



Lustre-Benutzerhandbuch

FSx für Lustre



FSx für Lustre: Lustre-Benutzerhandbuch

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Die Handelsmarken und Handelsaufmachung von Amazon dürfen nicht in einer Weise in Verbindung mit nicht von Amazon stammenden Produkten oder Services verwendet werden, durch die Kunden irregeführt werden könnten oder Amazon in schlechtem Licht dargestellt oder diskreditiert werden könnte. Alle anderen Handelsmarken, die nicht Eigentum von Amazon sind, gehören den jeweiligen Besitzern, die möglicherweise zu Amazon gehören oder nicht, mit Amazon verbunden sind oder von Amazon gesponsert werden.

Table of Contents

Was ist Amazon FSx for Lustre?	1
Mehrere Bereitstellungsoptionen	2
Mehrere Speicheroptionen	2
FSx for Lustre und Datenrepositorien	3
FSx for Lustre S3-Datenrepository-Integration	3
FSx for Lustre und lokale Datenrepositorien	3
Zugreifen auf Dateisysteme	3
Integrationen mit Diensten AWS	4
Sicherheits und Compliance	5
Annahmen	5
Preise für Amazon FSx for Lustre	6
Foren zu Amazon FSx for Lustre	6
Verwenden Sie Amazon FSx for Lustre zum ersten Mal?	6
Einrichtung	7
Bei Amazon Web Services registrieren	7
Melde dich an für eine AWS-Konto	7
Erstellen Sie einen Benutzer mit Administratorzugriff	8
Hinzufügen von Berechtigungen zur Verwendung von Datenrepositorys in Amazon S3	9
Wie FSx for Lustre den Zugriff auf S3-Buckets überprüft	11
Nächster Schritt	12
Erste Schritte	13
Voraussetzungen	13
Erstellen Sie Ihr FSx for Lustre-Dateisystem	14
Installieren Sie den Lustre-Client	20
Hängen Sie das Dateisystem ein	21
Führen Sie Ihren Workflow aus	23
Bereinigen von -Ressourcen	23
Bereitstellungsoptionen für das Dateisystem	25
Optionen für die Bereitstellung	25
Scratch-Dateisysteme	26
Persistente Dateisysteme	27
Bereitstellungstyp Persistent_2	27
Bereitstellungstyp Persistent_1	28
Verfügbare Regionen	28

Verwenden von Datenrepositorys	31
Überblick über Datenrepositorien	31
Unterstützung für POSIX-Metadaten	33
Harte Links und Export nach S3	35
Anhängen von POSIX-Berechtigungen an einen S3-Bucket	36
Ihr Dateisystem mit einem S3-Bucket verknüpfen	39
Regions- und Kontounterstützung für verknüpfte S3-Buckets	42
Einen Link zu einem S3-Bucket erstellen	42
Arbeiten mit serverseitig verschlüsselten Amazon S3 S3-Buckets	52
Änderungen aus Ihrem Daten-Repository importieren	55
Automatisches Importieren von Updates aus Ihrem S3-Bucket	56
Verwenden von Datenrepository-Aufgaben zum Importieren von Änderungen	62
Vorladen von Dateien in Ihr Dateisystem	64
Änderungen in das Daten-Repository exportieren	65
Exportieren Sie Updates automatisch in Ihren S3-Bucket	67
Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen	70
Exportieren von Dateien mithilfe von HSM-Befehlen	73
Aufgaben im Datenarchiv	74
Arten von Datenrepository-Aufgaben	75
Status und Details der Aufgabe	76
Verwenden von Datenrepository-Aufgaben	77
Arbeiten mit Berichten über den Abschluss von Aufgaben	85
Behebung von Fehlern bei Aufgaben	86
Dateien werden freigegeben	91
Verwenden von Datenrepository-Aufgaben zur Freigabe von Dateien	93
Amazon FSx mit Ihren lokalen Daten verwenden	97
Ereignisprotokolle des Datenrepositorys	97
Mit älteren Bereitstellungstypen arbeiten	117
Verknüpfen Sie Ihr Dateisystem mit einem Amazon S3-Bucket	118
Automatisches Importieren von Updates aus Ihrem S3-Bucket	127
Leistung	132
So funktionieren FSx for Lustre-Dateisysteme	132
Aggregierte Dateisystemleistung	133
Beispiel: Aggregierter Baseline- und Burst-Durchsatz	138
Leistung der Metadaten des Dateisystems	138
Speicherlayout des Dateisystems	140

Daten in Ihrem Dateisystem entfernen	140
Ändern Sie Ihre Striping-Konfiguration	141
Progressive Datei-Layouts	143
Überwachung von Leistung und Nutzung	145
Tipps zur Leistung	145
Zugreifen auf Dateisysteme	148
Kompatibilität des Lustre-Dateisystems und des Client-Kernels	148
Den Lustre-Client installieren	152
Amazon Linux	152
CentOS, Rocky Linux und Red Hat	155
Ubuntu	166
SUSE Linux	172
Von Amazon EC2 aus montieren	175
Montage von Amazon ECS	177
Mounten von einer Amazon EC2 EC2-Instance aus, die Amazon ECS-Aufgaben hostet	178
Mounten aus einem Docker-Container	179
Mounten von einer lokalen oder einer anderen VPC	180
Automatisches Mounten von Amazon FSx	182
Automatisches Mounten mit /etc/fstab	182
Mounten bestimmter Dateisätze	185
Aufheben des Mountings von Dateisystemen	186
Verwendung von EC2-Spot-Instances	187
Umgang mit Amazon EC2-Spot-Instance-Unterbrechungen	188
Verwaltung von Dateisystemen	191
Sicherungen	191
Backup-Unterstützung in FSx for Lustre	193
Arbeiten mit automatischen täglichen Backups	193
Arbeiten mit vom Benutzer initiierten Backups	194
Verwendung AWS Backup mit Amazon FSx	195
Kopieren eines Backups	196
Backups werden innerhalb derselben Datei kopiert AWS-Konto	198
Backups wiederherstellen	200
Löschen eines Backups	201
Speicherkontingente	201
Durchsetzung von Kontingenten	202
Arten von Kontingenten	202

