seperti Amazon Macie, yang membantu menemukan dan mengamankan data sensitif yang disimpan di Amazon S3.
- Jika Anda memerlukan modul kriptografi tervalidasi FIPS 140-2 saat mengakses AWS melalui antarmuka baris perintah atau API, gunakan titik akhir FIPS. Lihat informasi yang lebih lengkap tentang titik akhir FIPS yang tersedia di [Standar Pemrosesan Informasi Federal \(FIPS\) 140-2](#).

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 SDK. Data apa pun yang Anda masukkan ke dalam tanda atau bidang isian bebas yang digunakan untuk nama dapat digunakan untuk log penagihan atau log diagnostik. Saat Anda memberikan URL ke server eksternal, kami sangat menganjurkan

supaya Anda tidak menyertakan informasi kredensial di dalam URL untuk memvalidasi permintaan Anda ke server itu.

Topik

- [Enkripsi data di Amazon FSx for Lustre](#)
- [Privasi lalu lintas antar jaringan](#)

Enkripsi data di Amazon FSx for Lustre

Amazon FSx for Lustre mensupport dua bentuk enkripsi untuk sistem file, enkripsi data at rest dan enkripsi saat transit. Enkripsi data at rest secara otomatis akan diaktifkan saat membuat sistem file Amazon FSx. Enkripsi data dalam transit secara otomatis diaktifkan saat Anda mengakses sistem file Amazon FSx dari [Instans Amazon EC2](#) yang mendukung fitur ini.

Kapan menggunakan enkripsi

Jika organisasi Anda tunduk pada kebijakan atau peraturan perusahaan yang memerlukan enkripsi data dan metadata saat istirahat, kami rekomendasikan sebaiknya buat sistem file terenkripsi dan pasang sistem file Anda menggunakan enkripsi data saat transit.

Untuk informasi selengkapnya tentang membuat sistem file yang dienkripsi saat istirahat menggunakan konsol, lihat [Membuat sistem file Amazon FSx for Lustre](#).

Topik

- [Mengenkripsi data saat istirahat](#)
- [Mengenkripsi data dalam perjalanan](#)

Mengenkripsi data saat istirahat

Enkripsi data saat istirahat diaktifkan secara otomatis saat Anda membuat sistem file Amazon FSx for Lustre melalui AWS CLI,, atau secara terprogram AWS Management Console melalui Amazon FSx API atau salah satu SDK. AWS Organisasi Anda mungkin memerlukan enkripsi semua data yang sesuai dengan klasifikasi tertentu atau yang diasosiasikan dengan aplikasi, beban kerja, atau lingkungan tertentu. Jika Anda membuat sistem file persisten, Anda dapat menentukan AWS KMS kunci untuk mengenkripsi data. Jika Anda membuat sistem file scratch, data tersebut dienkripsi menggunakan kunci yang dikelola oleh Amazon FSx. Untuk informasi selengkapnya

tentang membuat sistem file yang dienkripsi saat istirahat menggunakan konsol, lihat [Membuat sistem file Amazon FSx for Lustre](#).

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.

Untuk informasi lebih lanjut tentang bagaimana FSx for AWS KMS Lustre menggunakan, lihat [Bagaimana Amazon FSx for Lustre menggunakan AWS KMS](#)

Cara kerja enkripsi saat istirahat

Dalam sistem file yang dienkripsi, data dan metadata dienkripsi secara otomatis sebelum ditulis ke sistem file. Demikian pula, ketika data dan metadata terbaca, mereka secara otomatis didekripsi sebelum ditampilkan ke aplikasi. Proses ini ditangani secara transparan oleh Amazon FSx for Lustre, sehingga Anda tidak perlu memodifikasi aplikasi Anda.

Amazon FSx for Lustre menggunakan enkripsi algoritme standar industri AES-256 untuk mengenkripsi sistem file data at rest. Untuk informasi selengkapnya, lihat [Dasar-dasar Kriptografi](#) di Panduan Developer AWS Key Management Service .

Bagaimana Amazon FSx for Lustre menggunakan AWS KMS

Amazon FSx for Lustre mengenkripsi data secara otomatis sebelum ditulis ke sistem file, dan secara otomatis mendekripsi data saat dibaca. Data dienkripsi menggunakan cipher blok XTS-AES-256. Semua sistem file FSx for Lustre scratch dienkripsi saat istirahat dengan kunci yang dikelola oleh AWS KMS Amazon FSx for Lustre AWS KMS terintegrasi dengan manajemen kunci. Kunci yang digunakan untuk mengenkripsi sistem file scratch saat istirahat unik per sistem file nya, dan akan hancur setelah sistem file dihapus. Untuk sistem file persisten, Anda memilih kunci KMS yang digunakan untuk mengenkripsi dan mendekripsi data. Anda menentukan kunci mana yang akan digunakan saat Anda membuat sistem file tetap. Anda dapat mengaktifkan, menonaktifkan, atau mencabut hibah pada kunci KMS ini. Kunci KMS ini dapat menjadi salah satu dari dua jenis berikut:

- Kunci yang dikelola AWS untuk Amazon FSx - Ini adalah kunci KMS default. Anda tidak dikenakan biaya untuk membuat dan menyimpan kunci KMS, tetapi ada biaya penggunaan. Untuk informasi selengkapnya, lihat [harga AWS Key Management Service](#).

- Kunci terkelola pelanggan - Ini adalah kunci KMS yang paling fleksibel untuk digunakan, karena Anda dapat mengonfigurasi kebijakan dan hibah utamanya untuk beberapa pengguna atau layanan. Untuk informasi selengkapnya tentang membuat kunci terkelola pelanggan, lihat [Membuat kunci](#) di Panduan AWS Key Management Service Pengembang.

Jika Anda menggunakan kunci yang dikelola pelanggan sebagai kunci KMS Anda untuk enkripsi dan dekripsi data file, Anda dapat mengaktifkan rotasi kunci. Ketika Anda mengaktifkan rotasi kunci, AWS KMS secara otomatis memutar kunci Anda sekali per tahun. Selain itu, dengan kunci yang dikelola pelanggan, Anda dapat memilih kapan harus menonaktifkan, mengaktifkan kembali, menghapus, atau mencabut akses ke kunci yang dikelola pelanggan kapan saja.

 Important

Amazon FSx hanya menerima kunci KMS enkripsi simetris. Anda tidak dapat menggunakan kunci KMS asimetris dengan Amazon FSx.

Kebijakan utama Amazon FSx 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 terkait AWS KMS yang didukung oleh Amazon FSx untuk sistem file at rest terenkripsi:

- kms:Encrypt – (Opsional) Mengenkripsi plaintext ke ciphertext. Izin ini termasuk dalam kebijakan kunci default.
- kms:Decrypt – (Wajib) Mendekripsi ciphertext. Ciphertext adalah plaintext yang telah dienkripsi sebelumnya. Izin ini termasuk dalam kebijakan kunci default.
- kms: ReEncrypt — (Opsional) Mengenkripsi data di sisi server dengan kunci KMS baru, tanpa mengekspos plaintext data di sisi klien. Data pertama kali didekripsi dan kemudian dienkripsi ulang. Izin ini termasuk dalam kebijakan kunci default.
- kms: GenerateData KeyWithout Plaintext — (Diperlukan) Mengembalikan kunci enkripsi data yang dienkripsi di bawah kunci KMS. Izin ini disertakan dalam kebijakan kunci default di bawah kms: GenerateData Key*.
- kms: CreateGrant — (Diperlukan) Menambahkan hibah ke kunci untuk menentukan siapa yang dapat menggunakan kunci dan dalam kondisi apa. Hibah adalah mekanisme izin lainnya untuk kebijakan kunci. Untuk informasi selengkapnya tentang hibah, lihat [Menggunakan hibah](#) di

Panduan AWS Key Management Service Pengembang. Izin ini termasuk dalam kebijakan kunci default.

- kms: DescribeKey - (Diperlukan) Memberikan informasi rinci tentang kunci KMS yang ditentukan. Izin ini termasuk dalam kebijakan kunci default.
- kms: ListAliases — (Opsional) Daftar semua alias kunci di akun. Saat Anda menggunakan konsol untuk membuat sistem file terenkripsi, izin ini mengisi daftar untuk memilih 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

Scratch 2 dan sistem file persisten dapat secara otomatis mengenkripsi data dalam perjalanan. Dalam tabel berikut, jika ada tanda centang di sel untuk jenis penyebaran itu dan Wilayah AWS, maka data dienkripsi saat transit ketika sistem file diakses dari instans Amazon EC2 yang mendukung enkripsi dalam perjalanan dan juga untuk semua komunikasi antar host dalam sistem file. Untuk mempelajari instans EC2 mana yang mendukung enkripsi saat transit, lihat [Enkripsi saat transit di Panduan Pengguna Amazon EC2](#).

Enkripsi data dalam transit untuk scratch 2 dan sistem file persisten tersedia di berikut Wilayah AWS ini.

Wilayah AWS	Scratch_2	Persistent_1	Persistent_2
AS Timur (Ohio)	✓	✓	✓
AS Timur (Virginia Utara)	✓	✓	✓
Zona Lokal AS Timur (Atlanta) *			✓
AS Barat (Oregon)	✓	✓	✓
AS Barat (California N.) *	✓	✓	
Zona Lokal AS Barat (Los Angeles)	✓	✓	
AWS GovCloud (AS-Timur) *	✓	✓	
AWS GovCloud (AS-Barat)	✓	✓	

Wilayah AWS	Scratch_2	Persistent_1	Persistent_2
Kanada (Tengah) *	✓	✓	✓
Kanada Barat (Calgary) *			✓
Eropa (Irlandia)	✓	✓	✓
Eropa (Milan)	✓	✓	
Eropa (Frankfurt)	✓	✓	✓
Eropa (Paris)	✓	✓	
Eropa (London)	✓	✓	✓
Eropa (Stockholm) *	✓	✓	✓
Asia Pasifik (Seoul)	✓	✓	✓
Asia Pasifik (Singapura)	✓	✓	✓
Asia Pasifik (Tokyo) *	✓	✓	✓
Asia Pasifik (Mumbai) *	✓	✓	✓
Asia Pasifik (Hong Kong) *	✓	✓	✓
Asia Pasifik (Sydney) *	✓	✓	✓
Israel (Tel Aviv) *	✓		✓
Amerika Selatan (São Paulo) *	✓	✓	

 Note

* Enkripsi data dalam transit tersedia untuk sistem file yang dibuat setelah 11 April 2021.

Privasi lalu lintas antar jaringan

Topik ini menjelaskan cara Amazon FSx mengamankan koneksi dari layanan ke lokasi lain.

Lalu lintas antara Amazon FSx dan klien lokal

Anda memiliki dua opsi konektivitas antara jaringan pribadi Anda dan AWS:

- AWS Site-to-Site VPN Koneksi. Untuk informasi lebih lanjut, lihat [Apa itu AWS Site-to-Site VPN?](#)
- AWS Direct Connect Koneksi. Untuk informasi lebih lanjut, lihat [Apa itu AWS Direct Connect?](#)

Anda dapat mengakses FSx for Lustre melalui jaringan untuk mencapai operasi API yang diterbitkan AWS untuk melakukan tugas administratif dan port Lustre untuk berinteraksi dengan sistem file.

Mengenkripsi lalu lintas API

Untuk mengakses operasi API AWS yang diterbitkan, klien harus mendukung Transport Layer Security (TLS) 1.2 atau yang lebih baru. Kami mensyaratkan TLS 1.2 dan menganjurkan TLS 1.3. Klien juga harus mendukung suite cipher dengan perfect forward secrecy (PFS) seperti Ephemeral Diffie-Hellman (DHE) atau Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Sebagian besar sistem modern seperti Java 7 dan versi lebih baru mendukung mode-mode ini. Selain itu, permintaan harus ditandatangani menggunakan ID kunci akses dan kunci akses rahasia yang terkait dengan prinsipal IAM. Atau Anda dapat menggunakan [AWS Security Token Service \(STS\)](#) untuk menghasilkan kredensial keamanan sementara untuk menandatangani permintaan.

Mengenkripsi lalu lintas data

Enkripsi data dalam perjalanan diaktifkan dari instans EC2 yang didukung yang mengakses sistem file dari dalam. AWS Cloud Untuk informasi selengkapnya, lihat [Mengenkripsi data dalam perjalanan](#). FSx for Lustre tidak secara native menawarkan enkripsi dalam perjalanan antara klien on-premise dan sistem file.

Manajemen identitas dan akses untuk Amazon FSx for Lustre

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 for Lustre bekerja dengan IAM](#)
- [Contoh kebijakan berbasis identitas untuk Amazon FSx for Lustre](#)
- [AWS kebijakan terkelola untuk Amazon FSx](#)
- [Memecahkan masalah identitas dan akses Amazon FSx for Lustre](#)
- [Menggunakan tanda dengan Amazon FSx](#)
- [Menggunakan peran terkait layanan untuk Amazon FSx](#)

Audiens

Cara Anda menggunakan AWS Identity and Access Management (IAM) berbeda, tergantung pada pekerjaan yang Anda lakukan di Amazon FSx.

Pengguna layanan - Jika Anda menggunakan layanan Amazon FSx untuk melakukan pekerjaan Anda, administrator Anda memberi Anda kredensi dan izin yang Anda butuhkan. Saat Anda menggunakan lebih banyak fitur Amazon FSx untuk melakukan pekerjaan Anda, Anda mungkin memerlukan izin tambahan. Memahami cara akses dikelola dapat membantu Anda meminta izin yang tepat dari administrator Anda. Jika Anda tidak dapat mengakses fitur di Amazon FSx, lihat. [Memecahkan masalah identitas dan akses Amazon FSx for Lustre](#)

Administrator layanan - Jika Anda bertanggung jawab atas sumber daya Amazon FSx di perusahaan Anda, Anda mungkin memiliki akses penuh ke Amazon FSx. Tugas Anda adalah menentukan fitur dan sumber daya Amazon FSx mana yang harus diakses pengguna layanan Anda. Kemudian, Anda harus mengirimkan permintaan kepada administrator IAM untuk mengubah izin pengguna layanan Anda. Tinjau informasi di halaman ini untuk memahami konsep Basic IAM. Untuk mempelajari lebih lanjut tentang bagaimana perusahaan Anda dapat menggunakan IAM dengan Amazon FSx, lihat. [Bagaimana Amazon FSx for Lustre bekerja dengan IAM](#)

Administrator IAM - Jika Anda administrator IAM, Anda mungkin ingin mempelajari detail tentang cara menulis kebijakan untuk mengelola akses ke Amazon FSx. Untuk melihat contoh kebijakan berbasis identitas Amazon FSx yang dapat Anda gunakan di IAM, lihat. [Contoh kebijakan berbasis identitas untuk Amazon FSx for Lustre](#)

Mengautentikasi dengan identitas

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

Anda dapat masuk AWS sebagai identitas federasi dengan menggunakan kredensi yang disediakan melalui sumber identitas. AWS IAM Identity Center Pengguna (IAM Identity Center), autentikasi masuk tunggal perusahaan Anda, dan kredensi Google atau Facebook Anda adalah contoh identitas federasi. Saat Anda masuk sebagai identitas terfederasi, administrator Anda sebelumnya menyiapkan federasi identitas menggunakan peran IAM. Ketika Anda mengakses AWS dengan menggunakan federasi, Anda secara tidak langsung mengambil peran.

Bergantung pada jenis pengguna Anda, Anda dapat masuk ke AWS Management Console atau portal AWS akses. Untuk informasi selengkapnya tentang masuk AWS, lihat [Cara masuk ke Panduan AWS Sign-In Pengguna Anda Akun AWS](#).

Jika Anda mengakses AWS secara terprogram, AWS sediakan kit pengembangan perangkat lunak (SDK) dan antarmuka baris perintah (CLI) untuk menandatangani permintaan Anda secara kriptografis dengan menggunakan kredensial Anda. Jika Anda tidak menggunakan AWS alat, Anda harus menandatangani permintaan sendiri. Untuk informasi selengkapnya tentang penggunaan metode yang disarankan untuk menandatangani permintaan sendiri, lihat [Menandatangani permintaan AWS API](#) di Panduan Pengguna IAM.

Apa pun metode autentikasi yang digunakan, Anda mungkin diminta untuk menyediakan informasi keamanan tambahan. Misalnya, AWS merekomendasikan agar Anda menggunakan otentikasi multi-faktor (MFA) untuk meningkatkan keamanan akun Anda. Untuk mempelajari selengkapnya, lihat [Autentikasi multi-faktor](#) dalam Panduan Pengguna AWS IAM Identity Center dan [Menggunakan autentikasi multi-faktor \(MFA\) dalam AWS](#) dalam Panduan Pengguna IAM.

Akun AWS pengguna root

Saat Anda membuat Akun AWS, Anda mulai dengan satu identitas masuk yang memiliki akses lengkap ke semua Layanan AWS dan sumber daya di akun. Identitas ini disebut pengguna Akun AWS root dan diakses dengan masuk dengan alamat email dan kata sandi yang Anda gunakan untuk membuat akun. Kami sangat menyarankan agar Anda tidak menggunakan pengguna root untuk tugas sehari-hari. Lindungi kredensial pengguna root Anda dan gunakan kredensial tersebut untuk melakukan tugas yang hanya dapat dilakukan pengguna root. Untuk daftar lengkap tugas

yang mengharuskan Anda masuk sebagai pengguna root, lihat [Tugas yang memerlukan kredensial pengguna root](#) dalam Panduan Pengguna IAM.

Identitas gabungan

Sebagai praktik terbaik, mewajibkan pengguna manusia, termasuk pengguna yang memerlukan akses administrator, untuk menggunakan federasi dengan penyedia identitas untuk mengakses Layanan AWS dengan menggunakan kredensi sementara.

Identitas federasi adalah pengguna dari direktori pengguna perusahaan Anda, penyedia identitas web, direktori Pusat Identitas AWS Directory Service, atau pengguna mana pun yang mengakses Layanan AWS dengan menggunakan kredensial yang disediakan melalui sumber identitas. Ketika identitas federasi mengakses Akun AWS, mereka mengambil peran, dan peran memberikan kredensi sementara.

Untuk manajemen akses terpusat, kami sarankan Anda menggunakan AWS IAM Identity Center. Anda dapat membuat pengguna dan grup di Pusat Identitas IAM, atau Anda dapat menghubungkan dan menyinkronkan ke sekumpulan pengguna dan grup di sumber identitas Anda sendiri untuk digunakan di semua aplikasi Akun AWS dan aplikasi Anda. Untuk informasi tentang Pusat Identitas IAM, lihat [Apakah itu Pusat Identitas IAM?](#) dalam Panduan Pengguna AWS IAM Identity Center .

Pengguna dan grup IAM

[Pengguna IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus untuk satu orang atau aplikasi. Jika memungkinkan, kami merekomendasikan untuk mengandalkan kredensial sementara, bukan membuat pengguna IAM yang memiliki kredensial jangka panjang seperti kata sandi dan kunci akses. Namun, jika Anda memiliki kasus penggunaan tertentu yang memerlukan kredensial jangka panjang dengan pengguna IAM, kami merekomendasikan Anda merotasi kunci akses. Untuk informasi selengkapnya, lihat [Merotasi kunci akses secara teratur untuk kasus penggunaan yang memerlukan kredensial jangka panjang](#) dalam Panduan Pengguna IAM.

[Grup IAM](#) adalah identitas yang menentukan sekumpulan pengguna IAM. Anda tidak dapat masuk sebagai grup. Anda dapat menggunakan grup untuk menentukan izin bagi beberapa pengguna sekaligus. Grup mempermudah manajemen izin untuk sejumlah besar pengguna sekaligus. Misalnya, Anda dapat memiliki grup yang bernama IAMAdmins dan memberikan izin ke grup tersebut untuk mengelola sumber daya IAM.

Pengguna berbeda dari peran. Pengguna secara unik terkait dengan satu orang atau aplikasi, tetapi peran dimaksudkan untuk dapat digunakan oleh siapa pun yang membutuhkannya. Pengguna

memiliki kredensial jangka panjang permanen, tetapi peran memberikan kredensial sementara. Untuk mempelajari selengkapnya, lihat [Kapan harus membuat pengguna IAM \(bukan peran\)](#) dalam Panduan Pengguna IAM.

Peran IAM

[Peran IAM](#) adalah identitas dalam diri Anda Akun AWS yang memiliki izin khusus. Peran ini mirip dengan pengguna IAM, tetapi tidak terkait dengan orang tertentu. Anda dapat mengambil peran IAM untuk sementara AWS Management Console dengan [beralih peran](#). Anda dapat mengambil peran dengan memanggil operasi AWS CLI atau AWS API atau dengan menggunakan URL kustom. Untuk informasi selengkapnya tentang cara menggunakan peran, lihat [Menggunakan peran IAM](#) dalam Panduan Pengguna IAM.

Peran IAM dengan kredensial sementara berguna dalam situasi berikut:

- Akses pengguna terfederasi – Untuk menetapkan izin ke identitas terfederasi, Anda membuat peran dan menentukan izin untuk peran tersebut. Ketika identitas terfederasi mengautentikasi, identitas tersebut terhubung dengan peran dan diberi izin yang ditentukan oleh peran. Untuk informasi tentang peran untuk federasi, lihat [Membuat peran untuk Penyedia Identitas pihak ketiga](#) dalam Panduan Pengguna IAM. Jika menggunakan Pusat Identitas IAM, Anda harus mengonfigurasi set izin. Untuk mengontrol apa yang dapat diakses identitas Anda setelah identitas tersebut diautentikasi, Pusat Identitas IAM akan mengorelasikan set izin ke peran dalam IAM. Untuk informasi tentang set izin, lihat [Set izin](#) dalam Panduan Pengguna AWS IAM Identity Center .
- Izin pengguna IAM sementara – Pengguna atau peran IAM dapat mengambil peran IAM guna mendapatkan berbagai izin secara sementara untuk tugas tertentu.
- Akses lintas akun – Anda dapat menggunakan peran IAM untuk mengizinkan seseorang (prinsipal tepercaya) di akun lain untuk mengakses sumber daya di akun Anda. Peran adalah cara utama untuk memberikan akses lintas akun. Namun, dengan beberapa Layanan AWS, Anda dapat melampirkan kebijakan secara langsung ke sumber daya (alih-alih menggunakan peran sebagai proxy). Untuk mempelajari perbedaan antara peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya](#) dalam Panduan Pengguna IAM.
- Akses lintas layanan — Beberapa Layanan AWS menggunakan fitur lain Layanan AWS. Sebagai contoh, ketika Anda memanggil suatu layanan, biasanya layanan tersebut menjalankan aplikasi di Amazon EC2 atau menyimpan objek di Amazon S3. Sebuah layanan mungkin melakukannya menggunakan izin prinsipal yang memanggil, menggunakan peran layanan, atau peran terkait layanan.

- Sesi akses teruskan (FAS) — Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses maju](#).
- Peran layanan – Peran layanan adalah [peran IAM](#) yang dijalankan oleh layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.
- Peran terkait layanan — Peran terkait layanan adalah jenis peran layanan yang ditautkan ke. Layanan AWS Layanan tersebut dapat menjalankan peran untuk melakukan tindakan atas nama Anda. Peran terkait layanan muncul di Anda Akun AWS dan dimiliki oleh layanan. Administrator IAM dapat melihat, tetapi tidak dapat mengedit izin untuk peran terkait layanan.
- Aplikasi yang berjalan di Amazon EC2 — Anda dapat menggunakan peran IAM untuk mengelola kredensi sementara untuk aplikasi yang berjalan pada instans EC2 dan membuat atau permintaan API. AWS CLI AWS Cara ini lebih dianjurkan daripada menyimpan kunci akses dalam instans EC2. Untuk menetapkan AWS peran ke instans EC2 dan membuatnya tersedia untuk semua aplikasinya, Anda membuat profil instance yang dilampirkan ke instance. Profil instans berisi peran dan memungkinkan program yang berjalan di instans EC2 mendapatkan kredensial sementara. Untuk informasi selengkapnya, lihat [Menggunakan peran IAM untuk memberikan izin ke aplikasi yang berjalan dalam instans Amazon EC2](#) dalam Panduan Pengguna IAM.

Untuk mempelajari apakah kita harus menggunakan peran IAM atau pengguna IAM, lihat [Kapan harus membuat peran IAM \(bukan pengguna\)](#) dalam Panduan Pengguna IAM.

Mengelola akses menggunakan kebijakan

Anda mengontrol akses AWS dengan membuat kebijakan dan melampirkannya ke AWS identitas atau sumber daya. Kebijakan adalah objek AWS yang, ketika dikaitkan dengan identitas atau sumber daya, menentukan izinnya. AWS mengevaluasi kebijakan ini ketika prinsipal (pengguna, pengguna root, atau sesi peran) membuat permintaan. Izin dalam kebijakan menentukan apakah permintaan diizinkan atau ditolak. Sebagian besar kebijakan disimpan AWS sebagai dokumen JSON. Untuk

informasi selengkapnya tentang struktur dan isi dokumen kebijakan JSON, lihat [Gambaran umum kebijakan JSON](#) dalam Panduan Pengguna IAM.

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

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

Kebijakan IAM mendefinisikan izin untuk suatu tindakan terlepas dari metode yang Anda gunakan untuk melakukan operasinya. Misalnya, anggaplah Anda memiliki kebijakan yang mengizinkan tindakan `iam:GetRole`. Pengguna dengan kebijakan tersebut bisa mendapatkan informasi peran dari AWS Management Console, API AWS CLI, atau AWS API.

Kebijakan berbasis identitas

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

Kebijakan berbasis identitas dapat dikategorikan lebih lanjut sebagai kebijakan inline atau kebijakan yang dikelola. Kebijakan inline disematkan langsung ke satu pengguna, grup, atau peran. Kebijakan terkelola adalah kebijakan mandiri yang dapat dilampirkan ke beberapa pengguna, grup, dan peran dalam. Akun AWS Kebijakan AWS terkelola mencakup kebijakan terkelola dan kebijakan yang dikelola pelanggan. Untuk mempelajari cara memilih antara kebijakan yang dikelola atau kebijakan inline, lihat [Memilih antara kebijakan yang dikelola dan kebijakan inline](#) dalam Panduan Pengguna IAM.

Kebijakan berbasis sumber daya

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

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

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

Daftar kontrol akses (ACL)

Daftar kontrol akses (ACL) mengendalikan prinsipal mana (anggota akun, pengguna, atau peran) yang memiliki izin untuk mengakses sumber daya. ACL serupa dengan kebijakan berbasis sumber daya, meskipun kebijakan tersebut tidak menggunakan format dokumen kebijakan JSON.

Amazon S3, AWS WAF, dan Amazon VPC adalah contoh layanan yang mendukung ACL. Untuk mempelajari ACL selengkapnya, lihat [Gambaran umum daftar kontrol akses \(ACL\)](#) dalam Panduan Developer Amazon Simple Storage Service.

Jenis-jenis kebijakan lain

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

- Batasan izin – Batasan izin adalah fitur lanjutan tempat Anda mengatur izin maksimum yang dapat diberikan oleh kebijakan berbasis identitas ke entitas IAM (pengguna IAM atau peran IAM). Anda dapat menetapkan batasan izin untuk suatu entitas. Izin yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas milik entitas dan batasan izinnya. Kebijakan berbasis sumber daya yang menentukan pengguna atau peran dalam bidang `Principal` tidak dibatasi oleh batasan izin. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya tentang batasan izin, lihat [Batasan izin untuk entitas IAM](#) dalam Panduan Pengguna IAM.
- Kebijakan kontrol layanan (SCP) — SCP adalah kebijakan JSON yang menentukan izin maksimum untuk organisasi atau unit organisasi (OU) di AWS Organizations. AWS Organizations adalah layanan untuk mengelompokkan dan mengelola secara terpusat beberapa Akun AWS yang dimiliki bisnis Anda. Jika Anda mengaktifkan semua fitur di organisasi, Anda dapat menerapkan kebijakan kontrol layanan (SCP) ke salah satu atau semua akun Anda. SCP membatasi izin untuk entitas di akun anggota, termasuk masing-masing. Pengguna root akun AWS Untuk informasi selengkapnya tentang Organisasi dan SCP, lihat [Cara kerja SCP](#) dalam Panduan Pengguna AWS Organizations .

- Kebijakan sesi – Kebijakan sesi adalah kebijakan lanjutan yang Anda berikan sebagai parameter ketika Anda membuat sesi sementara secara programatis untuk peran atau pengguna terfederasi. Izin sesi yang dihasilkan adalah perpotongan antara kebijakan berbasis identitas pengguna atau peran dan kebijakan sesi. Izin juga bisa datang dari kebijakan berbasis sumber daya. Penolakan eksplisit dalam salah satu kebijakan ini akan menggantikan pemberian izin. Untuk informasi selengkapnya, lihat [Kebijakan sesi](#) dalam Panduan Pengguna IAM.

Berbagai jenis kebijakan

Ketika beberapa jenis kebijakan berlaku pada suatu permintaan, izin yang dihasilkan lebih rumit untuk dipahami. Untuk mempelajari cara AWS menentukan apakah akan mengizinkan permintaan saat beberapa jenis kebijakan terlibat, lihat [Logika evaluasi kebijakan](#) di Panduan Pengguna IAM.

Bagaimana Amazon FSx for Lustre 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 for Lustre

Fitur IAM	Dukungan Amazon FSx
Kebijakan berbasis identitas	Ya
Kebijakan berbasis sumber daya	Tidak
Tindakan kebijakan	Ya
Sumber daya kebijakan	Ya
Kunci kondisi kebijakan	Ya
ACL	Tidak
ABAC (tanda dalam kebijakan)	Ya
Kredensial sementara	Ya
Sesi akses teruskan (FAS)	Ya

Fitur IAM	Dukungan Amazon FSx
Peran layanan	Tidak
Peran terkait layanan	Ya

Untuk mendapatkan tampilan tingkat tinggi tentang cara kerja Amazon FSx dan layanan AWS lainnya dengan sebagian besar fitur IAM, [AWS lihat 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 [Membuat kebijakan IAM](#) dalam Panduan Pengguna IAM.

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

Contoh kebijakan berbasis identitas untuk Amazon FSx

Untuk melihat contoh kebijakan berbasis identitas Amazon FSx, lihat. [Contoh kebijakan berbasis identitas untuk Amazon FSx for Lustre](#)

Kebijakan berbasis sumber daya dalam 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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Action` dari kebijakan JSON menjelaskan tindakan yang dapat Anda gunakan untuk mengizinkan atau menolak akses dalam sebuah kebijakan. Tindakan kebijakan biasanya memiliki nama yang sama dengan operasi AWS API terkait. Ada beberapa pengecualian, misalnya tindakan hanya izin yang tidak memiliki operasi API yang cocok. Ada juga beberapa operasi yang memerlukan beberapa tindakan dalam suatu kebijakan. Tindakan tambahan ini disebut tindakan dependen.

Menyertakan tindakan dalam kebijakan untuk memberikan izin untuk melakukan operasi terkait.

Untuk melihat daftar tindakan Amazon FSx, lihat [Tindakan yang ditentukan oleh Amazon FSx for Lustre](#) 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 berbasis identitas Amazon FSx, lihat [Contoh kebijakan berbasis identitas untuk Amazon FSx for Lustre](#)

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. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen kebijakan JSON `Resource` menentukan objek yang menjadi target penerapan tindakan. Pernyataan harus menyertakan elemen `Resource` atau `NotResource`. Praktik terbaiknya, tentukan sumber daya menggunakan [Amazon Resource Name \(ARN\)](#). Anda dapat melakukan ini untuk tindakan yang mendukung jenis sumber daya tertentu, yang dikenal sebagai izin tingkat sumber daya.

Untuk tindakan yang tidak mendukung izin di tingkat sumber daya, misalnya operasi pencantuman, gunakan wildcard (*) untuk menunjukkan bahwa pernyataan tersebut berlaku untuk semua sumber daya.

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

Untuk melihat daftar jenis sumber daya Amazon FSx dan ARNnya, lihat Sumber daya yang [ditetapkan oleh Amazon FSx for Lustre](#) dalam Referensi Otorisasi Layanan. Untuk mempelajari tindakan mana yang dapat Anda tentukan ARN dari setiap sumber daya, lihat [Tindakan yang ditetapkan oleh Amazon FSx for Lustre](#).

Untuk melihat contoh kebijakan berbasis identitas Amazon FSx, lihat. [Contoh kebijakan berbasis identitas untuk Amazon FSx for Lustre](#)

Kunci kondisi kebijakan untuk Amazon FSx

Mendukung kunci kondisi kebijakan khusus layanan	Ya
--	----

Administrator dapat menggunakan kebijakan AWS JSON untuk menentukan siapa yang memiliki akses ke apa. Artinya, prinsipal manakah yang dapat melakukan tindakan pada sumber daya apa, dan dengan kondisi apa.

Elemen `Condition` (atau blok `Condition`) akan memungkinkan Anda menentukan kondisi yang menjadi dasar suatu pernyataan berlaku. Elemen `Condition` bersifat opsional. Anda dapat membuat ekspresi bersyarat yang menggunakan [operator kondisi](#), misalnya sama dengan atau kurang dari, untuk mencocokkan kondisi dalam kebijakan dengan nilai-nilai yang diminta.

Jika Anda menentukan beberapa elemen Condition dalam sebuah pernyataan, atau beberapa kunci dalam elemen Condition tunggal, maka AWS akan mengevaluasinya menggunakan operasi AND logis. Jika Anda menentukan beberapa nilai untuk satu kunci kondisi, AWS mengevaluasi kondisi menggunakan OR operasi logis. Semua kondisi harus dipenuhi sebelum izin pernyataan diberikan.

Anda juga dapat menggunakan variabel placeholder saat menentukan kondisi. Sebagai contoh, Anda dapat memberikan izin kepada pengguna IAM untuk mengakses sumber daya hanya jika izin tersebut mempunyai tag yang sesuai dengan nama pengguna IAM mereka. Untuk informasi selengkapnya, lihat [Elemen kebijakan IAM: variabel dan tag](#) dalam Panduan Pengguna IAM.

AWS mendukung kunci kondisi global dan kunci kondisi khusus layanan. Untuk melihat semua kunci kondisi AWS global, lihat [kunci konteks kondisi AWS global](#) di Panduan Pengguna IAM.

Untuk melihat daftar kunci kondisi Amazon FSx, lihat Kunci kondisi [untuk Amazon FSx for Lustre](#) di Referensi Otorisasi Layanan. Untuk mempelajari tindakan dan sumber daya yang dapat Anda gunakan kunci kondisi, lihat [Tindakan yang ditentukan oleh Amazon FSx for Lustre](#).

Untuk melihat contoh kebijakan berbasis identitas Amazon FSx, lihat. [Contoh kebijakan berbasis identitas untuk Amazon FSx for Lustre](#)

Daftar kontrol akses (ACL) di Amazon FSx

Mendukung ACL

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. Dalam AWS, atribut ini disebut tag. Anda dapat melampirkan tag ke entitas IAM (pengguna atau peran) dan ke banyak AWS sumber daya. Penandaan ke entitas dan sumber daya adalah langkah pertama dari ABAC. Kemudian rancanglah kebijakan ABAC untuk mengizinkan operasi ketika tag milik prinsipal cocok dengan tag yang ada di sumber daya yang ingin diakses.

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

Untuk mengendalikan akses berdasarkan tag, berikan informasi tentang tag 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 [Apa itu 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 sumber daya Amazon FSx, lihat [Tandai sumber daya Amazon FSx Anda](#)

Untuk melihat contoh kebijakan berbasis identitas untuk membatasi akses ke sumber daya berdasarkan tag pada sumber daya tersebut, lihat [Menggunakan tanda untuk mengontrol akses ke sumber daya Amazon FSx sumber daya](#).

Menggunakan kredensial Sementara dengan Amazon FSx

Mendukung penggunaan kredensial sementara Ya

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

Anda menggunakan kredensi sementara jika Anda masuk AWS Management Console menggunakan metode apa pun kecuali nama pengguna dan kata sandi. Misalnya, ketika Anda mengakses AWS menggunakan tautan masuk tunggal (SSO) perusahaan Anda, proses tersebut secara otomatis membuat kredensial sementara. Anda juga akan secara otomatis membuat kredensial sementara ketika Anda masuk ke konsol sebagai seorang pengguna lalu beralih peran. Untuk informasi selengkapnya tentang peralihan peran, lihat [Peralihan peran \(konsol\)](#) dalam Panduan Pengguna IAM.

Anda dapat membuat kredensial sementara secara manual menggunakan API AWS CLI atau AWS . Anda kemudian dapat menggunakan kredensial sementara tersebut untuk mengakses AWS . AWS merekomendasikan agar Anda secara dinamis menghasilkan kredensial sementara alih-

alih menggunakan kunci akses jangka panjang. Untuk informasi selengkapnya, lihat [Kredensial keamanan sementara di IAM](#).

Teruskan sesi akses untuk Amazon FSx

Mendukung sesi akses maju (FAS)	Ya
---------------------------------	----

Saat Anda menggunakan pengguna atau peran IAM untuk melakukan tindakan AWS, Anda dianggap sebagai prinsipal. Ketika Anda menggunakan beberapa layanan, Anda mungkin melakukan sebuah tindakan yang kemudian menginisiasi tindakan lain di layanan yang berbeda. FAS menggunakan izin dari pemanggilan utama Layanan AWS, dikombinasikan dengan permintaan Layanan AWS untuk membuat permintaan ke layanan hilir. Permintaan FAS hanya dibuat ketika layanan menerima permintaan yang memerlukan interaksi dengan orang lain Layanan AWS atau sumber daya untuk menyelesaikannya. Dalam hal ini, Anda harus memiliki izin untuk melakukan kedua tindakan tersebut. Untuk detail kebijakan ketika mengajukan permintaan FAS, lihat [Sesi akses maju](#).