Kontingentgrenzen und Übergangsfristen	203
Kontingente festlegen und anzeigen	204
Kontingente und mit Amazon S3 verknüpfte Buckets	208
Kontingente und Wiederherstellung von Backups	209
Speicherkapazität	209
Überlegungen zur Erhöhung der Speicherkapazität	210
Wann sollte die Speicherkapazität erhöht werden	211
Wie werden gleichzeitige Speicherskalierungs- und Backup-Anfragen behandelt	212
Wie erhöht man die Speicherkapazität	212
Überwachung: Die Speicherkapazität steigt	214
Die Leistung von Metadaten verwalten	218
Leistungskonfiguration für Lustre-Metadaten	219
Überlegungen zur Steigerung der Metadaten-Performance	220
Wann sollte die Leistung von Metadaten erhöht werden	220
Wie kann die Leistung von Metadaten gesteigert werden	221
Ändern des Metadaten-Konfigurationsmodus	222
Überwachung von Aktualisierungen der Metadaten-Konfiguration	224
Durchsatzkapazität	226
Überlegungen zur Aktualisierung der Durchsatzkapazität	227
Wann muss die Durchsatzkapazität geändert werden	227
Wie ändert man die Durchsatzkapazität	228
Überwachung von Änderungen der Durchsatzkapazität	229
Datenkompression	231
Verwaltung der Datenkomprimierung	233
Komprimieren zuvor geschriebener Dateien	236
Dateigrößen anzeigen	236
Metriken verwenden CloudWatch	237
Wurzelkürbis	237
Wie funktioniert Root Squash	238
Root Squash verwalten	239
Status des Dateisystems	245
Markieren Ihrer -Ressourcen mit Tags (Markierungen)	245
Grundlagen zu Tags (Markierungen)	246
Markieren Ihrer -Ressourcen	247
Tag-Einschränkungen	247
Berechtigungen und Tag	248

Wartung	248
Löschen eines Dateisystems	250
Migration zu FSx for Lustre mit DataSync	251
Migrieren von Dateien mit AWS DataSync	251
Voraussetzungen	251
DataSync grundlegende Schritte zur Migration	252
Dateisysteme überwachen	253
Überwachung mit CloudWatch	253
Metriken des Dateisystems	254
Metriken für Metadaten des Dateisystems	261
AutoImport AutoExport und Metriken	264
Abmessungen von Amazon FSx for Lustre	266
So verwenden Sie Amazon FSx for Lustre-Metriken	267
Zugriff auf CloudWatch Metriken	268
Erstellen von Alarmen	269
Protokollierung mit CloudWatch Protokollen	271
Überblick über die Protokollierung	271
Ziele protokollieren	272
Verwaltung der Protokollierung	273
Anzeigen von -Protokollen	275
Protokollierung mit AWS CloudTrail	275
Informationen zu Amazon FSx for Lustre in CloudTrail	276
Grundlegendes zu Amazon FSx for Lustre-Protokolldateieinträgen	277
Sicherheit	280
Datenschutz	281
Datenverschlüsselung	282
Richtlinie für den Datenverkehr zwischen Netzwerken	287
Identity and Access Management	288
Zielgruppe	288
Authentifizierung mit Identitäten	289
Verwalten des Zugriffs mit Richtlinien	293
FSx for Lustre und IAM	296
Beispiele für identitätsbasierte Richtlinien	303
AWS verwaltete Richtlinien	306
Fehlerbehebung	321
Verwenden von Tags mit Amazon FSx	323

Verwenden von serviceverknüpften Rollen	329
Zugriffskontrolle für Dateisysteme mit Amazon VPC	336
Amazon VPC-Sicherheitsgruppen	337
VPC-Sicherheitsgruppenregeln für Lustre-Clients	342
Amazon VPC-Netzwerk-ACLs	345
Compliance-Validierung	345
Schnittstellen-VPC-Endpunkte	347
Überlegungen zu VPC-Endpunkten mit Amazon FSx-Schnittstelle	347
Erstellen eines VPC-Schnittstellen-Endpunkts für Amazon FSx API	348
Erstellen einer VPC-Endpunktrichtlinie für Amazon FSx	349
Kontingente	350
Kontingente, die Sie erhöhen können	350
Ressourcenkontingente für jedes Dateisystem	352
Weitere Überlegungen	353
Fehlerbehebung	354
Das Erstellen eines Dateisystems schlägt fehl	354
Aufgrund einer falsch konfigurierten Sicherheitsgruppe kann kein Dateisystem erstellt werden	354
Es kann kein Dateisystem erstellt werden, das mit einem S3-Bucket verknüpft ist	355
Das Einhängen des Dateisystems schlägt fehl	355
Das Einhängen des Dateisystems schlägt sofort fehl	356
Das Mounting des Dateisystems hängt und schlägt dann mit einem Timeout-Fehler fehl	356
Automatisches Mounting schlägt fehl und die Instance reagiert nicht	356
Das Einhängen des Dateisystems schlägt beim Systemstart fehl	357
Das Einhängen des Dateisystems mithilfe des DNS-Namens schlägt fehl	357
Sie können nicht auf Ihr Dateisystem zugreifen	358
Die Elastic IP-Adresse, die an die elastic network interface des Dateisystems angehängt ist, wurde gelöscht	359
Die elastic network interface des Dateisystems wurde geändert oder gelöscht	359
Das Erstellen eines DRA schlägt fehl	359
Das Umbenennen von Verzeichnissen dauert sehr lange	361
Falsch konfigurierter verknüpfter S3-Bucket	361
Probleme mit dem Speicher	363
Schreibfehler, da auf dem Speicherziel kein Speicherplatz verfügbar ist	363
Unausgeglichener Speicher auf OSTs	364
Probleme mit dem CSI-Treiber	367

Zusätzliche Informationen	368
Einrichten eines benutzerdefinierten Backup-Zeitplans	368
Übersicht über die Architektur	369
AWS CloudFormation-Vorlage	369
Automatisierte Bereitstellung	370
Zusätzliche Optionen	372
Dokumentverlauf	373
.....	cccxciii

Was ist Amazon FSx for Lustre?