Peran layanan untuk Amazon FSx

Mendukung peran layanan	Tidak
-------------------------	-------

Peran layanan adalah sebuah [peran IAM](#) yang diambil oleh sebuah layanan untuk melakukan tindakan atas nama Anda. Administrator IAM dapat membuat, mengubah, dan menghapus peran layanan dari dalam IAM. Untuk informasi selengkapnya, lihat [Membuat sebuah peran untuk mendelegasikan izin ke Layanan AWS](#) dalam Panduan pengguna IAM.

Warning

Mengubah izin untuk peran layanan dapat merusak fungsionalitas Amazon FSx. Edit peran layanan hanya jika Amazon FSx memberikan panduan untuk melakukannya.

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 informasi selengkapnya tentang membuat dan mengelola peran terkait layanan Amazon FSx, lihat [Menggunakan peran terkait layanan untuk Amazon FSx](#)

Contoh kebijakan berbasis identitas untuk Amazon FSx for Lustre

Secara default, pengguna dan peran tidak memiliki izin untuk membuat atau memodifikasi sumber daya Amazon FSx. Mereka juga tidak dapat melakukan tugas dengan menggunakan AWS Management Console, AWS Command Line Interface (AWS CLI), atau AWS API. Untuk memberikan izin kepada pengguna untuk melakukan tindakan di sumber daya yang mereka perlukan, administrator IAM dapat membuat kebijakan IAM. Administrator kemudian akan dapat menambahkan kebijakan IAM ke peran, dan pengguna dapat mengambil peran.

Untuk mempelajari cara membuat kebijakan berbasis identitas IAM menggunakan contoh dokumen kebijakan JSON ini, lihat [Membuat kebijakan IAM](#) dalam Panduan Pengguna IAM.

Untuk detail tentang tindakan dan jenis sumber daya yang ditentukan oleh Amazon FSx, termasuk format ARN untuk setiap jenis sumber daya, lihat [Kunci tindakan, sumber daya, dan kondisi untuk Amazon FSx for Lustre](#) dalam Referensi Otorisasi Layanan.

Topik

- [Praktik terbaik kebijakan](#)
- [Menggunakan konsol Amazon FSx](#)
- [Mengizinkan pengguna melihat izin mereka sendiri](#)

Praktik terbaik kebijakan

Kebijakan berbasis identitas menentukan apakah seseorang dapat membuat, mengakses, atau menghapus sumber daya Amazon FSx di akun Anda. Tindakan ini membuat Akun AWS Anda dikenai biaya. Ketika Anda membuat atau mengedit kebijakan berbasis identitas, ikuti panduan dan rekomendasi ini:

- Mulailah dengan kebijakan AWS terkelola dan beralih ke izin hak istimewa paling sedikit — Untuk mulai memberikan izin kepada pengguna dan beban kerja Anda, gunakan kebijakan AWS terkelola

yang memberikan izin untuk banyak kasus penggunaan umum. Mereka tersedia di Anda Akun AWS. Kami menyarankan Anda mengurangi izin lebih lanjut dengan menentukan kebijakan yang dikelola AWS pelanggan yang khusus untuk kasus penggunaan Anda. Untuk informasi selengkapnya, lihat [Kebijakan yang dikelola AWS](#) atau [Kebijakan yang dikelola AWS untuk fungsi tugas](#) dalam Panduan Pengguna IAM.

- Menerapkan izin dengan hak akses paling rendah – Ketika Anda menetapkan izin dengan kebijakan IAM, hanya berikan izin yang diperlukan untuk melakukan tugas. Anda melakukannya dengan mendefinisikan tindakan yang dapat diambil pada sumber daya tertentu dalam kondisi tertentu, yang juga dikenal sebagai izin dengan hak akses paling rendah. Untuk informasi selengkapnya tentang cara menggunakan IAM untuk mengajukan izin, lihat [Kebijakan dan izin dalam IAM](#) dalam Panduan Pengguna IAM.
- Gunakan kondisi dalam kebijakan IAM untuk membatasi akses lebih lanjut – Anda dapat menambahkan suatu kondisi ke kebijakan Anda untuk membatasi akses ke tindakan dan sumber daya. Sebagai contoh, Anda dapat menulis kondisi kebijakan untuk menentukan bahwa semua permintaan harus dikirim menggunakan SSL. Anda juga dapat menggunakan ketentuan untuk memberikan akses ke tindakan layanan jika digunakan melalui yang spesifik Layanan AWS, seperti AWS CloudFormation. Untuk informasi selengkapnya, lihat [Elemen kebijakan JSON IAM: Kondisi](#) dalam Panduan Pengguna IAM.
- Gunakan IAM Access Analyzer untuk memvalidasi kebijakan IAM Anda untuk memastikan izin yang aman dan fungsional – IAM Access Analyzer memvalidasi kebijakan baru dan yang sudah ada sehingga kebijakan tersebut mematuhi bahasa kebijakan IAM (JSON) dan praktik terbaik IAM. IAM Access Analyzer menyediakan lebih dari 100 pemeriksaan kebijakan dan rekomendasi yang dapat ditindaklanjuti untuk membantu Anda membuat kebijakan yang aman dan fungsional. Untuk informasi selengkapnya, lihat [Validasi kebijakan 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 [Mengonfigurasi akses API yang dilindungi MFA](#) dalam Panduan Pengguna IAM.

Untuk informasi selengkapnya tentang praktik terbaik dalam IAM, lihat [Praktik terbaik keamanan dalam IAM](#) dalam Panduan Pengguna IAM.

Menggunakan konsol Amazon FSx

Untuk mengakses konsol Amazon FSx for Lustre, Anda harus memiliki set izin minimum. Izin ini harus memungkinkan Anda untuk membuat daftar dan melihat detail tentang sumber daya Amazon FSx di Anda. Akun AWS Jika Anda membuat kebijakan berbasis identitas yang lebih ketat daripada izin minimum yang diperlukan, konsol tidak akan berfungsi sebagaimana mestinya untuk entitas (pengguna atau peran) dengan kebijakan tersebut.

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

Untuk memastikan bahwa pengguna dan peran masih dapat menggunakan konsol Amazon FSx, 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 terkelola Amazon FSx lainnya di [AWS kebijakan terkelola untuk Amazon FSx](#)

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:ListGroupsWithUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
  ],
}
```

```
{
  "Sid": "NavigateInConsole",
  "Effect": "Allow",
  "Action": [
    "iam:GetGroupPolicy",
    "iam:GetPolicyVersion",
    "iam:GetPolicy",
    "iam:ListAttachedGroupPolicies",
    "iam:ListGroupPolicies",
    "iam:ListPolicyVersions",
    "iam:ListPolicies",
    "iam:ListUsers"
  ],
  "Resource": "*"
}
```

AWS kebijakan terkelola untuk Amazon FSx

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 [AWS kebijakan yang dikelola](#) dalam Panduan Pengguna IAM.

AmazonF SxServiceRolePolicy

Memungkinkan Amazon FSx mengelola AWS sumber daya atas nama Anda. Lihat [Menggunakan peran terkait layanan untuk Amazon FSx](#) untuk mempelajari selengkapnya.

AWS kebijakan terkelola: AmazonF SxDeleteServiceLinkedRoleAccess

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 for Lustre.

Detail izin

Kebijakan ini mencakup izin iam untuk mengizinkan Amazon FSx melihat, menghapus, dan melihat status penghapusan untuk Peran Tertaut Layanan FSx untuk akses Amazon S3.

Untuk melihat izin kebijakan ini, lihat [AmazonF SxDeleteServiceLinkedRoleAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AmazonF SxFullAccess

Anda dapat melampirkan `AmazonF SxFullAccess` ke entitas IAM Anda. Kebijakan ini juga dilampirkan ke peran layanan yang mengizinkan Amazon FSx untuk melakukan tindakan atas nama Anda.

Menyediakan akses penuh ke Amazon FSx dan akses ke layanan terkait AWS .

Detail izin

Kebijakan ini mencakup izin berikut.

- `fsx`— Memungkinkan kepala sekolah akses penuh untuk melakukan semua tindakan Amazon FSx, kecuali untuk `BypassSnaplockEnterpriseRetention`
- `ds`— Memungkinkan kepala sekolah untuk melihat informasi tentang direktori. AWS Directory Service
- `ec2`
 - Memungkinkan prinsipal untuk membuat tag di bawah kondisi yang ditentukan.
 - Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.

- `iam` – Mengizinkan prinsipal untuk membuat layanan Amazon FSx terkait peran atas nama pengguna. Ini diperlukan agar Amazon FSx dapat mengelola AWS sumber daya atas nama pengguna.
- `logs` — Mengizinkan prinsipal untuk membuat grup log, aliran log, dan menulis peristiwa untuk aliran log. Ini diperlukan agar pengguna dapat memantau akses sistem file FSx for Windows File Server dengan mengirimkan log akses audit CloudWatch ke Log.
- `firehose`— Memungkinkan kepala sekolah untuk menulis catatan ke Amazon Data Firehose. Ini diperlukan agar pengguna dapat memantau akses sistem file FSx for Windows File Server dengan mengirimkan log akses audit ke Firehose.

Untuk melihat izin kebijakan ini, lihat [AmazonF SxFullAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AmazonF SxConsoleFullAccess

Anda dapat melampirkan kebijakan `AmazonFSxConsoleFullAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin administratif yang memungkinkan akses penuh ke Amazon FSx dan akses ke layanan terkait AWS melalui AWS Management Console

Detail izin

Kebijakan ini mencakup izin berikut.

- `fsx`— Memungkinkan kepala sekolah untuk melakukan semua tindakan di konsol manajemen Amazon FSx, kecuali untuk `BypassSnaplockEnterpriseRetention`
- `cloudwatch`— Memungkinkan kepala sekolah untuk melihat CloudWatch Alarm dan metrik di konsol manajemen Amazon FSx.
- `ds`— Memungkinkan kepala sekolah untuk daftar informasi tentang direktori. AWS Directory Service
- `ec2`
 - Memungkinkan prinsipal untuk membuat tag pada tabel rute, daftar antarmuka jaringan, tabel rute, grup keamanan, subnet dan VPC yang terkait dengan sistem file Amazon FSx.
 - Memungkinkan prinsipal untuk Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.
- `kms`— Memungkinkan kepala sekolah untuk daftar alias untuk kunci. AWS Key Management Service

- `s3` – Mengizinkan prinsipal utama untuk mendaftar beberapa atau semua objek dalam bucket Amazon S3 (hingga 1000).
- `iam` – Memberikan izin untuk membuat peran tertaut layanan yang mengizinkan Amazon FSx melakukan tindakan atas nama pengguna.

Untuk melihat izin kebijakan ini, lihat [AmazonF SxConsoleFullAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AmazonF SxConsoleReadOnlyAccess

Anda dapat melampirkan kebijakan `AmazonFSxConsoleReadOnlyAccess` ke identitas IAM Anda.

Kebijakan ini memberikan izin hanya-baca ke Amazon FSx dan layanan AWS terkait sehingga pengguna dapat melihat informasi tentang layanan ini di AWS Management Console

Detail izin

Kebijakan ini mencakup izin berikut.

- `fsx` – Mengizinkan prinsipal untuk melihat informasi tentang sistem file Amazon FSx, termasuk semua tag, di Konsol Manajemen Amazon FSx.
- `cloudwatch`— Memungkinkan kepala sekolah untuk melihat CloudWatch Alarm dan metrik di Konsol Manajemen Amazon FSx.
- `ds`— Memungkinkan kepala sekolah untuk melihat informasi tentang AWS Directory Service direktori di Amazon FSx Management Console.
- `ec2`
 - Memungkinkan prinsipal untuk melihat antarmuka jaringan, grup keamanan, subnet, dan VPC yang terkait dengan sistem file Amazon FSx di Konsol Manajemen Amazon FSx.
 - Untuk memberikan validasi grup keamanan yang ditingkatkan dari semua grup keamanan yang dapat digunakan dengan VPC.
- `kms`— Memungkinkan prinsipal untuk melihat alias untuk kunci AWS Key Management Service di Amazon FSx Management Console.
- `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 FSx for Windows File Server.

- **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 FSx for Windows File Server.

Untuk melihat izin kebijakan ini, lihat [AmazonF SxConsoleReadOnlyAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

AWS kebijakan terkelola: AmazonF SxReadOnlyAccess

Anda dapat melampirkan kebijakan AmazonFSxReadOnlyAccess ke identitas IAM Anda.

Kebijakan ini mencakup izin berikut.

- **fsx** – Mengizinkan prinsipal untuk melihat informasi tentang sistem file Amazon FSx, 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 [AmazonF SxReadOnlyAccess](#) di Panduan Referensi Kebijakan AWS Terkelola.

Pembaruan Amazon FSx ke AWS kebijakan terkelola

Lihat detail tentang pembaruan kebijakan AWS terkelola untuk Amazon FSx sejak layanan ini mulai melacak perubahan ini. Untuk pemberitahuan otomatis tentang perubahan laman ini, berlangganalah ke umpan RSS pada laman Amazon FSx [Riwayat dokumen](#).

Perubahan	Deskripsi	Tanggal
AmazonF SxServiceRolePolicy - 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 09, 2024

Perubahan	Deskripsi	Tanggal
AmazonF SxReadOnlyAccess - 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 09, 2024
AmazonF SxConsoleReadOnlyAccess - 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 09, 2024
AmazonF SxFullAccess - 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 09, 2024

Perubahan	Deskripsi	Tanggal
AmazonF SxConsole 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 09, 2024
AmazonF SxFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi data lintas wilayah dan lintas akun untuk FSx untuk sistem file OpenZFS.	20 Desember 2023
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi data lintas wilayah dan lintas akun untuk FSx untuk sistem file OpenZFS.	20 Desember 2023
AmazonF SxFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi volume sesuai permintaan untuk FSx untuk sistem file OpenZFS.	26 November 2023

Perubahan	Deskripsi	Tanggal
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melakukan replikasi volume sesuai permintaan untuk FSx untuk sistem file OpenZFS.	26 November 2023
AmazonF SxFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melihat, mengaktifkan, dan menonaktifkan dukungan VPC bersama untuk FSx untuk sistem file Multi-AZ ONTAP.	14 November 2023
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melihat, mengaktifkan, dan menonaktifkan dukungan VPC bersama untuk FSx untuk sistem file Multi-AZ ONTAP.	14 November 2023
AmazonF SxFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx mengelola konfigurasi jaringan untuk FSx untuk sistem file Multi-AZ OpenZFS.	9 Agustus 2023

Perubahan	Deskripsi	Tanggal
AWS kebijakan terkelola: AmazonFSxServiceRolePolicy - 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
AmazonFSxFullAccess - Perbarui ke kebijakan yang ada	Amazon FSx memperbarui kebijakan untuk menghapus <code>fsx:*</code> izin dan menambahkan tindakan tertentu <code>fsx</code> .	13 Juli 2023
AmazonFSxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx memperbarui kebijakan untuk menghapus <code>fsx:*</code> izin dan menambahkan tindakan tertentu <code>fsx</code> .	13 Juli 2023
AmazonFSxConsole ReadOnlyAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melihat metrik kinerja yang ditingkatkan dan tindakan yang direkomendasikan untuk sistem file FSx for Windows File Server di konsol Amazon FSx.	21 September 2022
AmazonFSxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan pengguna melihat metrik kinerja yang ditingkatkan dan tindakan yang direkomendasikan untuk sistem file FSx for Windows File Server di konsol Amazon FSx.	21 September 2022

Perubahan	Deskripsi	Tanggal
AmazonF SxReadOnlyAccess - Memulai kebijakan pelacakan	Kebijakan ini memberikan akses hanya-baca ke semua sumber daya Amazon FSx dan tag apa pun yang terkait dengannya.	4 Februari 2022
AmazonF SxDeleteServiceLinkedRoleAccess - Memulai kebijakan pelacakan	Kebijakan ini memberikan izin administratif yang memungkinkan Amazon FSx menghapus Peran Tertaut Layanan untuk akses Amazon S3.	7 Januari 2022
AmazonF SxServiceRolePolicy - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx mengelola konfigurasi jaringan untuk Amazon FSx untuk sistem file ONTAP. NetApp	2 September 2021
AmazonF SxFullAccess - 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
AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada	Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx membuat Amazon NetApp FSx untuk sistem file Multi-AZ ONTAP.	2 September 2021
AmazonF SxConsole 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

Perubahan	Deskripsi	Tanggal
AmazonF SxServiceRolePolicy - Perbarui ke kebijakan yang ada	<p>Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx mendeskripsikan dan menulis ke aliran log Log. CloudWatch</p> <p>Ini diperlukan agar pengguna dapat melihat log audit akses file untuk sistem file FSx for Windows File Server CloudWatch menggunakan Log.</p>	8 Juni 2021
AmazonF SxServiceRolePolicy - Perbarui ke kebijakan yang ada	<p>Amazon FSx menambahkan izin baru untuk memungkinkan Amazon FSx mendeskripsikan dan menulis ke aliran pengiriman Amazon Data Firehose.</p> <p>Ini diperlukan agar pengguna dapat melihat log audit akses file untuk sistem file FSx for Windows File Server menggunakan Amazon Data Firehose.</p>	8 Juni 2021

Perubahan	Deskripsi	Tanggal
<p>AmazonF SxFullAccess - Perbarui ke kebijakan yang ada</p>	<p>Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan dan membuat grup log Log, aliran CloudWatch log, dan menulis peristiwa ke aliran log.</p> <p>Ini diperlukan agar prinsipal dapat melihat log audit akses file untuk sistem file FSx for Windows File Server menggunakan Log. CloudWatch</p>	8 Juni 2021
<p>AmazonF SxFullAccess - Perbarui ke kebijakan yang ada</p>	<p>Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan dan menulis catatan ke Amazon Data Firehose.</p> <p>Ini diperlukan agar pengguna dapat melihat log audit akses file untuk sistem file FSx for Windows File Server menggunakan Amazon Data Firehose.</p>	8 Juni 2021

Perubahan	Deskripsi	Tanggal
<p>AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada</p>	<p>Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan grup log CloudWatch Amazon Logs yang terkait dengan akun yang membuat permintaan.</p> <p>Ini diperlukan agar prinsipal dapat memilih grup CloudWatch log Log yang ada saat mengonfigurasi audit akses file untuk sistem file FSx for Windows File Server.</p>	8 Juni 2021
<p>AmazonF SxConsole FullAccess - Perbarui ke kebijakan yang ada</p>	<p>Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal menjelaskan aliran pengiriman Amazon Data Firehose yang terkait dengan akun yang membuat permintaan.</p> <p>Ini diperlukan agar prinsipal dapat memilih aliran pengiriman Firehose yang ada saat mengonfigurasi audit akses file untuk sistem file FSx for Windows File Server.</p>	8 Juni 2021

Perubahan	Deskripsi	Tanggal
AmazonF SxConsole ReadOnlyAccess - Perbarui ke kebijakan yang ada	<p>Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal mendeskripsikan grup log CloudWatch Amazon Logs yang terkait dengan akun yang membuat permintaan.</p> <p>Ini diperlukan agar prinsipal dapat melihat konfigurasi audit akses file yang ada untuk sistem file FSx for Windows File Server.</p>	8 Juni 2021
AmazonF SxConsole ReadOnlyAccess - Perbarui ke kebijakan yang ada	<p>Amazon FSx menambahkan izin baru untuk memungkinkan prinsipal menjelaskan aliran pengiriman Amazon Data Firehose yang terkait dengan akun yang membuat permintaan.</p> <p>Ini diperlukan agar prinsipal dapat melihat konfigurasi audit akses file yang ada untuk sistem file FSx for Windows File Server.</p>	8 Juni 2021
Amazon FSx mulai melacak perubahan	Amazon FSx mulai melacak perubahan untuk kebijakan yang AWS dikelola.	8 Juni 2021

Memecahkan masalah identitas dan akses Amazon FSx for Lustre

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 untuk mengakses sumber daya Amazon FSx 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 untuk mengakses sumber daya Amazon FSx 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 (ACL), 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 for Lustre 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 penggunaan kebijakan peran dan kebijakan berbasis sumber daya untuk akses lintas akun, lihat [Bagaimana peran IAM berbeda dari kebijakan berbasis sumber daya](#) dalam Panduan Pengguna IAM.

Menggunakan tanda dengan Amazon FSx

Anda dapat menggunakan tanda untuk mengontrol akses ke sumber daya Amazon FSx sumber daya dan menerapkan kontrol akses berbasis atribut (ABAC). Untuk menerapkan tag ke sumber daya Amazon FSx 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 Amazon FSx for Lustre API tindakan, Anda dapat menentukan tanda saat Anda menciptakan sumber daya. Anda dapat menggunakan tanda sumber daya ini untuk menerapkan kontrol akses berbasis atribut (ABAC). Untuk informasi lebih lanjut, lihat [Untuk apa ABAC untuk AWS?](#) dalam Panduan Pengguna IAM.

Agar pengguna menandai sumber daya pada pembuatan, mereka harus memiliki izin untuk menggunakan tindakan yang membuat sumber daya, seperti `fsx:CreateFileSystem`. Jika tanda ditentukan dalam aksi pembuatan sumber daya, IAM melakukan otorisasi tambahan pada `fsx:TagResource` tindakan untuk memverifikasi apakah pengguna memiliki izin untuk membuat tanda. Oleh karena itu, para pengguna juga harus memiliki izin eksplisit untuk menggunakan tindakan `fsx:TagResource`.

Kebijakan contoh berikut memungkinkan pengguna untuk membuat sistem file dan menerapkan tag kepada mereka selama pembuatan dalam spesifik Akun AWS.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
      ],
      "Resource": [
        "arn:aws:fsx:region:account-id:file-system/*"
      ]
    }
  ]
}
```

Demikian pula, kebijakan berikut memungkinkan pengguna membuat cadangan pada sistem file tertentu dan menerapkan tag apa pun pada 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 akan dievaluasi hanya jika tanda diterapkan selama tindakan penciptaan sumber daya. Oleh karena itu, pengguna yang memiliki izin untuk menciptakan sumber daya (dengan asumsi tidak ada ketentuan untuk pemberian tag) 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 penandaan Amazon FSx sumber daya sumber daya, lihat [Tandai sumber daya Amazon FSx Anda](#). Untuk informasi selengkapnya tentang menggunakan tanda untuk mengontrol akses ke sumber daya Amazon FSx for Lustre sumber daya, lihat [Menggunakan tanda untuk mengontrol akses ke sumber daya Amazon FSx sumber daya](#).

Menggunakan tanda untuk mengontrol akses ke sumber daya Amazon FSx sumber daya

Untuk mengontrol akses ke sumber daya Amazon FSx sumber daya dan tindakan, Anda dapat menggunakan kebijakan IAM berdasarkan tanda. Anda dapat memberikan kontrol ini dengan dua cara:

- Anda dapat mengontrol akses ke sumber daya Amazon FSx sumber daya berdasarkan tag pada sumber daya tersebut.
- Anda dapat mengontrol tag yang dapat diteruskan dalam ketentuan 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 penandaan Amazon FSx sumber daya pada pembuatan, lihat [Memberikan izin untuk memberi tanda pada sumber daya saat sumber daya tersebut dibuat](#). Untuk informasi selengkapnya tentang penandaan sumber daya sumber daya, lihat [Tandai sumber daya Amazon FSx Anda](#).

Mengontrol akses berdasarkan tanda pada sumber daya

Untuk mengontrol tindakan mana yang dapat dilakukan pengguna atau peran pada sumber daya Amazon FSx, Anda dapat menggunakan tag pada sumber daya. Misalnya, Anda mungkin ingin mengizinkan atau menolak operasi API tertentu pada sumber daya sistem file berdasarkan pasangan kunci-nilai tag pada sumber daya.

Example Contoh kebijakan - Membuat sistem file pada saat menyediakan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat sistem file hanya ketika 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 Contoh kebijakan - Buat backup hanya pada sistem file dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat cadangan hanya pada sistem file yang ditandai dengan pasangan nilai kuncikey=Department, value=Finance, dan cadangan akan dibuat dengan tagDepartment=Finance.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:TagResource",
        "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Department": "Finance"
        }
      }
    }
  ]
}

```

Example Contoh kebijakan - Membuat sistem file dengan tag tertentu dari cadangan dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat sistem file yang ditandai dengan `Department=Finance` hanya dari backup yang ditandai dengan `Department=Finance`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystemFromBackup",
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Department": "Finance"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystemFromBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    }
  ]
}
```

Example Contoh kebijakan - Hapus sistem file dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk menghapus sistem file yang diberi tag dengan `Department=Finance`. Jika mereka membuat cadangan akhir, maka

harus ditandai dengan `Department=Finance`. Untuk sistem file Lustre, pengguna memerlukan `fsx:CreateBackup` hak istimewa untuk membuat cadangan akhir.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:DeleteFileSystem"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateBackup",
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Department": "Finance"
        }
      }
    }
  ]
}
```

Example Contoh kebijakan - Membuat tugas repositori data pada sistem file dengan tag tertentu

Kebijakan ini memungkinkan pengguna untuk membuat tugas repositori data yang ditandai dengan `Department=Finance`, dan hanya pada sistem file yang ditandai dengan `Department=Finance`.

```
{
  "Version": "2012-10-17",
```

```

"Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "fsx:CreateDataRepositoryTask"
    ],
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/Department": "Finance"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "fsx:CreateDataRepositoryTask",
      "fsx:TagResource"
    ],
    "Resource": "arn:aws:fsx:region:account-id:task/*",
    "Condition": {
      "StringEquals": {
        "aws:RequestTag/Department": "Finance"
      }
    }
  }
]
}

```

Menggunakan peran terkait layanan untuk Amazon FSx

[Amazon FSx menggunakan peran terkait layanan AWS Identity and Access Management \(IAM\).](#)

Peran tertaut layanan adalah jenis IAM role unik yang terkait langsung dengan Amazon FSx. Peran terkait layanan telah ditentukan sebelumnya oleh Amazon FSx dan menyertakan semua izin yang diperlukan layanan untuk memanggil layanan lain atas nama Anda. AWS

Peran tertaut layanan mempermudah pengaturan Amazon FSx karena Anda tidak perlu menambahkan izin yang diperlukan secara manual. Amazon FSx menentukan izin atas peran tertaut layanan, dan kecuali ditentukan lain, hanya Amazon FSX yang dapat menjalankan perannya. Izin yang ditentukan mencakup kebijakan kepercayaan dan kebijakan izin, dan kebijakan izin tersebut tidak dapat dilampirkan ke entitas IAM lainnya.

Anda dapat menghapus peran tertaut layanan hanya setelah menghapus sumber daya terkait terlebih dahulu. Ini melindungi sumber daya Amazon FSx karena Anda tidak dapat secara ceroboh menghapus izin untuk mengakses sumber daya.

Untuk informasi tentang layanan lain yang mendukung peran terkait layanan, silakan lihat [layanan AWS yang bisa digunakan dengan IAM](#) dan carilah layanan yang memiliki opsi Ya di kolom Peran terkait layanan. Pilih Ya bersama tautan untuk melihat dokumentasi peran tertaut layanan untuk layanan tersebut.

Izin peran terkait layanan untuk Amazon FSx

Amazon FSx menggunakan dua peran terkait layanan bernama `AWSServiceRoleForAmazonFSx` dan `AWSServiceRoleForFSxS3Access_fs-01234567890` yang melakukan tindakan tertentu di akun Anda. Contoh tindakan ini adalah menciptakan antarmuka jaringan elastis untuk sistem file Anda di VPC Anda mengakses repositori data Anda dalam bucket Amazon S3. Untuk `AWSServiceRoleForFSxS3Access_fs-01234567890`, peran terkait layanan ini dibuat untuk setiap sistem file Amazon FSx for Lustre yang Anda buat yang terhubung ke bucket S3.

`AWSServiceRoleForAmazonFSx` rincian izin

Untuk `AWSServiceRoleForAmazonFSx`, kebijakan izin peran memungkinkan Amazon FSx untuk menyelesaikan tindakan administratif berikut atas nama pengguna atas semua AWS sumber daya yang berlaku:

Untuk pembaruan kebijakan ini, lihat [Amazon FSx Service Role Policy](#)

Note

`AWSServiceRoleForAmazonFSx` Ini digunakan oleh semua jenis sistem file Amazon FSx; beberapa izin yang terdaftar tidak berlaku untuk FSx for Lustre.

- `ds`— Memungkinkan Amazon FSx untuk melihat, mengotorisasi, dan tidak mengotorisasi aplikasi di direktori Anda. AWS Directory Service
- `ec2` — Mengizinkan Amazon FSx untuk melakukan hal berikut:
 - Melihat, membuat, dan memisahkan antarmuka jaringan yang terkait dengan sistem file Amazon FSx.
 - Lihat satu atau lebih alamat IP Elastis yang terkait dengan sistem file Amazon FSx.

- Lihat Amazon VPC, grup keamanan, dan subnet yang terkait dengan sistem file Amazon FSx.
- 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 untuk mempublikasikan titik data metrik ke CloudWatch bawah namespace `AWS/fsX`.
- `route53` — Mengizinkan Amazon FSx mengasosiasikan Amazon VPC dengan zona yang dihosting privat.
- `logs`— Memungkinkan Amazon FSx untuk mendeskripsikan dan menulis ke aliran CloudWatch log Log. Ini agar pengguna dapat mengirim log audit akses file untuk sistem file FSx for Windows File Server ke CloudWatch aliran Log.
- `firehose`— Memungkinkan Amazon FSx untuk mendeskripsikan dan menulis ke aliran pengiriman Amazon Data Firehose. Ini agar pengguna dapat mempublikasikan log audit akses file untuk sistem file FSx for Windows File Server ke aliran pengiriman Amazon Data Firehose.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateFileSystem",
      "Effect": "Allow",
      "Action": [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVPCs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
```

```
        "route53:AssociateVPCWithHostedZone"
    ],
    "Resource": "*"
},
{
    "Sid": "PutMetrics",
    "Effect": "Allow",
    "Action": [
        "cloudwatch:PutMetricData"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringEquals": {
            "cloudwatch:namespace": "AWS/FSx"
        }
    }
},
{
    "Sid": "TagResourceNetworkInterface",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": "CreateNetworkInterface"
        },
        "ForAllValues:StringEquals": {
            "aws:TagKeys": "AmazonFSx.FileSystemId"
        }
    }
},
{
    "Sid": "ManageNetworkInterface",
    "Effect": "Allow",
    "Action": [
        "ec2:AssignPrivateIpAddresses",
        "ec2:ModifyNetworkInterfaceAttribute",
```

```

        "ec2:UnassignPrivateIpAddresses"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:network-interface/*"
    ],
    "Condition": {
        "Null": {
            "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
        }
    }
},
{
    "Sid": "ManageRouteTable",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateRoute",
        "ec2:ReplaceRoute",
        "ec2>DeleteRoute"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:route-table/*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
        }
    }
},
{
    "Sid": "PutCloudWatchLogs",
    "Effect": "Allow",
    "Action": [
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents"
    ],
    "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
},
{
    "Sid": "ManageAuditLogs",
    "Effect": "Allow",
    "Action": [
        "firehose:DescribeDeliveryStream",
        "firehose:PutRecord",

```

```
        "firehose:PutRecordBatch"
      ],
      "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    }
  ]
}
```

Setiap pembaruan untuk kebijakan ini dijelaskan dalam [Pembaruan Amazon FSx ke AWS kebijakan 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](#).

AWSServiceRoleForFSxS3Access rincian izin

Untuk `AWSServiceRoleForFSxS3Access_`*file-system-id*, kebijakan izin peran memungkinkan Amazon FSx menyelesaikan tindakan berikut pada bucket Amazon S3 yang menghosting repositori data untuk sistem file Amazon FSx for Lustre.

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:Get*`
- `s3:List*`
- `s3:PutBucketNotification`
- `s3:PutObject`

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](#) dalam 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 AWS Management Console, API AWS CLI, atau AWS API, Amazon FSx 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 tertaut layanan ini, dan ingin membuatnya lagi, Anda dapat mengulangi proses yang sama untuk membuat kembali peran tersebut di akun Anda. Ketika Anda membuat sistem file, Amazon FSx membuat peran tertaut layanan untuk Anda kembali.

Mengedit peran terkait layanan untuk Amazon FSx

Amazon FSx tidak mengizinkan Anda mengedit peran terkait layanan ini. Setelah Anda membuat peran terkait layanan, Anda tidak dapat mengubah nama peran karena berbagai entitas mungkin mereferensikan 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, kami merekomendasikan Anda menghapus peran tersebut. Dengan begitu, Anda tidak memiliki entitas yang tidak digunakan yang tidak dipantau atau dipelihara secara aktif. Namun, Anda harus menghapus semua sistem file Anda sebelum Anda dapat menghapus peran tertaut layanan secara manual.

ℹ Note

Jika layanan Amazon FSx menggunakan peran saat Anda mencoba untuk menghapus sumber daya, maka penghapusan tersebut kemungkinan gagal. Jika hal itu terjadi, tunggu beberapa menit dan coba mengoperasikannya lagi.

Untuk menghapus peran terkait layanan secara manual menggunakan IAM

Gunakan konsol IAM, IAM CLI, atau IAM API untuk menghapus peran terkait layanan. `AWSServiceRoleForAmazonFSx` Untuk informasi lebih lanjut, lihat [Menghapus Peran Tertaut Layanan](#) di Panduan Pengguna IAM.

Wilayah yang didukung untuk peran terkait layanan Amazon FSx

Amazon FSx mensupport penggunaan peran terkait layanan di semua wilayah tempat layanan tersedia. Untuk informasi lebih lanjut, lihat [Wilayah dan Titik Akhir AWS](#).

Kontrol akses sistem file dengan Amazon VPC

Sistem file Amazon FSx dapat diakses melalui antarmuka jaringan elastis yang berada di virtual private cloud (VPC) berdasarkan layanan Amazon VPC yang Anda kaitkan dengan sistem file Anda. Anda mengakses sistem file Amazon FSx Anda melalui nama DNS, yang memetakan ke antarmuka jaringan sistem file. Hanya sumber daya dalam VPC terkait, atau VPC mengintip, dapat mengakses antarmuka jaringan sistem file Anda. Untuk informasi lebih lanjut, lihat [Apa itu Amazon VPC?](#) di Panduan Pengguna Amazon VPC.

Warning

Anda tidak boleh mengubah atau menghapus antarmuka jaringan elastis Amazon FSx. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan koneksi hilang permanen antara VPC dan sistem file Anda.

Grup keamanan Amazon VPC

Untuk lebih mengontrol lalu lintas jaringan yang akan melalui antarmuka jaringan sistem file Anda dalam VPC Anda, Anda menggunakan grup keamanan untuk membatasi akses ke sistem file Anda. Grup keamanan bertindak sebagai firewall virtual untuk mengendalikan lalu lintas untuk sumber daya terkait. Dalam hal ini, sumber daya terkait adalah antarmuka jaringan sistem file Anda. Anda juga menggunakan grup keamanan VPC untuk mengendalikan lalu lintas jaringan untuk klien Lustre Anda.

Mengendalikan akses menggunakan aturan inbound dan Outbound

Untuk menggunakan grup keamanan untuk mengendalikan akses ke sistem file Amazon FSx dan klien Lustre Anda, Anda menambahkan aturan inbound untuk mengendalikan lalu lintas masuk dan aturan outbound untuk mengendalikan lalu lintas keluar dari sistem file dan klien Lustre Anda. Pastikan untuk memiliki aturan lalu lintas jaringan yang tepat di grup keamanan Anda untuk memetakan berbagi file sistem file Amazon FSx Anda ke folder pada instans komputasi yang didukung.

Untuk informasi selengkapnya tentang aturan grup [keamanan](#), lihat [Aturan Grup Keamanan](#) di Panduan Pengguna Amazon EC2.

Untuk membuat grup keamanan untuk sistem file Amazon FSx Anda

1. [Buka konsol Amazon EC2 di https://console.aws.amazon.com/ec2](https://console.aws.amazon.com/ec2).
2. Di panel navigasi, pilih Grup Keamanan.
3. Pilih Create Security Group (Buat Grup Keamanan).
4. Tentukan nama dan deskripsi untuk grup keamanan.
5. Untuk VPC, pilih VPC yang terkait dengan sistem file Amazon FSx Anda untuk membuat grup keamanan di dalam VPC tersebut.
6. Pilih Buat untuk membuat grup keamanan.

Selanjutnya, Anda menambahkan aturan masuk ke grup keamanan yang baru saja Anda buat untuk mengaktifkan lalu lintas Lustre antara server file FSx for Lustre Anda.

Untuk menambahkan aturan inbound ke guro keamanan Anda

1. Pilih grup keamanan yang baru saja Anda buat jika belum dipilih. Untuk Tindakan, pilih Edit aturan inbound.
2. Tambahkan aturan inbound berikut ini.