FSx for Lustre macht es einfach und kostengünstig, das beliebte, leistungsstarke Lustre-Dateisystem zu starten und auszuführen. Sie verwenden Lustre für Workloads, bei denen es auf Geschwindigkeit ankommt, wie z. B. maschinelles Lernen, High Performance Computing (HPC), Videoverarbeitung und Finanzmodellierung.

Das Open-Source-Dateisystem Lustre wurde für Anwendungen entwickelt, die schnellen Speicher benötigen — bei denen Sie möchten, dass Ihr Speicher mit Ihrer Rechenleistung Schritt hält. Lustre wurde entwickelt, um das Problem der schnellen und kostengünstigen Verarbeitung der ständig wachsenden Datensätze der Welt zu lösen. Es ist ein weit verbreitetes Dateisystem, das für die schnellsten Computer der Welt entwickelt wurde. Es bietet Latenzen von unter einer Millisekunde, einen Durchsatz von bis zu Hunderten von Gbit/s und bis zu Millionen von IOPS.

[Weitere Informationen zu Lustre finden Sie auf der Lustre-Website.](#)

Als vollständig verwalteter Service erleichtert Ihnen Amazon FSx die Verwendung von Lustre für Workloads, bei denen es auf die Speichergeschwindigkeit ankommt. FSx for Lustre beseitigt die herkömmliche Komplexität der Einrichtung und Verwaltung von Lustre-Dateisystemen und ermöglicht es Ihnen, innerhalb weniger Minuten ein kampferprobtes Hochleistungsdateisystem einzurichten und auszuführen. Es bietet auch mehrere Bereitstellungsoptionen, sodass Sie die Kosten an Ihre Bedürfnisse anpassen können.

FSx for Lustre ist POSIX-konform, sodass Sie Ihre aktuellen Linux-basierten Anwendungen verwenden können, ohne Änderungen vornehmen zu müssen. FSx for Lustre bietet eine native Dateisystemschnittstelle und funktioniert wie jedes andere Dateisystem mit Ihrem Linux-Betriebssystem. Es bietet auch read-after-write Konsistenz und unterstützt das Sperren von Dateien.

Themen

- [Mehrere Bereitstellungsoptionen](#)
- [Mehrere Speicheroptionen](#)
- [FSx for Lustre und Datenrepositorien](#)
- [Zugreifen auf FSx for Lustre-Dateisysteme](#)
- [Integrationen mit Diensten AWS](#)
- [Sicherheits und Compliance](#)
- [Annahmen](#)

- [Preise für Amazon FSx for Lustre](#)
- [Foren zu Amazon FSx for Lustre](#)
- [Verwenden Sie Amazon FSx for Lustre zum ersten Mal?](#)

Mehrere Bereitstellungsoptionen

Amazon FSx for Lustre bietet eine Auswahl an Scratch - und persistenten Dateisystemen für unterschiedliche Datenverarbeitungsanforderungen. Scratch-Dateisysteme eignen sich ideal für die temporäre Speicherung und die kurzfristige Verarbeitung von Daten. Daten werden nicht repliziert und bleiben auch dann nicht erhalten, wenn ein Dateiserver ausfällt. Persistente Dateisysteme eignen sich ideal für längerfristige Speicherung und Workloads, bei denen der Durchsatz im Vordergrund steht. In persistenten Dateisystemen werden Daten repliziert, und Dateiserver werden ersetzt, wenn sie ausfallen. Weitere Informationen finden Sie unter [Bereitstellungsoptionen für FSx for Lustre-Dateisysteme](#).

Mehrere Speicheroptionen

Amazon FSx for Lustre bietet eine Auswahl an Speichertypen wie Solid State Drive (SSD) und Hard Disk Drive (HDD), die für unterschiedliche Datenverarbeitungsanforderungen optimiert sind:

- SSD-Speicheroptionen — Wählen Sie für IOPS-intensive Workloads mit niedriger Latenz, die typischerweise kleine, zufällige Dateioperationen erfordern, eine der SSD-Speicheroptionen.
- HDD-Speicheroptionen — Wählen Sie für durchsatzintensive Workloads, die typischerweise große, sequentielle Dateioperationen erfordern, eine der HDD-Speicheroptionen.

Wenn Sie ein Dateisystem mit der HDD-Speicheroption bereitstellen, können Sie optional einen schreibgeschützten SSD-Cache bereitstellen, der auf 20 Prozent Ihrer Festplattenspeicherkapazität ausgelegt ist. Dies bietet Latenzen von unter einer Millisekunde und höhere IOPS für Dateien, auf die häufig zugegriffen wird. Sowohl SSD-basierte als auch HDD-basierte Dateisysteme werden mit SSD-basierten Metadatenservern ausgestattet. Daher werden alle Metadatenoperationen, die den Großteil der Dateisystemoperationen ausmachen, mit Latenzen von unter einer Millisekunde ausgeführt.

Weitere Informationen zur Leistung dieser Speicheroptionen finden Sie unter [Leistung von Amazon FSx for Lustre](#)

FSx for Lustre und Datenrepositorien

Sie können FSx for Lustre-Dateisysteme mit Datenrepositorys auf Amazon S3 oder mit lokalen Datenspeichern verknüpfen.

FSx for Lustre S3-Datenrepository-Integration

FSx for Lustre ist in Amazon S3 integriert und erleichtert Ihnen so die Verarbeitung von Cloud-Datensätzen mithilfe des Lustre-Hochleistungsdateisystems. Wenn ein FSx for Lustre-Dateisystem mit einem Amazon S3 S3-Bucket verknüpft ist, stellt es S3-Objekte transparent als Dateien dar. Amazon FSx importiert bei der Erstellung des Dateisystems Auflistungen aller vorhandenen Dateien in Ihrem S3-Bucket. Amazon FSx kann auch Listen von Dateien importieren, die dem Daten-Repository hinzugefügt wurden, nachdem das Dateisystem erstellt wurde. Sie können die Importeinstellungen an Ihre Workflow-Anforderungen anpassen. Das Dateisystem ermöglicht es Ihnen auch, Dateisystemdaten zurück nach S3 zu schreiben. Datenrepository-Aufgaben vereinfachen die Übertragung von Daten und Metadaten zwischen Ihrem FSx for Lustre-Dateisystem und seinem dauerhaften Daten-Repository auf Amazon S3. Weitere Informationen finden Sie unter [Verwenden von Datenrepositorys mit Amazon FSx for Lustre](#) und [Datenrepository-Aufgaben](#).