Tipe	Protokol	Baris Port	Sumber	Deskripsi
Aturan TCP kustom	TCP	988	Pilih Khusus dan masukkan ID grup keamanan untuk grup keamanan yang baru saja Anda buat	Memungkinkan lalu lintas Lustre antara FSx for Lustre file server
Aturan TCP kustom	TCP	988	Pilih Kustom dan masukkan ID grup	Memungkinkan lalu lintas Lustre antara

Tipe	Protokol	Baris Port	Sumber	Deskripsi
			keamanan untuk grup keamanan yang terkait dengan klien Lustre Anda	FSx for Lustre file server dan Lustre client
Aturan TCP kustom	TCP	1018-1023	Pilih Khusus dan masukkan ID grup keamanan untuk grup keamanan yang baru saja Anda buat	Memungkinkan lalu lintas Lustre antara FSx for Lustre file server
Aturan TCP kustom	TCP	1018-1023	Pilih Kustom dan masukkan ID grup keamanan untuk grup keamanan yang terkait dengan klien Lustre Anda	Memungkinkan lalu lintas Lustre antara FSx for Lustre file server dan Lustre client

3. Pilih Simpan untuk menyimpan dan menerapkan aturan inbound baru.

Secara default, aturan grup keamanan mengizinkan semua lalu lintas outbound (Semua, 0.0.0.0/0). Jika grup keamanan Anda tidak mengizinkan semua lalu lintas outbound, tambahkan aturan outbound berikut ke grup keamanan Anda. Aturan ini memungkinkan lalu lintas antara FSx for Lustre file server dan Lustre client, dan antara server file Lustre.

Untuk menambahkan aturan outbound ke grup keamanan Anda

1. Pilih grup keamanan yang sama yang baru saja Anda tambahkan aturan inbound. Untuk Tindakan, pilih Edit aturan outbound.
2. Tambahkan aturan outbound berikut ini.

Tipe	Protokol	Baris Port	Sumber	Deskripsi
Aturan TCP kustom	TCP	988	Pilih Khusus dan masukkan ID grup keamanan untuk grup keamanan yang baru saja Anda buat	Izinkan lalu lintas Lustre antara FSx for Lustre file server
Aturan TCP kustom	TCP	988	Pilih Kustom dan masukkan ID grup keamanan untuk grup keamanan yang terkait dengan klien Lustre Anda	Izinkan lalu lintas Lustre antara FSx for Lustre file server dan Lustre client
Aturan TCP kustom	TCP	1018-1023	Pilih Khusus dan masukkan ID grup keamanan untuk grup keamanan yang baru saja Anda buat	Memungkinkan lalu lintas Lustre antara FSx for Lustre file server

Tipe	Protokol	Baris Port	Sumber	Deskripsi
Aturan TCP kustom	TCP	1018-1023	Pilih Kustom dan masukkan ID grup keamanan untuk grup keamanan yang terkait dengan klien Lustre Anda	Memungkinkan lalu lintas Lustre antara FSx for Lustre file server dan Lustre client

- Pilih Simpan untuk menyimpan dan menerapkan aturan outbound baru.

Untuk mengaitkan grup keamanan untuk Sistem file Amazon FSx Anda

- Buka konsol Amazon FSx di <https://console.aws.amazon.com/fsx/>.
- Pada dasbor konsol, pilih sistem file Anda untuk melihat detailnya.
- Pada tab Jaringan & Keamanan, pilih ID antarmuka jaringan sistem file Anda (misalnya, ENI-01234567890123456). Melakukan hal ini mengarahkan Anda kembali ke konsol Amazon EC2.
- Pilih setiap ID antara muka jaringan. Setiap tindakan membuka instans baru dari konsol Amazon EC2 di peramban Anda. Untuk setiap grup keamanan, pilih Ubah Grup Keamanan untuk Tindakan.
- Di kotak dialog Ubah Grup Keamanan, pilih grup keamanan yang akan digunakan, dan pilih Simpan.

Lustre klien aturan grup keamanan VPC

Untuk menggunakan grup keamanan VPC untuk mengendalikan akses ke sistem file Amazon FSx dan klien Lustre Anda, Anda menambahkan aturan inbound untuk mengendalikan lalu lintas masuk dan aturan outbound untuk mengendalikan lalu lintas keluar dari klien Lustre Anda. Pastikan untuk memiliki aturan lalu lintas jaringan yang tepat di grup keamanan Anda untuk memastikan bahwa lalu lintas Lustre dapat mengalir antara klien Lustre Anda dan sistem file Amazon FSx Anda.

Tambahkan aturan inbound berikut ke grup keamanan yang diterapkan untuk klien Lustre Anda.

Tipe	Protokol	Baris Port	Sumber	Deskripsi
Aturan TCP kustom	TCP	988	Pilih Kustom dan masukkan ID grup keamanan untuk grup keamanan yang terkait dengan klien Lustre Anda	Mengizinkan lalu lintas Lustre antar klien Lustre
Aturan TCP kustom	TCP	988	Pilih Kustom dan masukkan ID grup keamanan yang terkait dengan sistem file FSx for Lustre Anda	Memungkinkan lalu lintas Lustre antara FSx for Lustre file server dan Lustre client
Aturan TCP kustom	TCP	1018-1023	Pilih Kustom dan masukkan ID grup keamanan untuk grup keamanan yang terkait dengan klien Lustre Anda	Mengizinkan lalu lintas Lustre antar klien Lustre
Aturan TCP kustom	TCP	1018-1023	Pilih Kustom dan masukkan ID grup keamanan yang terkait dengan sistem file FSx for Lustre Anda	Memungkinkan lalu lintas Lustre antara FSx for Lustre file server dan Lustre client

Tambahkan aturan outbound berikut ke grup keamanan yang diterapkan untuk klien Lustre Anda.

Tipe	Protokol	Baris Port	Sumber	Deskripsi
Aturan TCP kustom	TCP	988	Pilih Kustom dan masukkan ID grup keamanan untuk grup keamanan yang terkait dengan klien Lustre Anda	Mengizinkan lalu lintas Lustre antar klien Lustre
Aturan TCP kustom	TCP	988	Pilih Kustom dan masukkan ID grup keamanan yang terkait dengan sistem file FSx for Lustre Anda	Izinkan lalu lintas Lustre antara FSx for Lustre file server dan Lustre client
Aturan TCP kustom	TCP	1018-1023	Pilih Kustom dan masukkan ID grup keamanan untuk grup keamanan yang terkait dengan klien Lustre Anda	Mengizinkan lalu lintas Lustre antar klien Lustre
Aturan TCP kustom	TCP	1018-1023	Pilih Kustom dan masukkan ID grup keamanan yang terkait dengan sistem	Memungkinkan lalu lintas Lustre antara FSx for Lustre file server dan Lustre client

Tipe	Protokol	Baris Port	Sumber	Deskripsi
			file FSx for Lustre Anda	

ACL jaringan VPC Amazon

Pilihan lain untuk mengamankan akses ke sistem file dalam VPC Anda adalah dengan menetapkan daftar kontrol akses jaringan (ACL jaringan). ACL jaringan terpisah dari grup keamanan, tetapi memiliki fungsionalitas yang sama untuk menambahkan lapisan keamanan tambahan untuk sumber daya di VPC Anda. Untuk informasi selengkapnya tentang penerapan kontrol akses menggunakan ACL jaringan, lihat [Mengontrol lalu lintas ke subnet menggunakan ACL Jaringan di Panduan Pengguna Amazon VPC](#).

Validasi Kepatuhan untuk Amazon FSx for Lustre

Untuk mempelajari apakah an Layanan AWS berada dalam lingkup program kepatuhan tertentu, lihat [Layanan AWS di Lingkup oleh Program Kepatuhan Layanan AWS](#) dan pilih program kepatuhan yang Anda minati. Untuk informasi umum, lihat [Program AWS Kepatuhan Program AWS](#).

Anda dapat mengunduh laporan audit pihak ketiga menggunakan AWS Artifact. Untuk informasi selengkapnya, lihat [Mengunduh Laporan di AWS Artifact](#).

Tanggung jawab kepatuhan Anda saat menggunakan Layanan AWS ditentukan oleh sensitivitas data Anda, tujuan kepatuhan perusahaan Anda, dan hukum dan peraturan yang berlaku. AWS menyediakan sumber daya berikut untuk membantu kepatuhan:

- [Panduan Memulai Cepat Keamanan dan Kepatuhan — Panduan](#) penerapan ini membahas pertimbangan arsitektur dan memberikan langkah-langkah untuk menerapkan lingkungan dasar AWS yang berfokus pada keamanan dan kepatuhan.
- [Arsitektur untuk Keamanan dan Kepatuhan HIPAA di Amazon Web Services](#) — Whitepaper ini menjelaskan bagaimana perusahaan dapat menggunakan AWS untuk membuat aplikasi yang memenuhi syarat HIPAA.

Note

Tidak semua memenuhi Layanan AWS syarat HIPAA. Untuk informasi selengkapnya, lihat [Referensi Layanan yang Memenuhi Syarat HIPAA](#).

- [AWS Sumber Daya AWS](#) — Kumpulan buku kerja dan panduan ini mungkin berlaku untuk industri dan lokasi Anda.
- [AWS Panduan Kepatuhan Pelanggan](#) - Memahami model tanggung jawab bersama melalui lensa kepatuhan. Panduan ini merangkum praktik terbaik untuk mengamankan Layanan AWS dan memetakan panduan untuk kontrol keamanan di berbagai kerangka kerja (termasuk Institut Standar dan Teknologi Nasional (NIST), Dewan Standar Keamanan Industri Kartu Pembayaran (PCI), dan Organisasi Internasional untuk Standardisasi (ISO)).
- [Mengevaluasi Sumber Daya dengan Aturan](#) dalam Panduan AWS Config Pengembang — AWS Config Layanan menilai seberapa baik konfigurasi sumber daya Anda mematuhi praktik internal, pedoman industri, dan peraturan.
- [AWS Security Hub](#)— Ini Layanan AWS memberikan pandangan komprehensif tentang keadaan keamanan Anda di dalamnya AWS. Security Hub menggunakan kontrol keamanan untuk sumber daya AWS Anda serta untuk memeriksa kepatuhan Anda terhadap standar industri keamanan dan praktik terbaik. Untuk daftar layanan dan kontrol yang didukung, lihat [Referensi kontrol Security Hub](#).
- [Amazon GuardDuty](#) — Ini Layanan AWS mendeteksi potensi ancaman terhadap beban kerja Akun AWS, kontainer, dan data Anda dengan memantau lingkungan Anda untuk aktivitas yang mencurigakan dan berbahaya. GuardDuty dapat membantu Anda mengatasi berbagai persyaratan kepatuhan, seperti PCI DSS, dengan memenuhi persyaratan deteksi intrusi yang diamanatkan oleh kerangka kerja kepatuhan tertentu.
- [AWS Audit Manager](#)Ini Layanan AWS membantu Anda terus mengaudit AWS penggunaan Anda untuk menyederhanakan cara Anda mengelola risiko dan kepatuhan terhadap peraturan dan standar industri.

Amazon FSx for Lustre dan titik akhir VPC antarmuka ()AWS PrivateLink

Anda dapat meningkatkan postur keamanan VPC Anda dengan mengonfigurasi Amazon FSx untuk menggunakan titik akhir VPC antarmuka. Endpoint VPC antarmuka didukung oleh [AWS PrivateLink](#),

teknologi yang memungkinkan Anda mengakses Amazon fsX API secara pribadi tanpa gateway internet, perangkat NAT, koneksi VPN, atau koneksi. AWS Direct Connect Instans di VPC Anda tidak memerlukan alamat IP publik untuk berkomunikasi dengan Amazon fsX API. Lalu lintas antara VPC Anda dan Amazon 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.

Pertimbangan untuk titik akhir VPC antarmuka Amazon FSx

Sebelum Anda 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 for Lustre dengan CreateFileSystem memanggil API dari dalam VPC Anda. Untuk daftar lengkap API Amazon FSx, lihat [Tindakan](#) di Referensi API Amazon FSx.

Pertimbangan mengintip VPC

Anda dapat menghubungkan VPC lain ke VPC dengan titik akhir VPC antarmuka menggunakan VPC peering. Peering VPC adalah koneksi jaringan di antara dua VPC. Anda dapat membuat koneksi peering VPC antara dua VPC Anda sendiri, atau dengan VPC di VPC lain. Akun AWS VPC juga bisa dalam dua hal yang berbeda Wilayah AWS.

Lalu lintas antara VPC peered tetap berada di AWS jaringan dan tidak melintasi internet publik. Setelah VPC dipeer, sumber daya seperti Amazon Elastic Compute Cloud (Amazon EC2) instans di kedua VPC dapat mengakses Amazon fsX API melalui titik akhir VPC antarmuka yang dibuat di salah satu VPC.

Membuat titik akhir VPC antarmuka untuk Amazon FSx API

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 daftar lengkap titik akhir Amazon FSx, lihat titik akhir dan kuota Amazon [FSx](#) di. Referensi Umum Amazon Web Services

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 China, jika Anda mengaktifkan DNS pribadi untuk titik akhir, Anda dapat membuat permintaan API ke Amazon FSx dengan titik akhir VPC menggunakan nama DNS default untuk, misalnya. Wilayah `AWSfsx.us-east-1.amazonaws.com` Untuk China (Beijing) dan China (Ningxia) Wilayah AWS, Anda dapat membuat permintaan API dengan titik akhir VPC `fsx-api.cn-north-1.amazonaws.com.cn` menggunakan `fsx-api.cn-northwest-1.amazonaws.com.cn` dan, masing-masing.

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 lebih lanjut ke Amazon FSx API, Anda dapat melampirkan kebijakan AWS Identity and Access Management (IAM) secara opsional ke titik akhir VPC Anda. Kebijakan menentukan informasi berikut:

- Prinsipal yang dapat melakukan tindakan.
- Tindakan yang dapat dilakukan.
- Sumber daya yang menjadi target tindakan.

Untuk informasi selengkapnya, lihat [Mengontrol Akses ke Layanan dengan titik akhir VPC](#) dalam Panduan Pengguna Amazon VPC.

Kuota

Berikut ini, Anda dapat mengetahui tentang kuota saat bekerja dengan Amazon FSx for Lustre.

Topik

- [Kuota yang dapat Anda tingkatkan](#)
- [Sumber daya kuota untuk setiap sistem file](#)
- [Pertimbangan tambahan](#)

Kuota yang dapat Anda tingkatkan

Berikut ini adalah kuota untuk Amazon FSx for AWS Lustre per akun, per Wilayah AWS , yang dapat Anda tingkatkan.

Sumber daya	Default	Deskripsi
Sistem berkas Lustre Persistent_1	100	Jumlah maksimum sistem file Amazon FSx for Lustre Persistent_1 yang dapat Anda buat di akun ini.
Sistem berkas Lustre Persistent_2	100	Jumlah maksimum sistem file Amazon FSx for Lustre Persistent_2 yang dapat Anda buat di akun ini.
Kapasitas penyimpanan persisten HDD Lustre (per sistem file)	102000	Jumlah maksimum kapasitas penyimpanan HDD (dalam GiB) yang dapat Anda konfigurasi untuk sistem file persisten Amazon FSx for Lustre.
Lustre Persistent_1 kapasitas penyimpanan file	100800	Jumlah maksimum kapasitas penyimpanan (dalam GiB) yang dapat Anda konfigurasi

Sumber daya	Default	Deskripsi
		sikan untuk semua sistem file Amazon FSx for Lustre Persistent_1 di akun ini.
Lustre Persistent_2 kapasitas penyimpanan file	100800	Jumlah maksimum kapasitas penyimpanan (dalam GiB) yang dapat Anda konfigurasi untuk semua sistem file Amazon FSx for Lustre Persistent_2 di akun ini.
Sistem file Lustre scratch	100	Jumlah maksimum Amazon FSx for Lustre untuk sistem file scratch yang dapat Anda buat di akun ini.
Kapasitas penyimpanan Scratch Lustre	100800	Jumlah maksimum kapasitas penyimpanan (dalam GiB) yang dapat Anda konfigurasi untuk semua sistem file scratch Amazon FSx for Lustre di akun ini.
Backup Lustre	500	Jumlah maksimum backup yang diinisiasi pengguna yang dapat Anda miliki untuk semua sistem file Amazon FSx for Lustre di akun ini.

Meminta untuk penambahan Kuota

1. Buka [Konsol Service Quotas](#).
2. Di panel navigasi, pilih Layanan AWS .
3. Pilih Amazon FSx.
4. Pilih kuota.

5. Pilih Permintaan peningkatan kuota, dan ikuti petunjuk arahan untuk meminta peningkatan kuota.
6. Untuk melihat status permintaan kuota, pilih Riwayat permintaan kuota di panel navigasi konsol.

Untuk informasi lebih lanjut, lihat [Meminta peningkatan kuota](#) di Panduan Pengguna Service Quotas.

Sumber daya kuota untuk setiap sistem file

Berikut ini adalah batas pada sumber daya Amazon FSx for Lustre untuk setiap sistem file dalam sebuah Wilayah AWS .

Sumber daya	Batas per sistem file
Jumlah maksimum tag	50
Periode penyimpanan maksimum untuk cadangan otomatis	90 hari
Jumlah maksimum permintaan salinan cadangan yang sedang berlangsung ke satu Wilayah tujuan per akun.	5
Jumlah pembaruan file dari tautan bucket S3 per sistem file	10 juta/bulan
Kapasitas penyimpanan minimum, sistem file SSD	1,2 TiB
Kapasitas penyimpanan minimum, sistem file HDD	6 TiB
TPenyimpanan throughput minimum per unit SSD	50 MBps
Throughput maksimum per unit penyimpanan, SSD	1000 MBps
Throughput minimum per unit penyimpanan, HDD	12 MBps
Throughput maksimum per unit penyimpanan, HDD	40 MBps

Pertimbangan tambahan

Selain itu, perhatikan hal berikut:

- Anda dapat menggunakan setiap tombol AWS Key Management Service (AWS KMS) hingga 125 Amazon FSx for Lustre file system.
- Untuk daftar AWS Wilayah tempat Anda dapat membuat sistem file, lihat [Titik Akhir dan Kuota Amazon FSx](#) di bagian. Referensi Umum AWS

Pemecahan Masalah

Gunakan informasi berikut untuk membantu Anda menyelesaikan masalah yang mungkin Anda temui saat bekerja dengan sistem file Amazon FSx for Lustre.

Jika Anda mengalami masalah yang tidak tercantum berikut, coba ajukan pertanyaan di forum [Amazon FSx for Lustre](#).

Topik

- [Mencoba membuat sistem file FSx for Lustre gagal](#)
- [Memecahkan masalah pemasangan sistem file](#)
- [Anda tidak dapat mengakses sistem file Anda](#)
- [Tidak dapat memvalidasi akses ke bucket S3 saat membuat asosiasi repositori data](#)
- [Mengganti nama direktori membutuhkan waktu lama](#)
- [Memecahkan masalah bucket S3 terkait yang salah dikonfigurasi](#)
- [Pemecahan masalah penyimpanan](#)
- [Memecahkan masalah driver FSx for Lustre CSI](#)

Mencoba membuat sistem file FSx for Lustre gagal

Ada sejumlah penyebab potensial ketika permintaan pembuatan sistem file gagal, seperti yang dijelaskan dalam topik berikut.

Tidak dapat membuat sistem file karena grup keamanan yang salah dikonfigurasi

Membuat sistem file FSx for Lustre gagal dengan pesan kesalahan berikut:

```
The file system cannot be created because the default security group in the subnet provided or the provided security groups do not permit Lustre LNET network traffic on port 988
```

Tindakan yang harus diambil

Pastikan grup keamanan VPC yang Anda gunakan untuk operasi pembuatan dikonfigurasi seperti yang dijelaskan dalam. [Kontrol akses sistem file dengan Amazon VPC](#) Anda harus mengatur

grup keamanan untuk memungkinkan lalu lintas masuk pada port 988 dan 1018-1023 dari grup keamanan itu sendiri atau CIDR subnet penuh, yang diperlukan untuk memungkinkan host sistem file berkomunikasi satu sama lain.

Tidak dapat membuat sistem file yang tertaut ke bucket S3

Jika membuat sistem file baru yang tertaut dengan bucket S3 gagal dengan pesan kesalahan yang mirip dengan berikut ini.

```
User: arn:aws:iam::012345678901:user/username is not authorized to perform:  
iam:PutRolePolicy on resource: resource ARN
```

Kesalahan ini dapat terjadi jika Anda mencoba untuk membuat sistem file yang terhubung ke bucket Amazon S3 tanpa izin IAM yang diperlukan. Izin IAM yang diperlukan memberikan support Amazon FSx for Lustre untuk peran terkait layanan yang digunakan untuk mengakses bucket Amazon S3 tertentu atas nama Anda.

Tindakan yang harus diambil

Pastikan bahwa entitas IAM Anda (pengguna, grup, atau peran) memiliki izin yang sesuai untuk membuat sistem file. Melakukan hal ini termasuk menambahkan kebijakan izin yang mendukung peran terkait layanan Amazon FSx for Lustre. Untuk informasi selengkapnya, lihat [Menambahkan izin untuk menggunakan repositori data di Amazon S3](#).

Untuk mengetahui informasi selengkapnya tentang peran terkait layanan, lihat [Menggunakan peran terkait layanan untuk Amazon FSx](#).

Memecahkan masalah pemasangan sistem file

Ada sejumlah penyebab potensial ketika perintah pemasangan sistem file gagal, seperti yang dijelaskan dalam topik berikut.

Pemasangan sistem file gagal segera

Pemasangan sistem file gagal segera. Kode berikut menunjukkan contoh.

```
mount.lustre: mount fs-0123456789abcdef0.fsx.us-east-1.aws@tcp:/fsx at /lustre  
failed: No such file or directory
```

```
Is the MGS specification correct?  
Is the filesystem name correct?
```

Kesalahan ini dapat terjadi jika Anda tidak menggunakan nilai `mountname` ketika memasang sistem file scratch 2 persisten atau menggunakan perintah `mount`. Anda bisa mendapatkan `mountname` nilai dari respons [describe-file-systems](#) AWS CLI perintah atau operasi [DescribeFileSystemsAPI](#).

Pemasangan sistem file hang dan kemudian gagal dengan kesalahan timeout

Perintah pemasangan sistem file hang selama satu atau dua menit, dan kemudian gagal dengan kesalahan timeout.

Kode berikut menunjukkan contoh.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx  
  
[2+ minute wait here]  
Connection timed out
```

Kesalahan ini dapat terjadi karena grup keamanan untuk instans Amazon EC2 atau sistem file tidak dikonfigurasi dengan benar.

Tindakan yang harus diambil

Pastikan bahwa grup keamanan untuk sistem file memiliki aturan inbound yang ditentukan dalam [Grup keamanan Amazon VPC](#).

Pemasangan otomatis gagal dan instans tidak responsif

Dalam beberapa kasus, pemasangan otomatis mungkin gagal untuk sistem file dan instans Amazon EC2 Anda mungkin berhenti merespons.

Masalah ini dapat terjadi jika pilihan `_netdev` tidak dideklarasikan. Jika `_netdev` hilang, instans Amazon EC2 Anda dapat berhenti merespons. Hasil ini didapatkan karena sistem file jaringan perlu diinisialisasi setelah instans komputasi memulai jaringannya.

Tindakan yang harus diambil

Jika masalah ini terjadi, hubungi AWS Support.

Pemasangan sistem file gagal selama boot sistem

Pemasangan sistem file gagal selama boot sistem. Pemasangan otomatis menggunakan `/etc/fstab`. Ketika sistem file tidak terpasang, kesalahan berikut terlihat di syslog untuk kerangka waktu booting instans.

```
LNetError: 3135:0:(lib-socket.c:583:lnet_sock_listen()) Can't create socket: port 988
already in use
LNetError: 122-1: Can't start acceptor on port 988: port already in use
```

Kesalahan ini dapat terjadi ketika port 988 tidak tersedia. Ketika instans dikonfigurasi untuk memasang sistem file NFS, ada kemungkinan bahwa pemasangan NFS akan mengikat port klien ke port 988

Tindakan yang harus diambil

Anda dapat mengatasi masalah ini dengan tuning klien NFS `noresvport` dan opsi pemasangan `noauto` jika memungkinkan.

Pemasangan sistem file menggunakan nama DNS gagal

Nama Layanan Nama Domain (DNS) yang salah konfigurasi dapat menyebabkan kegagalan pemasangan sistem file, seperti yang ditunjukkan dalam skenario berikut ini.

Skenario 1: pemasangan sistem file yang menggunakan nama Layanan Nama Domain (DNS) gagal. Kode berikut menunjukkan contoh.

```
sudo mount -t lustre file_system_dns_name@tcp://mounname /mnt/fsx
mount.lustre: Can't parse NID
'file_system_dns_name@tcp://mounname'
```

Tindakan yang harus diambil

Periksa konfigurasi virtual private cloud (VPC) Anda. Jika Anda menggunakan VPC kustom, pastikan bahwa pengaturan DNS diaktifkan. Untuk informasi lebih lanjut, lihat [Menggunakan DNS dengan VPC](#) di Panduan Pengguna Amazon VPC.

Untuk menentukan nama DNS di Perintah mount ini, lakukan hal berikut:

- Pastikan bahwa instans Amazon EC2 berada di VPC yang sama seperti sistem file Amazon FSx for Lustre Anda untuk sistem file.

- Connect instans Amazon EC2 Anda di VPC yang dikonfigurasi untuk menggunakan server DNS yang disediakan oleh Amazon. Untuk informasi lebih lanjut, lihat [Pengaturan Opsi DHCP](#) di Panduan Pengguna Amazon VPC.
- Pastikan bahwa Amazon VPC instans Amazon EC2 untuk connect memiliki nama host DNS yang diaktifkan. Untuk informasi lebih lanjut, lihat [Memperbarui Support DNS untuk VPC Anda](#) di Panduan Pengguna Amazon VPC.

Skenario 2: pemasangan sistem file yang menggunakan nama Layanan Nama Domain (DNS) gagal. Kode berikut menunjukkan contoh.

```
mount -t lustre file_system_dns_name@tcp:/mounname /mnt/fsx
mount.lustre: mount file_system_dns_name@tcp:/mounname at /mnt/fsx failed: Input/output error Is the MGS running?
```

Tindakan yang harus diambil

Pastikan bahwa grup keamanan VPC klien memiliki aturan lalu lintas outbound tepat yang diterapkan. Rekomendasi ini berlaku terutama jika Anda tidak menggunakan grup keamanan default, atau jika Anda telah mengubah grup keamanan default. Untuk informasi selengkapnya, lihat [Grup keamanan Amazon VPC](#).

Anda tidak dapat mengakses sistem file Anda

Ada beberapa kemungkinan penyebab Anda tidak dapat mengakses sistem file Anda, masing-masing memiliki penyelesaian masalah sendiri, sebagai berikut.

Alamat IP Elastis yang dilekatkan pada antarmuka jaringan elastis sistem file telah dihapus

Amazon FSx tidak support sistem file akses dari internet publik. Amazon FSx secara otomatis melepaskan alamat IP Elastis, yang merupakan alamat IP publik yang dapat dijangkau dari internet, yang akan dilampirkan pada antarmuka jaringan elastis sistem file ini.

Antarmuka jaringan elastis sistem file telah dimodifikasi atau dihapus

Anda tidak boleh mengubah atau menghapus antarmuka jaringan elastis sistem file. Memodifikasi atau menghapus antarmuka jaringan dapat menyebabkan koneksi hilang permanen antara VPC dan

sistem file Anda. Buat sistem file baru, dan tidak mengubah atau menghapus antarmuka jaringan elastis FSx. Untuk informasi selengkapnya, lihat [Kontrol akses sistem file dengan Amazon VPC](#).

Tidak dapat memvalidasi akses ke bucket S3 saat membuat asosiasi repositori data

Membuat asosiasi repositori data (DRA) dari konsol Amazon FSx atau menggunakan perintah `create-data-repository-association` CLI ([CreateDataRepositoryAssociation](#) adalah tindakan API yang setara) gagal dengan pesan kesalahan berikut.

```
Amazon FSx is unable to validate access to the S3 bucket. Ensure the IAM role or user you are using has s3:Get*, s3:List* and s3:PutObject permissions to the S3 bucket prefix.
```

Note

Anda juga bisa mendapatkan kesalahan di atas saat membuat sistem file Scratch 1, Scratch 2, atau Persistent 1 yang ditautkan ke repositori data (bucket atau awalan S3) menggunakan konsol Amazon FSx atau perintah `create-file-system` [CreateFileSystem](#) CLI (adalah tindakan API yang setara).

Tindakan yang harus diambil

Jika sistem file FSx for Lustre berada di akun yang sama dengan bucket S3, kesalahan ini berarti peran IAM yang Anda gunakan untuk permintaan buat tidak memiliki izin yang diperlukan untuk mengakses bucket S3. Pastikan peran IAM memiliki izin yang tercantum dalam pesan kesalahan. Izin ini mendukung peran terkait layanan Amazon FSx for Lustre yang digunakan untuk mengakses bucket Amazon S3 yang ditentukan atas nama Anda.

Jika sistem file FSx for Lustre berada di akun yang berbeda sebagai bucket S3 (kasus lintas akun), selain memastikan peran IAM yang Anda gunakan memiliki izin yang diperlukan, kebijakan bucket S3 harus dikonfigurasi untuk mengizinkan akses dari akun tempat FSx for Lustre dibuat. Berikut ini adalah contoh kebijakan bucket,

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Effect": "Allow",
    "Principal": {
      "AWS": "*"
    },
    "Action": [
      "s3:AbortMultipartUpload",
      "s3:DeleteObject",
      "s3:PutObject",
      "s3:GetObject",
      "s3:GetBucketAcl",
      "s3:GetBucketNotification",
      "s3:ListBucket",
      "s3:PutBucketNotification"
    ],
    "Resource": [
      "arn:aws:s3:::bucket_name",
      "arn:aws:s3:::bucket_name/*"
    ],
    "Condition": {
      "StringLike": {
        "aws:PrincipalArn": [
          "arn:aws:iam::file_system_account_ID:role/aws-service-role/
s3.data-source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fs-*"
        ]
      }
    }
  ]
}

```

Untuk informasi selengkapnya tentang izin bucket lintas akun S3, lihat [Contoh 2: Pemilik bucket yang memberikan izin bucket lintas akun di](#) Panduan Pengguna Layanan Penyimpanan Sederhana Amazon.

Mengganti nama direktori membutuhkan waktu lama

Pertanyaan

Saya mengganti nama direktori pada sistem file yang ditautkan ke bucket Amazon S3 dan mengaktifkan ekspor otomatis. Mengapa file di dalam direktori ini membutuhkan waktu lama untuk diganti namanya pada bucket S3?

Menjawab

Saat Anda mengganti nama direktori pada sistem file, FSx for Lustre membuat objek S3 baru untuk semua file dan direktori di dalam direktori yang diganti namanya. Jumlah waktu yang diperlukan untuk menyebarkan nama direktori ke S3 secara langsung berkorelasi dengan jumlah file dan direktori yang merupakan keturunan dari direktori yang diganti namanya.

Memecahkan masalah bucket S3 terkait yang salah dikonfigurasi

Dalam beberapa kasus, bucket S3 tertaut sistem file FSx for Lustre mungkin memiliki status siklus hidup repositori data yang salah dikonfigurasi.

Kemungkinan penyebab

Kesalahan ini dapat terjadi jika Amazon FSx tidak memiliki izin yang diperlukan AWS Identity and Access Management (IAM) yang diperlukan untuk mengakses repositori data tertaut. Izin IAM yang diperlukan memberikan support Amazon FSx for Lustre untuk peran terkait layanan yang digunakan untuk mengakses bucket Amazon S3 tertentu atas nama Anda.

Tindakan yang harus diambil

1. Pastikan bahwa entitas IAM Anda (pengguna, grup, atau peran) memiliki izin yang sesuai untuk membuat sistem file. Melakukan hal ini termasuk menambahkan kebijakan izin yang mendukung peran terkait layanan Amazon FSx for Lustre. Untuk informasi selengkapnya, lihat [Menambahkan izin untuk menggunakan repositori data di Amazon S3](#).
2. Menggunakan Amazon FSx CLI atau API, segarkan sistem file dengan `AutoImportPolicy` perintah `update-file-system` CLI ([UpdateFileSystem](#) adalah tindakan API yang setara), sebagai berikut.

```
aws fsx update-file-system \  
--file-system-id fs-0123456789abcdef0 \  
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Untuk mengetahui informasi selengkapnya tentang peran terkait layanan, lihat [Menggunakan peran terkait layanan untuk Amazon FSx](#).

Kemungkinan Penyebabnya

Kesalahan ini dapat terjadi jika repositori data Amazon S3 tertaut memiliki konfigurasi notifikasi peristiwa yang ada dengan jenis peristiwa yang tumpang tindih dengan konfigurasi notifikasi peristiwa Amazon FSx (`s3:ObjectCreated:*`, `s3:ObjectRemoved:*`).

Hal ini juga dapat terjadi jika konfigurasi notifikasi peristiwa Amazon FSx pada bucket S3 tertaut dihapus atau diubah.

Tindakan yang harus diambil

1. Hapus notifikasi peristiwa yang ada pada bucket S3 terkait yang menggunakan salah satu atau kedua jenis peristiwa yang menggunakan konfigurasi peristiwa FSx, `s3:ObjectCreated:*` dan `s3:ObjectRemoved:*`.
2. Silakan pastikan bahwa ada Konfigurasi Notifikasi Peristiwa S3 di bucket S3 tertaut Anda dengan nama FSx, jenis peristiwa `s3:ObjectCreated:*` dan `s3:ObjectRemoved:*`, dan kirim ke topik SNS dengan ARN: *topic_arn_returned_in_API_response*.
3. Terapkan kembali konfigurasi notifikasi peristiwa FSx pada bucket S3 dengan menggunakan Amazon FSx CLI atau API, untuk menyegarkan sistem file `AutoImportPolicy`. Lakukan dengan perintah `update-file-system` CLI ([UpdateFileSystem](#) adalah tindakan API yang setara), sebagai berikut.

```
aws fsx update-file-system \  
--file-system-id fs-0123456789abcdef0 \  
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Pemecahan masalah penyimpanan

Pada beberapa kasus, Anda mungkin mengalami masalah penyimpanan dengan sistem file Anda. Anda dapat memecahkan masalah ini dengan menggunakan perintah `lfs`, seperti perintah `lfs migrate`.

Kesalahan tulis karena tidak ada ruang pada target penyimpanan

Anda dapat memeriksa penggunaan penyimpanan sistem file Anda dengan menggunakan perintah `lfs df -h`, seperti yang dijelaskan di [Layout penyimpanan sistem file](#). Bidang `filesystem_summary` melaporkan total penggunaan penyimpanan sistem file.

Jika penggunaan disk sistem file 100%, pertimbangkan untuk meningkatkan kapasitas penyimpanan sistem file Anda. Untuk informasi selengkapnya, lihat [Mengelola kapasitas penyimpanan](#).

Jika penggunaan penyimpanan sistem file tidak 100% dan Anda masih mendapatkan kesalahan menulis, file yang Anda tulis mungkin menjadi stripe pada OST yang penuh.

Tindakan yang harus diambil

- Jika sebagian besar OST Anda penuh, tingkatkan kapasitas penyimpanan sistem file Anda. Periksa penyimpanan yang tidak seimbang pada OST dengan mengikuti tindakan bagian [Penyimpanan tidak seimbang pada OST](#).
- Jika OST Anda tidak penuh, atur ukuran buffer halaman kotor klien dengan menerapkan penyetelan berikut ke semua instance klien Anda:

```
sudo lctl set_param osc.*.max_dirty_mb=64
```

Penyimpanan tidak seimbang pada OST

Amazon FSx for Lustre mendistribusikan stripe file baru secara merata di seluruh OST. Namun, sistem file Anda mungkin masih menjadi tidak seimbang karena pola I/O atau tata letak penyimpanan file. Akibatnya, beberapa target penyimpanan dapat menjadi penuh sementara yang lain tetap relatif kosong.

Anda menggunakan `lfs migrate` perintah untuk memindahkan file atau direktori dari OST yang lebih penuh ke kurang penuh. Anda dapat menggunakan `lfs migrate` perintah dalam mode blok atau non-blok.

- Mode blok adalah mode default untuk `lfs migrate` perintah. Saat dijalankan dalam mode blok, `lfs migrate` pertama-tama memperoleh kunci grup pada file dan direktori sebelum migrasi data untuk mencegah modifikasi pada file, lalu lepaskan kunci saat migrasi selesai. Dengan mencegah proses lain memodifikasi file, mode blok mencegah proses ini mengganggu migrasi. Kelemahannya adalah mencegah aplikasi memodifikasi file dapat mengakibatkan penundaan atau kesalahan untuk aplikasi.
- Mode non-blok diaktifkan untuk `lfs migrate` perintah dengan `-n` opsi. Saat berjalan `lfs migrate` dalam mode non-blok, proses lain masih dapat memodifikasi file yang sedang dimigrasikan. Jika proses memodifikasi file sebelum `lfs migrate` selesai memigrasinya, `lfs migrate` akan gagal memigrasikan file itu, meninggalkan file dengan tata letak garis aslinya.

Kami menyarankan Anda menggunakan mode non-blok, karena kecil kemungkinannya mengganggu aplikasi Anda.