FSx for Lustre und lokale Datenrepositorien

Mit Amazon FSx for Lustre können Sie Ihre Datenverarbeitungs-Workloads von lokalen auf die verteilen, AWS Cloud indem Sie Daten mit oder importieren. AWS Direct Connect AWS VPN Weitere Informationen finden Sie unter [Amazon FSx mit Ihren lokalen Daten verwenden](#).

Zugreifen auf FSx for Lustre-Dateisysteme

Sie können die Compute-Instance-Typen und Linux-Amls (Amazon Machine Images), die mit einem einzigen FSx for Lustre-Dateisystem verbunden sind, beliebig kombinieren.

Auf Amazon FSx for Lustre-Dateisysteme kann über Rechen-Workloads zugegriffen werden, die auf Amazon Elastic Compute Cloud (Amazon EC2) -Instances, auf Docker-Containern von Amazon Elastic Container Service (Amazon ECS) und auf Containern ausgeführt werden, die auf Amazon Elastic Kubernetes Service (Amazon EKS) laufen.

- Amazon EC2 — Sie greifen mit dem Open-Source-Lustre-Client von Ihren Amazon EC2 EC2-Compute-Instances auf Ihr Dateisystem zu. Amazon EC2 EC2-Instances können von anderen Availability Zones innerhalb derselben Amazon Virtual Private Cloud (Amazon VPC) auf Ihr

Dateisystem zugreifen, sofern Ihre Netzwerkkonfiguration den Zugriff über Subnetze innerhalb der VPC ermöglicht. Nachdem Ihr Amazon FSx for Lustre-Dateisystem bereitgestellt wurde, können Sie mit seinen Dateien und Verzeichnissen genauso arbeiten, wie Sie es mit einem lokalen Dateisystem tun würden.

- Amazon EKS — Sie greifen über Container, die auf Amazon EKS laufen, mithilfe des [Open-Source-CSI-Treibers FSx for Lustre auf Amazon FSx for Lustre](#) zu, wie im Amazon EKS-Benutzerhandbuch beschrieben. Ihre Container, die auf Amazon EKS laufen, können leistungsstarke persistente Volumes (PVs) verwenden, die von Amazon FSx for Lustre unterstützt werden.
- Amazon ECS — Sie greifen über Amazon ECS-Docker-Container auf Amazon EC2-Instances auf Amazon FSx for Lustre zu. Weitere Informationen finden Sie unter [Montage über Amazon Elastic Container Service](#).

Amazon FSx for Lustre ist mit den gängigsten Linux-basierten AMIs kompatibel, darunter Amazon Linux 2 und Amazon Linux, Red Hat Enterprise Linux (RHEL), CentOS, Ubuntu und SUSE Linux. Der Lustre-Client ist in Amazon Linux 2 und Amazon Linux enthalten. Für RHEL, CentOS und Ubuntu bietet ein AWS Lustre-Client-Repository Clients, die mit diesen Betriebssystemen kompatibel sind.

Mit FSx for Lustre können Sie Ihre rechenintensiven Workloads von lokalen Standorten auf die verteilen, indem Sie Daten über oder importieren. AWS Cloud AWS Direct Connect AWS Virtual Private Network Sie können lokal auf Ihr Amazon FSx-Dateisystem zugreifen, Daten nach Bedarf in Ihr Dateisystem kopieren und rechenintensive Workloads auf In-Cloud-Instances ausführen.

Weitere Informationen zu den Clients, Recheninstanzen und Umgebungen, von denen aus Sie auf FSx for Lustre-Dateisysteme zugreifen können, finden Sie unter [Zugreifen auf Dateisysteme](#)

Integrationen mit Diensten AWS

Amazon FSx for Lustre lässt sich in Amazon SageMaker als Eingabedatenquelle integrieren. Bei der Verwendung SageMaker mit FSx for Lustre werden Ihre Trainingsaufgaben für maschinelles Lernen beschleunigt, da der anfängliche Download-Schritt von Amazon S3 entfällt. Darüber hinaus werden Ihre Gesamtbetriebskosten (TCO) reduziert, da Sie das wiederholte Herunterladen gängiger Objekte für iterative Jobs auf demselben Datensatz vermeiden und so Kosten für S3-Anfragen sparen.

[Weitere Informationen finden Sie unter Was ist? SageMaker](#) im Amazon SageMaker Developer Guide. Eine Anleitung zur Verwendung von Amazon FSx for Lustre als Datenquelle für SageMaker finden Sie im Machine Learning Learning-Blog unter [Beschleunigen Sie das Training auf Amazon SageMaker mit Amazon FSx for Lustre- und Amazon EFS-Dateisystemen](#).AWS

FSx for Lustre lässt sich AWS Batch mithilfe von EC2 Launch Templates integrieren. AWS Batch ermöglicht die Ausführung von Batch-Computing-Workloads auf dem AWS Cloud, einschließlich High Performance Computing (HPC), Machine Learning (ML) und anderen asynchronen Workloads. AWS Batch passt die Größe der Instanzen automatisch und dynamisch an die Anforderungen an die Arbeitsressourcen an. Weitere Informationen finden Sie unter [Was ist AWS Batch?](#) im AWS Batch Benutzerhandbuch.

FSx for Lustre lässt sich integrieren. AWS ParallelCluster ist ein AWS unterstütztes Open-Source-Cluster-Management-Tool, das zur Bereitstellung und Verwaltung von HPC-Clustern verwendet wird. Es kann automatisch FSx for Lustre Lustre-Dateisysteme erstellen oder bestehende Dateisysteme während des Clustererstellungsprozesses verwenden.