Tindakan yang harus diambil

1. Luncurkan instance klien yang relatif besar (seperti jenis c5n.4xlarge instans Amazon EC2) untuk dipasang ke sistem file.
2. Sebelum menjalankan skrip mode non-blok pr skrip mode blok, pertama-tama jalankan perintah berikut pada setiap instance klien untuk mempercepat proses:

```
sudo lctl set_param 'mdc.*.max_rpcs_in_flight=60'
sudo lctl set_param 'mdc.*.max_mod_rpcs_in_flight=59'
```

3. Mulai sesi layar dan jalankan skrip mode non-blok atau skrip mode blok. Pastikan untuk mengubah variabel yang sesuai dalam skrip:

- Skrip mode non-blok:

```
#!/bin/bash

# UNCOMMENT THE FOLLOWING LINES:
#
# TRY_COUNT=0
# MAX_MIGRATE_ATTEMPTS=100
# OSTS="fsname-OST0000_UUID"
# DIR_OR_FILE_MIGRATED="/mnt/subdir/"
# BATCH_SIZE=10
# PARALLEL_JOBS=16 # up to max-procs processes, set to 16 if client is
# c5n.4xlarge with 16 vcpu
# LUSTRE_STRIPING_CONFIG="-E 100M -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32" #
# should be consistent with the existing striping setup
#

if [ -z "$TRY_COUNT" -o -z "$MAX_MIGRATE_ATTEMPTS" -o -z "$OSTS" -o -z
"$DIR_OR_FILE_MIGRATED" -o -z "$BATCH_SIZE" -o -z "$PARALLEL_JOBS" -o -z
"$LUSTRE_STRIPING_CONFIG" ]; then
    echo "Some variables are not set."
    exit 1
fi

echo "lfs migrate starts"
while true; do
    output=$(sudo lfs find ! -L released --ost $OSTS --print0
$DIR_OR_FILE_MIGRATED | shuf -z | /bin/xargs -0 -P $PARALLEL_JOBS -n $BATCH_SIZE
sudo lfs migrate -n $LUSTRE_STRIPING_CONFIG 2>&1)
    if [[ $? -eq 0 ]]; then
```

```

    echo "lfs migrate succeeds for $DIR_OR_FILE_MIGRATED at the $TRY_COUNT
attempt, exiting."
    exit 0
    elif [[ $? -eq 123 ]]; then
        echo "WARN: Target data objects are not located on these OSTs. Skipping
lfs migrate"
        exit 1
    else
        echo "lfs migrate fails for $DIR_OR_FILE_MIGRATED at the $TRY_COUNT
attempt, retrying..."
        if (( ++TRY_COUNT >= MAX_MIGRATE_ATTEMPTS )); then
            echo "WARN: Exceeds max retry attempt. Skipping lfs migrate for
$DIR_OR_FILE_MIGRATED. Failed with the following error"
            echo $output
            exit 1
        fi
    fi
done

```

- Skrip mode blok:
 - Ganti nilai OSTs dengan nilai OST Anda.
 - Berikan nilai integer nproc untuk mengatur jumlah proses max-procs untuk dijalankan secara paralel. Misalnya, jenis c5n.4xlarge instans Amazon EC2 memiliki 16 vCPU, sehingga Anda dapat menggunakan 16 (atau nilai < 16) untuk nproc
 - Berikan jalur direktori mount Anda dimnt_dir_path.

```

# find all OSTs with usage above a certain threshold; for example, greater than
or equal to 85% full
for OST in $(lfs df -h |egrep '( 8[5-9]| 9[0-9]|100)%'|cut -d' ' -f1); do echo
${OST};done|tr '\012' ','

# customer can also just pass OST values directly to OSTs variable
OSTS='dzfevbmV-OST0000_UUID,dzfevbmV-OST0002_UUID,dzfevbmV-OST0004_UUID,dzfevbmV-
OST0005_UUID,dzfevbmV-OST0006_UUID,dzfevbmV-OST0008_UUID'

nproc=<Run up to max-procs processes if client is c5n.4xlarge with 16 vcpu, this
value can be set to 16>

mnt_dir_path=<mount dir, e.g. '/my_mnt'>

```

```
lfs find ${mnt_dir_path} --ost ${OSTS}| xargs -P ${nproc} -n2 lfs migrate -E 100M  
-c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32
```

Catatan

- Jika Anda melihat bahwa ada dampak pada kinerja pembacaan sistem file, Anda dapat menghentikan migrasi kapan saja dengan menggunakan `ctrl-c` atau `kill -9`, dan mengurangi jumlah utas (`nproc`nilai) kembali ke angka yang lebih rendah (seperti 8), dan melanjutkan migrasi file.
- `lfs migrate`Perintah akan gagal pada file yang juga dibuka oleh beban kerja klien. Ini akan menimbulkan kesalahan dan pindah ke file berikutnya; oleh karena itu, dimungkinkan jika ada banyak file yang diakses, skrip tidak akan dapat memigrasi file apa pun, dan itu akan tercermin karena migrasi membuat kemajuan yang sangat lambat.
- Anda dapat memantau penggunaan OST menggunakan salah satu metode berikut
 - Pada pemasangan klien, jalankan perintah berikut untuk memantau penggunaan OST dan temukan OST dengan penggunaan lebih dari 85%:

```
lfs df -h |egrep '( 8[5-9]| 9[1-9]|100)%'
```

- Periksa CloudWatch metrik Amazon,OST FreeDataStorageCapacity, periksaMinimum. Jika skrip Anda menemukan OST yang lebih dari 85% penuh, maka ketika metrik mendekati 15%, gunakan `ctrl-c` atau `kill -9` untuk menghentikan migrasi.
- Anda juga dapat mempertimbangkan mengubah konfigurasi stripe sistem file atau direktori, sehingga file baru memiliki stripe di beberapa target penyimpanan. Untuk informasi lebih lanjut, lihat di [Sedang melakukan stripe data di sistem file Anda](#).

Memecahkan masalah driver FSx for Lustre CSI

Jika Anda mengalami masalah dengan driver FSx for Lustre CSI untuk container yang berjalan di Amazon EKS, [lihat Memecahkan Masalah Driver CSI \(Masalah Umum\)](#) yang tersedia di GitHub

Informasi tambahan

Bagian ini menyediakan support referensi, namun tidak lagi menggunakan fitur Amazon FSx.

Topik

- [Mengatur jadwal backup khusus](#)

Mengatur jadwal backup khusus

Kami merekomendasikan penggunaan AWS Backup untuk mengatur jadwal backup khusus untuk sistem file Anda. Informasi yang diberikan di sini adalah untuk tujuan referensi jika Anda perlu lebih sering menjadwalkan backup dari sebelumnya ketika menggunakan AWS Backup.

Ketika diaktifkan, Amazon FSx secara otomatis mengambil backup dari sistem file Anda sekali sehari selama backup windows harian. Amazon FSx memberlakukan periode penyimpanan yang Anda tentukan untuk backup otomatis ini. Ini juga mendukung backup yang diinisiasi pengguna, sehingga Anda dapat membuat backup kapan saja.

Berikut, Anda dapat menemukan sumber daya dan konfigurasi untuk men-deploy penjadwalan backup khusus. Penjadwalan backup kustom menampilkan backup yang diinisiasi pengguna pada sistem file Amazon FSx for Lustre pada jadwal backup yang sudah ditentukan. Contohnya mungkin sekali setiap enam jam, sekali setiap minggu, dan seterusnya. Penulisan ini juga mengkonfigurasi penghapusan backup yang lebih lama dari periode penyimpanan yang ditentukan.

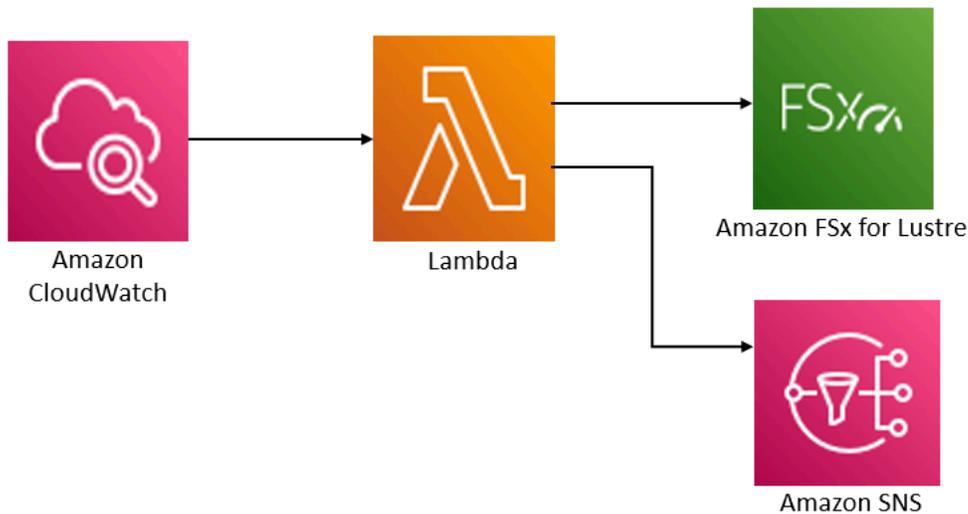
Solusi ini secara otomatis men-deploy semua komponen yang diperlukan, dan memerlukan parameter berikut:

- Sistem file
- Pola jadwal CRON untuk performa backup
- Periode retensi cadangan (dalam jumlah hari)
- Tanda nama backup

Untuk informasi selengkapnya tentang pola jadwal CRON, lihat [Ekspresi Jadwal untuk Aturan](#) di Panduan CloudWatch Pengguna Amazon.

Gambaran umum arsitektur

Men-deploy solusi ini untuk membangun sumber daya berikut di AWS Cloud.



Solusi ini dapat melakukan hal-hal berikut:

1. AWS CloudFormationTemplate menerapkan CloudWatch Peristiwa, fungsi Lambda, antrian Amazon SNS, dan peran IAM. IAM role memberikan izin fungsi Lambda untuk mengaktifkan operasi Amazon FSx for Lustre API.
2. CloudWatch Acara berjalan pada jadwal yang Anda tetapkan sebagai pola CRON, selama penerapan awal. Program ini mengaktifkan solusi pengelola backup fungsi Lambda yang dapat mengaktifkan Amazon FSx for Lustre CreateBackup Operasi API untuk memulai backup.
3. Pengelola backup mengambil daftar backup yang sudah ada yang diinisiasi pengguna untuk sistem file tertentu dengan menggunakan DescribeBackups. Jika kemudian menghapus backup yang lebih lama dari masa penyimpanan, yang Anda tentukan selama deployment awal.
4. Pengelola backup akan mengirimkan notifikasi olahpesan ke antrean Amazon SNS pada backup yang berhasil jika Anda memilih opsi untuk diberitahu selama deployment awal. Notifikasi selalu dikirim jika terjadi kegagalan.

AWS CloudFormation Templat

Solusi ini menggunakan AWS CloudFormation untuk mengotomatisasi deployment FSx Amazon FSx for Lustre untuk solusi penjadwalan backup khusus. Untuk menggunakan solusi ini, unduh [fsx-scheduled-backupAWS CloudFormationtemplate.template](#).

Otomatisasi deployment

Prosedur berikut mengkonfigurasi dan men-deploy solusi penjadwalan backup khusus ini. Dibutuhkan sekitar lima menit untuk men-deploy. Sebelum Anda mulai, Anda harus memiliki ID sistem file Amazon FSx for Lustre yang berfungsi di Amazon Virtual Private Cloud (Amazon VPC) pada akun Anda AWS . Untuk informasi lebih lanjut untuk membuat sumber daya ini, lihat [Memulai dengan Amazon FSx for Lustre](#).

Note

Menerapkan solusi ini dapat menyebabkan penagihan untuk layanan AWS yang dikaitkan. Untuk informasi lebih lanjut, lihat halaman detail harga untuk layanan tersebut.

Untuk meluncurkan tumpukan solusi backup khusus

1. Unduh [fsx-scheduled-backupAWS CloudFormationtemplate.template](#). Untuk informasi lebih lanjut tentang cara membuat tumpukan AWS CloudFormation, lihat [Membuat Tumpukan pada Konsol AWS CloudFormation](#) di Panduan Pengguna AWS CloudFormation.

Note

Secara default, templat ini diluncurkan di Wilayah AWS US East (N. Virginia). Amazon FSx for Lustre saat ini hanya tersedia secara khusus Wilayah AWS. Anda harus meluncurkan solusi ini dalam wilayah AWS di mana Amazon FSx for Lustre tersedia. Untuk informasi selengkapnya, lihat bagian Amazon FSx dari [Wilayah AWS dan Titik Akhir](#) 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
Sistem ID file Amazon FSx for Lustre	Tidak ada nilai default	Sistem ID file untuk sistem file yang ingin Anda backup.
Pola jadwal CRON untuk backup.	0 0/4 * * ? *	Jadwal untuk menjalankan CloudWatch acara,

Parameter	Default	Deskripsi
		memicu cadangan baru dan menghapus cadangan lama di luar periode retensi.
Penyimpanan Backup (dalam hari)	7	Beberapa hari untuk menyimpan backup yang diinisiasi pengguna. Fungsi Lambda menghapus backup yang diinisiasi pengguna yang telah dibuat sejak lama.
Nama untuk backup	Backup terjadwal pengguna	Nama untuk backup ini, yang muncul di Nama Backup ialah kolom konsol manajemen Amazon FSx for Lustre.
Notifikasi Backup	Ya	Pilih apakah akan diberitahu ketika inisiasi backup berhasil. Notifikasi selalu dikirim jika terjadi kesalahan.
Alamat Email	Tidak ada nilai default	Alamat email untuk berlangganan dengan notifikasi SNS.

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 pada konsol AWS CloudFormation pada kolom Status. Anda dapat melihat status CREATE_COMPLETE dalam waktu sekitar lima menit.

Opsi tambahan

Anda dapat menggunakan fungsi Lambda yang dibuat oleh solusi ini untuk melakukan backup terjadwal khusus lebih dari satu sistem file Amazon FSx for Lustre. ID sistem file diteruskan ke fungsi Amazon FSx for Lustre di JSON input untuk acara tersebut. CloudWatch JSON default yang diteruskan ke fungsi Lambda adalah sebagai berikut, saat nilai untuk `FileSystemId` dan `SuccessNotification` diteruskan dari parameter yang ditentukan saat meluncurkan tumpukan AWS CloudFormation.

```
{
  "start-backup": "true",
  "purge-backups": "true",
  "filesystem-id": "${FileSystemId}",
  "notify_on_success": "${SuccessNotification}"
}
```

Untuk menjadwalkan pencadangan untuk sistem file Amazon FSx for Lustre tambahan, buat aturan acara lain. CloudWatch Anda melakukannya dengan menggunakan sumber jadwal acara, dengan fungsi Lambda yang dibuat oleh solusi ini sebagai target. Pilih (teks JSON) konstan lalu pilih input konfigurasi. Untuk input JSON, cukup ganti ID sistem file Amazon FSx for Lustre untuk backup di tempat `${FileSystemId}`. Juga, ganti baik Yes atau No di tempat `${SuccessNotification}` di atas JSON.

Aturan CloudWatch Peristiwa tambahan apa pun yang Anda buat secara manual bukan merupakan bagian dari tumpukan solusi pencadangan terjadwal kustom Amazon fsX for Lustre. AWS CloudFormation Dengan demikian, mereka tidak dihapus jika Anda menghapus tumpukan.

Riwayat dokumen

- Versi API: 2018-03-01
- Pembaruan dokumentasi terbaru: 6 Juni 2024

Tabel berikut menjelaskan perubahan penting pada Panduan Pengguna Amazon FSx for Lustre. Untuk notifikasi tentang pembaruan dokumentasi, Anda dapat berlangganan ke umpan RSS.

Perubahan	Deskripsi	Tanggal
Support ditambahkan untuk meningkatkan kinerja metadata	Anda sekarang dapat membuat sistem file FSx for Lustre Persistent_2 dengan konfigurasi metadata yang menyediakan kemampuan untuk meningkatkan kinerja metadata. Untuk informasi selengkapnya, lihat Kinerja metadata sistem file dan Mengelola kinerja metadata .	Juni 6, 2024
Wilayah AWS Dukungan tambahan ditambahkan untuk jenis penyebaran Persistent_2	Persistent_2 SSD FSx untuk sistem file Lustre sekarang tersedia di Zona Lokal AS Timur (Atlanta). Untuk informasi selengkapnya, lihat Wilayah yang tersedia .	29 Mei 2024
Dukungan klien Lustre untuk CentOS, Rocky Linux, dan Red Hat Enterprise Linux (RHEL) 9.4 ditambahkan	Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS, Rocky Linux, dan Red Hat Enterprise Linux (RHEL) 9.4. Untuk informasi selengkapnya, lihat Menginstall Lustre client .	16 Mei 2024

Wilayah AWS Dukungan tambahan ditambahkan untuk jenis penyebaran Persistent_2	Persistent_2 SSD FSx untuk sistem file Lustre sekarang tersedia di Kanada Barat (Calgary). Wilayah AWS Untuk informasi selengkapnya, lihat Wilayah yang tersedia .	3 Mei 2024
Dukungan klien Lustre untuk Amazon Linux 2023 ditambahkan	Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan Amazon Linux 2023. Untuk informasi selengkapnya, lihat Menginstal Lustre client .	Maret 25, 2024
Dukungan klien Lustre untuk CentOS, Rocky Linux, dan Red Hat Enterprise Linux (RHEL) 8.9 ditambahkan	Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS, Rocky Linux, dan Red Hat Enterprise Linux (RHEL) 8.9. Untuk informasi selengkapnya, lihat Menginstal Lustre client .	Januari 9, 2024
Amazon FSx memperbarui kebijakan terkelola AmazonFSxFull Access, AmazonF, AmazonF, AmazonF Access SxConsoleFullAccess, dan AmazonF SxRead OnlyAccess SxConsole ReadOnly SxService RolePolicy AWS	Amazon FSx memperbarui kebijakan AmazonFSxFull Access, AmazonF, AmazonF, AmazonF Access SxConsole FullAccess, dan SxConsole ReadOnly AmazonF SxRead OnlyAccess untuk menambahkan izin. SxService RolePolicy ec2:GetSecurityGroupsForVpc Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola .	Januari 9, 2024

[Dukungan klien Lustre untuk CentOS, Rocky Linux, dan Red Hat Enterprise Linux \(RHEL\) 9.0 dan 9.3 ditambahkan](#)

Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS, Rocky Linux, dan Red Hat Enterprise Linux (RHEL) 9.0 dan 9.3. Untuk informasi selengkapnya, lihat [Menginstal Lustre client](#).

20 Desember 2023

[Amazon FSx untuk Lustre memperbarui SxFullAccess kebijakan terkelola AmazonF dan AmazonF SxConsole FullAccess AWS](#)

Amazon FSx memperbarui kebijakan AmazonF SxFullAccess dan AmazonF SxConsole FullAccess untuk menambahkan tindakan. ManageCrossAccountDataReplication Untuk informasi selengkapnya, lihat [Amazon FSx memperbarui kebijakan AWS terkelola](#).

20 Desember 2023

[Amazon FSx memperbarui kebijakan terkelola AmazonF SxFullAccess dan AmazonF SxConsole FullAccess AWS](#)

Amazon FSx memperbarui kebijakan AmazonF SxFullAccess dan AmazonF SxConsoleFullAccess untuk menambahkan izin. fsx:CopySnapshotAndUpdateVolume Untuk informasi selengkapnya, lihat [Amazon FSx memperbarui kebijakan AWS terkelola](#).

26 November 2023

[Support ditambahkan untuk penskalaan kapasitas throughput](#)

Anda sekarang dapat memodifikasi kapasitas throughput untuk sistem file berbasis SSD persisten FSx for Lustre yang ada saat persyaratan throughput Anda berkembang. Untuk informasi selengkapnya, lihat [Mengelola kapasitas throughput](#).

16 November 2023

[Amazon FSx memperbarui kebijakan terkelola AmazonFSxFullAccess dan AmazonFSxConsole FullAccess AWS](#)

Amazon FSx memperbarui SxConsoleFullAccess kebijakan AmazonF dan AmazonF untuk menambahkan SxFullAccess dan izin. fsx:DescribeSharedVPCConfiguration fsx:UpdateSharedVPCConfiguration Untuk informasi selengkapnya, lihat [Amazon FSx memperbarui kebijakan AWS terkelola](#).

14 November 2023

[Support ditambahkan untuk kuota proyek](#)

Anda sekarang dapat membuat kuota penyimpanan untuk proyek. Kuota proyek berlaku untuk semua file atau direktori yang terkait dengan proyek. Untuk informasi lebih lanjut, lihat [Kuota Penyimpanan](#).

29 Agustus 2023

Support ditambahkan untuk Lustre versi 2.15	Semua sistem file FSx for Lustre sekarang dibangun di atas Lustre versi 2.15 saat dibuat menggunakan konsol Amazon FSx. Untuk informasi selengkapnya, lihat Langkah 1: Membuat sistem file Amazon FSx for Lustre .	29 Agustus 2023
Wilayah AWS Dukungan tambahan ditambahkan untuk jenis penyebaran Persistent_2	Persistent_2 FSx untuk sistem file Lustre sekarang tersedia di Israel (Tel Aviv). Wilayah AWS Untuk informasi selengkapnya, lihat Opsi penerapan untuk sistem file FSx for Lustre .	24 Agustus 2023
Support ditambahkan untuk tugas repositori data rilis	FSx for Lustre sekarang menyediakan tugas repositori data rilis untuk merilis file yang diarsipkan dari sistem file yang ditautkan ke repositori data S3. Melepaskan file akan mempertahankan daftar file dan metadata, tetapi menghapus salinan lokal dari isi file tersebut. Untuk informasi selengkapnya, lihat Menggunakan tugas repositori data untuk merilis file .	9 Agustus 2023
Amazon FSx memperbarui kebijakan terkelola SxService RolePolicy AWS AmazonF	Amazon FSx memperbarui <code>cloudwatch:PutMetricData</code> izin di AmazonFSxService RolePolicy Untuk informasi selengkapnya, lihat Amazon FSx memperbarui kebijakan AWS terkelola .	Juli 24, 2023

Amazon FSx memperbarui kebijakan terkelola SxFull AmazonF Access AWS	Amazon FSx memperbarui SxFullAccess kebijakan AmazonF untuk menghapus <code>fsx:*</code> izin dan menambahkan tindakan tertentu. <code>fsx</code> Untuk informasi selengkapnya, lihat kebijakan SxFull Akses AmazonF .	13 Juli 2023
Amazon FSx memperbarui kebijakan terkelola SxConsole FullAccess AWS AmazonF	Amazon FSx memperbarui SxConsoleFullAccess kebijakan AmazonF untuk menghapus <code>fsx:*</code> izin dan menambahkan tindakan tertentu. <code>fsx</code> Untuk informasi selengkapnya, lihat kebijakan AmazonF SxConsole FullAccess .	13 Juli 2023
Dukungan klien Lustre untuk CentOS, Rocky Linux, dan Red Hat Enterprise Linux (RHEL) 8.8 ditambahkan	Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS, Rocky Linux, dan Red Hat Enterprise Linux (RHEL) 8.8. Untuk informasi selengkapnya, lihat Menginstall Lustre client .	25 Mei 2023

[Support ditambahkan untuk AutoImport dan AutoExport metrik](#)

FSx for Lustre sekarang CloudWatch menyediakan metrik Amazon yang memantau impor otomatis dan pembaruan ekspor otomatis untuk sistem file yang ditautkan ke repositori data. Untuk informasi selengkapnya, lihat [Memantau dengan Amazon CloudWatch](#).

31 Maret 2023

[Dukungan DRA untuk jenis penerapan Persistent_1 dan Scratch_2 ditambahkan](#)

Anda sekarang dapat membuat asosiasi repositori data untuk menautkan repositori data ke sistem file Lustre 2.12 dengan jenis penyebaran Persistent_1 atau Scratch_2. Untuk informasi selengkapnya, lihat [Menggunakan repositori data dengan Amazon FSx for Lustre](#).

29 Maret 2023

[Dukungan klien Lustre untuk CentOS, Rocky Linux, dan Red Hat Enterprise Linux \(RHEL\) 8.7 ditambahkan](#)

Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS, Rocky Linux, dan Red Hat Enterprise Linux (RHEL) 8.7. Untuk informasi selengkapnya, lihat [Menginstall Lustre client](#).

Desember 5, 2022

Wilayah AWS Dukungan tambahan ditambahkan untuk jenis penyebaran Persistent_2	Sistem file Persistent_2 SSD FSx for Lustre generasi berikutnya sekarang tersedia di Eropa (Stockholm), Asia Pasifik (Hong Kong), Asia Pasifik (Mumbai), dan Asia Pasifik (Seoul). Wilayah AWS Untuk informasi selengkapnya, lihat Opsi penerapan untuk sistem file FSx for Lustre .	10 November 2022
Dukungan klien Lustre untuk CentOS, Rocky Linux, dan Red Hat Enterprise Linux (RHEL) 8.6 ditambahkan	Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS, Rocky Linux, dan Red Hat Enterprise Linux (RHEL) 8.6. Untuk informasi selengkapnya, lihat Menginstall Lustre client .	8 September 2022
Dukungan klien Lustre untuk Ubuntu 22 ditambahkan	Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan Ubuntu 22.04. Untuk informasi selengkapnya, lihat Menginstall Lustre client .	28 Juli 2022
Dukungan klien Lustre untuk Rocky Linux ditambahkan	Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan Rocky Linux. Untuk informasi selengkapnya, lihat Menginstall Lustre client .	8 Juli 2022

[Support ditambahkan untuk Lustre root squash](#)

Anda sekarang dapat menggunakan fitur Lustre root squash untuk membatasi akses tingkat root dari klien yang mencoba mengakses sistem file FSx for Lustre Anda sebagai root. Untuk informasi lebih lanjut, lihat [Lustre root squash](#).

25 Mei 2022

[Wilayah AWS Dukungan tambahan ditambahkan untuk jenis penyebaran Persistent_2](#)

Sistem file Persistent_2 SSD FSx for Lustre generasi berikutnya sekarang tersedia di Eropa (London), Asia Pasifik (Singapura), dan Asia Pasifik (Sydney). Wilayah AWS Untuk informasi selengkapnya, lihat [Opsi penerapan untuk sistem file FSx for Lustre](#).

19 April 2022

[Support ditambahkan untuk digunakan AWS DataSync untuk memigrasikan file ke sistem file Amazon FSx for Lustre Anda.](#)

Anda sekarang dapat menggunakan AWS DataSync untuk memigrasikan file dari sistem file yang ada ke FSx for Lustre file systems. Untuk informasi selengkapnya, lihat [Cara memigrasi file yang ada ke FSx for Lustre menggunakan](#) [an](#). AWS DataSync

5 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 titik akhir VPC antarmuka](#).

5 April 2022

[Support ditambahkan untuk antrian Lustre DRA](#)

Anda sekarang dapat membuat DRA (asosiasi repositori data) ketika Anda membuat sistem file FSx for Lustre. Permintaan akan antri dan DRA akan dibuat setelah sistem file tersedia. Untuk informasi selengkapnya, lihat [Menautkan sistem file ke bucket S3](#).

28 Februari 2022

[Dukungan klien Lustre untuk CentOS dan Red Hat Enterprise Linux \(RHEL\) 8.5 ditambahkan](#)

Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS dan Red Hat Enterprise Linux (RHEL) 8.5. Untuk informasi selengkapnya, lihat [Menginstal Lustre client](#).

Desember 20, 2021

[Support untuk mengekspor perubahan dari FSx for Lustre ke repositori data tertaut](#)

Anda sekarang dapat mengonfigurasi FSx for Lustre untuk secara otomatis mengekspor file baru, diubah, dan dihapus dari sistem file Anda ke repositori data Amazon S3 yang ditautkan. Anda dapat menggunakan tugas repositori data untuk mengekspor data dan perubahan metadata ke repositori data. Anda juga dapat mengonfigurasi tautan ke beberapa repositori data. Untuk informasi selengkapnya, lihat [Mengekspor perubahan ke repositori data](#).

30 November 2021

[Support ditambahkan untuk pencatatan Lustre](#)

Anda sekarang dapat mengonfigurasi FSx for Lustre untuk mencatat kesalahan dan peringatan peristiwa untuk repositori data yang terkait dengan sistem file Anda ke Amazon Logs. CloudWatch Untuk informasi selengkapnya, lihat [Logging dengan Amazon CloudWatch Logs](#).

30 November 2021

[Sistem file SSD persisten mendukung throughput yang lebih tinggi dan kapasitas penyimpanan yang lebih kecil](#)

SSD Persisten generasi berikutnya FSx for Lustre file systems memiliki opsi throughput yang lebih tinggi dan memiliki kapasitas penyimpanan minimum yang lebih rendah. Untuk informasi selengkapnya, lihat [Opsi penerapan untuk sistem file FSx for Lustre](#).

30 November 2021

[Support ditambahkan untuk Lustre versi 2.12](#)

Anda sekarang dapat memilih Lustre versi 2.12 ketika Anda membuat sistem file FSx for Lustre. Untuk informasi selengkapnya, lihat [Langkah 1: Membuat sistem file Amazon FSx for Lustre](#).

5 Oktober 2021

[Dukungan klien Lustre untuk CentOS dan Red Hat Enterprise Linux \(RHEL\) 8.4 ditambahkan](#)

Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS dan Red Hat Enterprise Linux (RHEL) 8.4. Untuk informasi selengkapnya, lihat [Menginstal Lustre client](#).

9 Juni 2021

[Support ditambahkan untuk kompresi data](#)

Anda sekarang dapat mengaktifkan kompresi data ketika Anda membuat sistem file FSx for Lustre. Anda juga dapat mengaktifkan atau menonaktifkan kompresi data pada sistem file FSx for Lustre yang ada. Untuk informasi selengkapnya, lihat [kompresi data Lustre](#).

27 Mei 2021

[Support ditambahkan untuk menyalin backup](#)

Anda sekarang dapat menggunakan Amazon FSx untuk menyalin cadangan dalam hal yang sama Akun AWS ke yang lain Wilayah AWS (salinan lintas wilayah) atau dalam yang sama Wilayah AWS (Salinan dalam wilayah). Untuk informasi selengkapnya, lihat [Menyalin cadangan](#).

12 April 2021

[Dukungan klien Lustre untuk kumpulan file Lustre](#)

Klien FSx for Lustre sekarang mendukung penggunaan filesets untuk me-mount hanya subset dari namespace sistem file. Untuk informasi selengkapnya, lihat [Memasang Fileset Spesifik](#).

18 Maret 2021

[Support ditambahkan untuk akses klien menggunakan alamat IP non-pribadi](#)

Anda dapat mengakses sistem file FSx for Lustre dari klien lokal menggunakan alamat IP non-pribadi. Untuk informasi selengkapnya, lihat [Memasang sistem file Amazon FSx dari lokal atau VPC Amazon yang diintip](#).

17 Desember 2020

[Dukungan klien Lustre untuk CentOS 7.9 berbasis ARM ditambahkan](#)

Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS 7.9 berbasis ARM. Untuk informasi selengkapnya, lihat [Menginstal Lustre client](#).

17 Desember 2020

Dukungan klien Lustre untuk CentOS dan Red Hat Enterprise Linux (RHEL) 8.3 ditambahkan	Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS dan Red Hat Enterprise Linux (RHEL) 8.3. Untuk informasi selengkapnya, lihat Menginstal Lustre client .	16 Desember 2020
Support ditambahkan untuk penskalaan kapasitas penyimpanan dan throughput	Anda sekarang dapat meningkatkan kapasitas penyimpanan dan throughput untuk sistem file FSx for Lustre yang ada saat ini seiring dengan berkembangnya kebutuhan penyimpanan dan throughput Anda. Untuk informasi selengkapnya, lihat Mengelola kapasitas penyimpanan dan throughput .	24 November 2020
Support ditambahkan untuk kuota penyimpanan	Sekarang Anda dapat membuat kuota penyimpanan untuk pengguna dan grup. Kuota penyimpanan membatasi jumlah ruang disk dan jumlah file yang dapat dikonsumsi pengguna atau grup pada sistem file FSx for Lustre Anda. Untuk informasi lebih lanjut, lihat Kuota Penyimpanan .	9 November 2020

[Amazon FSx sekarang terintegrasi dengan AWS Backup](#)

Anda sekarang dapat menggunakan AWS Backup untuk mencadangkan dan memulihkan sistem file FSx Anda selain menggunakan cadangan Amazon FSx asli. Untuk informasi selengkapnya, lihat [Menggunakan AWS Backup dengan Amazon FSx](#).

9 November 2020

[Support ditambahkan untuk opsi penyimpanan HDD \(hard disk drive\)](#)

Selain opsi penyimpanan SSD (solid state drive), FSx for Lustre sekarang mendukung opsi penyimpanan HDD (hard disk drive). Anda dapat mengonfigurasi sistem file Anda untuk menggunakan HDD untuk beban kerja intensif throughput yang biasanya memiliki operasi file berurutan yang berukuran Large. Untuk informasi selengkapnya, lihat [Ragam Pilihan Penyimpanan](#).

12 Agustus 2020

[Support untuk mengimpor perubahan repositori data tertaut ke FSx for Lustre](#)

Anda sekarang dapat mengkonfigurasi sistem file FSx for Lustre Anda untuk secara otomatis mengimpor file baru yang ditambahkan ke dan file yang telah berubah dalam repositori data tertaut setelah pembuatan sistem file. Untuk informasi selengkapnya, lihat [mengimpor pembaruan secara otomatis dari repositori data](#).

23 Juli 2020

[Lustre dukungan klien untuk SUSE Linux SP4 dan SP5 ditambahkan](#)

Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan SUSE Linux SP4 dan SP5. Untuk informasi selengkapnya, lihat [Menginstal Lustre client](#).

20 Juli 2020

[Dukungan klien Lustre untuk CentOS dan Red Hat Enterprise Linux \(RHEL\) 8.2 ditambahkan](#)

Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan CentOS dan Red Hat Enterprise Linux (RHEL) 8.2. Untuk informasi selengkapnya, lihat [Menginstal Lustre client](#).

20 Juli 2020

[Support untuk backup sistem file otomatis dan manual ditambahkan](#)

Anda sekarang dapat melakukan backup harian otomatis dan backup manual dari sistem file yang tidak tertaut ke repositori data tahan lama Amazon S3. Untuk informasi lebih lanjut, lihat [Bekerja dengan backup](#).

23 Juni 2020

[Dua jenis penyebaran sistem file baru dirilis](#)

Scratch sistem file dirancang untuk penyimpanan sementara dan pemrosesan data jangka pendek. Sistem file yang persisten dirancang untuk penyimpanan dan beban kerja jangka panjang. Untuk informasi selengkapnya, lihat [Opsi Deployment FSx for Lustre](#).

12 Februari 2020

[Support untuk metadata POSIX ditambahkan](#)

FSx for Lustre mempertahankan metadata POSIX terkait saat mengimpor dan mengekspor file ke repositori data tahan lama yang ditautkan di Amazon S3. Untuk informasi selengkapnya, lihat [Dukungan metadata POSIX untuk repositori data](#).

23 Desember 2019

[Fitur tugas repositori data baru dirilis](#)

Anda sekarang dapat mengekspor data yang berubah dan metadata POSIX yang ter-associate ke repositori data tahan lama tertaut di Amazon S3 menggunakan fitur tugas repositori data. Untuk informasi selengkapnya, lihat [Mentransfer Data & Metadata Menggunakan Fitur Tugas Repositori Data](#).

23 Desember 2019

Wilayah AWS Dukungan tambahan ditambahkan	FSx for Lustre sekarang tersedia di Wilayah Eropa (London). Wilayah AWS Untuk batas spesifik wilayah FSx for Lustre, lihat Batas.	9 Juli 2019
Wilayah AWS Dukungan tambahan ditambahkan	FSx for Lustre sekarang tersedia di Asia Pasifik (Singapura). Wilayah AWS Untuk batas spesifik wilayah FSx for Lustre, lihat Batas.	26 Juni 2019
Dukungan klien Lustre untuk Amazon Linux dan Amazon Linux 2 ditambahkan	Klien FSx for Lustre sekarang mendukung instans Amazon EC2 yang menjalankan Amazon Linux dan Amazon Linux 2. Untuk informasi selengkapnya, lihat Menginstall Lustre client.	11 Maret 2019
Dukungan jalur ekspor data yang ditentukan pengguna ditambahkan	Para pengguna sekarang memiliki pilihan untuk melakukan overwrite objek asli di bucket Amazon S3 Anda atau tulis file baru atau file yang diubah ke prefiks yang Anda tentukan. Dengan opsi ini, Anda memiliki fleksibilitas tambahan untuk memasukkan FSx for Lustre ke dalam alur kerja pemrosesan data Anda. Untuk informasi lebih lanjut, lihat Mengekspor data ke Bucket Amazon S3 Anda.	6 Februari 2019

[Total batas default penyimpanan meningkat](#)

Total penyimpanan default untuk semua sistem file FSx for Lustre meningkat menjadi 100.800 GiB. Untuk informasi selengkapnya, lihat [Batasan-batasan](#).

11 Januari 2019

[Amazon FSx for Lustre sekarang tersedia secara umum](#)

Amazon FSx for Lustre adalah sistem file yang dikelola penuh yang dioptimalkan untuk beban kerja komputasi intensif, seperti komputasi performa tinggi, machine learning, dan alur kerja pemrosesan media.

28 November, 2018

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