Sicherheits und Compliance

FSx for Lustre-Dateisysteme unterstützen Verschlüsselung im Ruhezustand und bei der Übertragung. Amazon FSx verschlüsselt Dateisystemdaten im Ruhezustand automatisch mithilfe von Schlüsseln, die in AWS Key Management Service (AWS KMS) verwaltet werden. Übertragene Daten werden in bestimmten Dateisystemen auch automatisch verschlüsselt, AWS-Regionen wenn sie über unterstützte Amazon EC2 EC2-Instances abgerufen werden. Weitere Informationen zur Datenverschlüsselung in FSx for Lustre, einschließlich Informationen darüber, AWS-Regionen wo die Verschlüsselung von Daten bei der Übertragung unterstützt wird, finden Sie unter [Datenverschlüsselung in Amazon FSx for Lustre](#). Amazon FSx wurde auf die Einhaltung der ISO-, PCI-DSS- und SOC-Zertifizierungen geprüft und ist HIPAA-fähig. Weitere Informationen finden Sie unter [Sicherheit in FSx for Lustre](#).

Annahmen

In diesem Leitfaden gehen wir von den folgenden Annahmen aus:

- Wenn Sie Amazon Elastic Compute Cloud (Amazon EC2) verwenden, gehen wir davon aus, dass Sie mit diesem Service vertraut sind. Weitere Informationen zur Verwendung von Amazon EC2 finden Sie in der [Amazon EC2 EC2-Dokumentation](#).
- Wir gehen davon aus, dass Sie mit der Verwendung von Amazon Virtual Private Cloud (Amazon VPC) vertraut sind. Weitere Informationen zur Verwendung von Amazon VPC finden Sie im [Amazon VPC-Benutzerhandbuch](#).
- Wir gehen davon aus, dass Sie die Regeln für die Standardsicherheitsgruppe für Ihre VPC, die auf dem Amazon VPC-Service basiert, nicht geändert haben. Falls ja, stellen Sie sicher, dass

Sie die erforderlichen Regeln hinzufügen, um Netzwerkverkehr von Ihrer Amazon EC2 EC2-Instance zu Ihrem Amazon FSx for Lustre-Dateisystem zuzulassen. Weitere Details finden Sie unter [Zugriffskontrolle für Dateisysteme mit Amazon VPC](#).

Preise für Amazon FSx for Lustre

Mit Amazon FSx for Lustre fallen keine Hardware- oder Softwarekosten im Voraus an. Sie zahlen nur für die genutzten Ressourcen, ohne Mindestverpflichtungen, Einrichtungskosten oder zusätzliche Gebühren. Informationen zu den Preisen und Gebühren im Zusammenhang mit dem Service finden Sie unter [Amazon FSx for Lustre Pricing](#).

Foren zu Amazon FSx for Lustre

[Wenn Sie bei der Verwendung von Amazon FSx for Lustre auf Probleme stoßen, schauen Sie in den Foren nach.](#)

Verwenden Sie Amazon FSx for Lustre zum ersten Mal?

Wenn Sie Amazon FSx for Lustre zum ersten Mal verwenden, empfehlen wir Ihnen, die folgenden Abschnitte der Reihe nach zu lesen:

1. Wenn Sie bereit sind, Ihr erstes Amazon FSx for Lustre-Dateisystem zu erstellen, versuchen Sie es. [Erste Schritte mit Amazon FSx for Lustre](#)
2. Informationen zur Leistung finden Sie unter [Leistung von Amazon FSx for Lustre](#).
3. Informationen zum Verknüpfen Ihres Dateisystems mit einem Amazon S3 S3-Bucket-Daten-Repository finden Sie unter [Verwenden von Datenrepositorys mit Amazon FSx for Lustre](#).
4. Sicherheitsinformationen zu Amazon FSx for Lustre finden Sie unter. [Sicherheit in FSx for Lustre](#)
5. Informationen zu den Skalierbarkeitsgrenzen von Amazon FSx for Lustre, einschließlich Durchsatz und Dateisystemgröße, finden Sie unter. [Kontingente](#)
6. Informationen zur Amazon FSx for Lustre-API finden Sie in der [Amazon FSx for Lustre-API-Referenz](#).

Amazon FSx for Lustre einrichten

Bevor Sie Amazon FSx for Lustre zum ersten Mal verwenden, müssen Sie die Aufgaben im [Bei Amazon Web Services registrieren](#) Abschnitt abschließen. Um das [Tutorial Erste Schritte](#) abzuschließen, stellen Sie sicher, dass der Amazon S3 S3-Bucket, den Sie mit Ihrem Dateisystem verknüpfen, über die unter aufgeführten Berechtigungen verfügt [Hinzufügen von Berechtigungen zur Verwendung von Datenrepositories in Amazon S3](#).

Themen

- [Bei Amazon Web Services registrieren](#)
- [Hinzufügen von Berechtigungen zur Verwendung von Datenrepositories in Amazon S3](#)
- [Wie FSx for Lustre den Zugriff auf verknüpfte S3-Buckets prüft](#)
- [Nächster Schritt](#)

Bei Amazon Web Services registrieren

Führen Sie zur AWS Einrichtung die folgenden Aufgaben aus:

1. [Melde dich an für eine AWS-Konto](#)
2. [Erstellen Sie einen Benutzer mit Administratorzugriff](#)

Melde dich an für eine AWS-Konto

Wenn Sie noch keine haben AWS-Konto, führen Sie die folgenden Schritte aus, um eine zu erstellen.

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie <https://portal.aws.amazon.com/billing/signup>.
2. Folgen Sie den Online-Anweisungen.

Bei der Anmeldung müssen Sie auch einen Telefonanruf entgegennehmen und einen Verifizierungscode über die Telefontasten eingeben.

Wenn Sie sich für eine anmelden AWS-Konto, Root-Benutzer des AWS-Kontos wird eine erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Aus

Sicherheitsgründen sollten Sie einem Benutzer Administratorzugriff zuweisen und nur den Root-Benutzer verwenden, um [Aufgaben auszuführen, für die Root-Benutzerzugriff erforderlich](#) ist.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Sie können jederzeit Ihre aktuelle Kontoaktivität anzeigen und Ihr Konto verwalten. Rufen Sie dazu <https://aws.amazon.com/> auf und klicken Sie auf Mein Konto.

Erstellen Sie einen Benutzer mit Administratorzugriff

Nachdem Sie sich für einen angemeldet haben AWS-Konto, sichern Sie Ihren Root-Benutzer des AWS-Kontos AWS IAM Identity Center, aktivieren und erstellen Sie einen Administratorbenutzer, sodass Sie den Root-Benutzer nicht für alltägliche Aufgaben verwenden.

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich [AWS Management Console](#) als Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter [Anmelden als Root-Benutzer](#) im AWS-Anmeldung Benutzerhandbuch zu.

2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

Anweisungen finden Sie unter [Aktivieren eines virtuellen MFA-Geräts für Ihren AWS-Konto Root-Benutzer \(Konsole\)](#) im IAM-Benutzerhandbuch.

Erstellen Sie einen Benutzer mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

Anweisungen finden Sie unter [Aktivieren AWS IAM Identity Center](#) im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Benutzer in IAM Identity Center Administratorzugriff.

Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden [Sie unter Benutzerzugriff mit der Standardeinstellung konfigurieren IAM-Identity-Center-Verzeichnis](#) im AWS IAM Identity Center Benutzerhandbuch.

Melden Sie sich als Benutzer mit Administratorzugriff an

- Um sich mit Ihrem IAM-Identity-Center-Benutzer anzumelden, verwenden Sie die Anmelde-URL, die an Ihre E-Mail-Adresse gesendet wurde, als Sie den IAM-Identity-Center-Benutzer erstellt haben.

Hilfe bei der Anmeldung mit einem IAM Identity Center-Benutzer finden Sie [im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Zugriffsportal](#).

Weisen Sie weiteren Benutzern Zugriff zu

1. Erstellen Sie in IAM Identity Center einen Berechtigungssatz, der der bewährten Methode zur Anwendung von Berechtigungen mit den geringsten Rechten folgt.

Anweisungen finden Sie im Benutzerhandbuch unter [Einen Berechtigungssatz erstellen](#).AWS IAM Identity Center

2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

Anweisungen finden [Sie im AWS IAM Identity Center Benutzerhandbuch unter Gruppen hinzufügen](#).

Hinzufügen von Berechtigungen zur Verwendung von Datenrepositorys in Amazon S3

Amazon FSx for Lustre ist tief in Amazon S3 integriert. Diese Integration bedeutet, dass Anwendungen, die auf Ihr FSx for Lustre-Dateisystem zugreifen, auch nahtlos auf die Objekte zugreifen können, die in Ihrem verknüpften Amazon S3 S3-Bucket gespeichert sind. Weitere Informationen finden Sie unter [Verwenden von Datenrepositorys mit Amazon FSx for Lustre](#).

Um Datenrepositorys verwenden zu können, müssen Sie Amazon FSx for Lustre zunächst bestimmte IAM-Berechtigungen in einer Rolle gewähren, die mit dem Konto für Ihren Administratorbenutzer verknüpft ist.

Um mithilfe der Konsole eine Inline-Richtlinie für eine Rolle einzubetten

1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die IAM-Konsole unter <https://console.aws.amazon.com/iam/>.

2. Wählen Sie im Navigationsbereich Rollen aus.
3. Wählen Sie in der Liste den Namen der Rolle aus, in die Sie die Richtlinie integrieren möchten.
4. Wählen Sie die Registerkarte Berechtigungen.
5. Scrollen Sie auf der Seite nach unten und klicken Sie auf Add inline policy.

 Note

Sie können eine Inline-Richtlinie nicht in eine serviceverknüpfte Rolle in IAM einbetten. Da der verknüpfte Service definiert, ob Sie die Berechtigungen der Rolle ändern können, sind Sie möglicherweise in der Lage, zusätzliche Richtlinien von der Service-Konsole, einer API oder der AWS CLI aus hinzuzufügen. Informationen zur Dokumentation der dienstbezogenen Rolle für einen Dienst finden Sie unter AWS Dienste, die mit IAM funktionieren. Wählen Sie dort in der Spalte „Dienstverknüpfte Rolle“ für Ihren Service die Option Ja aus.

6. Wählen Sie Richtlinien mit dem Visual Editor erstellen
7. Fügen Sie die folgende Erklärung zur Berechtigungsrichtlinie hinzu.

```
{
  "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/*"
  }
}
```

Nachdem Sie eine Inline-Richtlinie erstellt haben, wird sie automatisch in Ihre Rolle eingebettet. Weitere Informationen zu serviceverknüpften Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#).

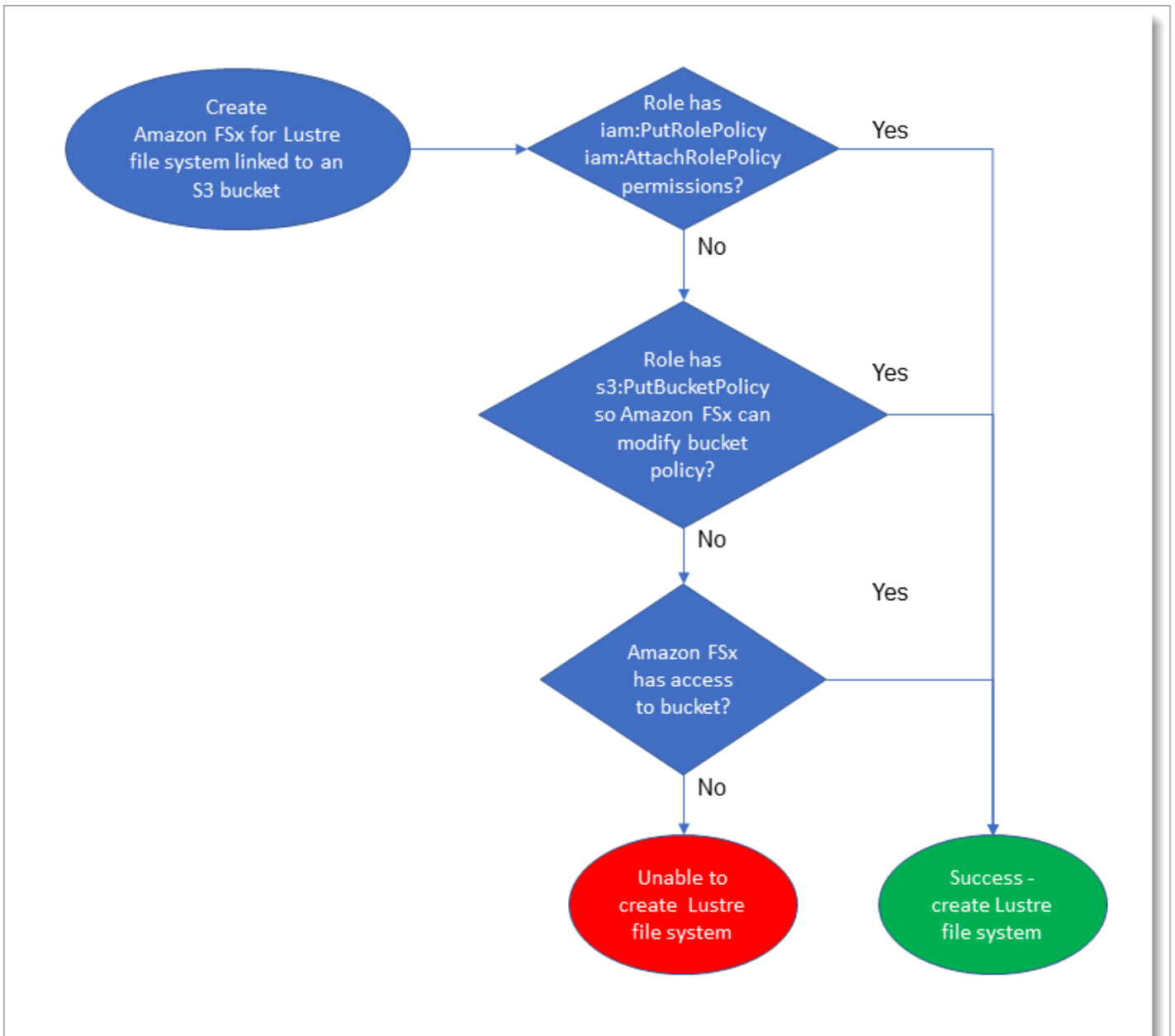
Wie FSx for Lustre den Zugriff auf verknüpfte S3-Buckets prüft

Wenn die IAM-Rolle, mit der Sie das FSx for Lustre-Dateisystem erstellen, nicht über die `iam:PutRolePolicy` Berechtigungen `iam:AttachRolePolicy` und verfügt, prüft Amazon FSx, ob es Ihre S3-Bucket-Richtlinie aktualisieren kann. Amazon FSx kann Ihre Bucket-Richtlinie aktualisieren, wenn in Ihrer IAM-Rolle die `s3:PutBucketPolicy` Berechtigung enthalten ist, dem Amazon FSx-Dateisystem den Import oder Export von Daten in Ihren S3-Bucket zu ermöglichen. Wenn Amazon FSx die Bucket-Richtlinie ändern darf, fügt Amazon FSx der Bucket-Richtlinie die folgenden Berechtigungen hinzu:

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

Wenn Amazon FSx die Bucket-Richtlinie nicht ändern kann, wird geprüft, ob die bestehende Bucket-Richtlinie Amazon FSx Zugriff auf den Bucket gewährt.

Wenn all diese Optionen fehlschlagen, schlägt die Anforderung zur Erstellung des Dateisystems fehl. Das folgende Diagramm zeigt die Prüfungen, die Amazon FSx befolgt, wenn es bestimmt, ob ein Dateisystem auf den S3-Bucket zugreifen kann, mit dem es verknüpft werden soll.



Nächster Schritt

Informationen zu den ersten Schritten mit FSx for Lustre finden Sie unter Anweisungen [Erste Schritte mit Amazon FSx for Lustre](#) zum Erstellen Ihrer Amazon FSx for Lustre-Ressourcen.

Erste Schritte mit Amazon FSx for Lustre

Im Folgenden erfahren Sie, wie Sie mit Amazon FSx for Lustre beginnen können. Diese Schritte führen Sie durch die Erstellung eines Amazon FSx for Lustre-Dateisystems und den Zugriff darauf von Ihren Compute-Instances aus. Optional zeigen sie, wie Sie Ihr Amazon FSx for Lustre-Dateisystem verwenden können, um die Daten in Ihrem Amazon S3 S3-Bucket mit Ihren dateibasierten Anwendungen zu verarbeiten.

Diese Übung für den Einstieg umfasst die folgenden Schritte.

Themen

- [Voraussetzungen](#)
- [Erstellen Sie Ihr FSx for Lustre-Dateisystem](#)
- [Installieren und konfigurieren Sie den Lustre-Client](#)
- [Hängen Sie das Dateisystem ein](#)
- [Führen Sie Ihren Workflow aus](#)
- [Bereinigen von -Ressourcen](#)

Voraussetzungen

Um diese Übung „Erste Schritte“ durchführen zu können, benötigen Sie Folgendes:

- Ein AWS Konto mit den erforderlichen Berechtigungen, um ein Amazon FSx for Lustre-Dateisystem und eine Amazon EC2 EC2-Instance zu erstellen. Weitere Informationen finden Sie unter [Amazon FSx for Lustre einrichten](#).
- Erstellen Sie eine Amazon VPC-Sicherheitsgruppe, die mit Ihrem FSx for Lustre-Dateisystem verknüpft werden soll, und ändern Sie sie nach der Erstellung des Dateisystems nicht. Weitere Informationen finden Sie unter [So erstellen Sie eine Sicherheitsgruppe für Ihr Amazon FSx-Dateisystem](#).
- Eine Amazon EC2 EC2-Instance, auf der eine unterstützte Linux-Version in Ihrer Virtual Private Cloud (VPC) ausgeführt wird, die auf dem Amazon VPC-Service basiert. Für diese Übung „Erste Schritte“ empfehlen wir die Verwendung von Amazon Linux 2023. Sie installieren den Lustre-Client auf dieser EC2-Instance und mounten dann Ihr FSx for Lustre-Dateisystem auf der EC2-Instance. Weitere Informationen zum Erstellen einer EC2-Instance finden Sie unter [Erste Schritte: Starten Sie eine Instance](#) oder [Starten Sie Ihre Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.

Der Lustre-Client unterstützt Amazon Linux, Amazon Linux 2, Amazon Linux 2023, CentOS und Red Hat Enterprise Linux 7.7 bis 7.9, 8.2 bis 8.9, 9.0, 9.3 und 9.4, Rocky Linux 8.4 bis 8.9, 9.0, 9.3 und 9.4, SUSE Linux Enterprise Server 12 SP3, SP4 und SP5 sowie Ubuntu 18.04, 20.04 und 22.04. Weitere Informationen finden Sie unter [Kompatibilität des Lustre-Dateisystems und des Client-Kernels](#).

Beachten Sie beim Erstellen Ihrer Amazon EC2 EC2-Instance für diese Übung „Erste Schritte“ Folgendes:

- Wir empfehlen, dass Sie Ihre Instance in Ihrer Standard-VPC erstellen.
- Wir empfehlen, dass Sie bei der Erstellung Ihrer EC2-Instance die Standardsicherheitsgruppe verwenden.
- Jedes FSx for Lustre-Dateisystem benötigt eine IP-Adresse für jeden Metadatenserver (MDS) und eine IP-Adresse für jeden Speicherserver (OSS).
 - Für Persistent_2-Dateisysteme mit Metadatenkonfiguration erfordert jeder IOPS-Wert von 12000 Metadaten auch eine IP-Adresse innerhalb des Subnetzes, in dem sich Ihr Dateisystem befindet.
 - Persistente SSD-Dateisysteme werden mit 2,4 TiB Speicher pro Betriebssystem bereitgestellt.
 - Persistente HDD-Dateisysteme mit einer Durchsatzkapazität von 12 MB/s/TiB werden mit 6 TiB Speicher pro Betriebssystem bereitgestellt.
 - Persistente HDD-Dateisysteme mit einer Durchsatzkapazität von 40 MB/s/TiB werden mit 1,8 TiB Speicher pro Betriebssystem bereitgestellt.
 - Scratch_2-Dateisysteme werden mit 2,4 TiB Speicher pro Betriebssystem bereitgestellt.
 - Scratch_1-Dateisysteme werden mit 3,6 TiB Speicher pro Betriebssystem bereitgestellt.
- Ein Amazon S3 S3-Bucket, in dem die Daten gespeichert werden, die Ihr Workload verarbeiten soll. Der S3-Bucket wird das verknüpfte dauerhafte Datenrepository für Ihr FSx for Lustre-Dateisystem sein.
- Ermitteln Sie, welche Art von Amazon FSx for Lustre-Dateisystem Sie erstellen möchten, ob es sich um ein Scratch-Dateisystem oder ein persistentes Dateisystem handelt. Weitere Informationen finden Sie unter [Optionen zur Dateisystembereitstellung für FSx for Lustre](#).

Erstellen Sie Ihr FSx for Lustre-Dateisystem

Als Nächstes erstellen Sie Ihr Dateisystem in der Konsole.

So erstellen Sie Ihr -Dateisystem:

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Dashboard Create file system (Dateisystem erstellen), um den Assistenten zur Dateisystemerstellung zu starten.
3. Wählen Sie FSx for Lustre und dann Weiter, um die Seite Create File System anzuzeigen.
4. Geben Sie die Informationen im Abschnitt Dateisystemdetails ein:
 - Geben Sie im Feld Dateisystemname — optional einen Namen für Ihr Dateisystem ein. Sie können bis zu 256 Unicode-Buchstaben, Leerzeichen und Zahlen sowie die Sonderzeichen + - =. _:/verwenden.
 - Wählen Sie für Bereitstellung und Speichertyp eine der folgenden Optionen aus:

SSD-Speicher bietet IOPS-intensive Workloads mit niedriger Latenz, die in der Regel kleine, zufällige Dateioperationen beinhalten. HDD-Speicher bietet durchsatzintensive Workloads, die in der Regel große, sequentielle Dateioperationen beinhalten.

Weitere Informationen zu Speichertypen finden Sie unter [Mehrere Speicheroptionen](#)

Weitere Informationen zu Bereitstellungstypen finden Sie unter [Bereitstellungsoptionen für FSx for Lustre-Dateisysteme](#).

Weitere Informationen darüber, AWS-Regionen wo die Verschlüsselung von Daten bei der Übertragung verfügbar ist, finden Sie unter [Verschlüsseln von Daten während der Übertragung](#).

- Wählen Sie den Bereitstellungstyp Persistent SSD für längerfristige Speicherung und für latenzempfindliche Workloads, die ein Höchstmaß an IOPS/Durchsatz erfordern. Die Dateiserver sind hochverfügbar, Daten werden automatisch innerhalb der Availability Zone des Dateisystems repliziert und unterstützen die Verschlüsselung von Daten während der Übertragung. Persistent, SSD verwendet Persistent 2, die neueste Generation persistenter Dateisysteme.
- Wählen Sie den Bereitstellungstyp Persistent HDD für längerfristige Speicherung und für durchsatzorientierte Workloads, die nicht latenzempfindlich sind. Die Dateiserver sind hochverfügbar, Daten werden automatisch innerhalb der Availability Zone des Dateisystems repliziert, und dieser Typ unterstützt die Verschlüsselung von Daten während der Übertragung. Persistent, HDD verwendet den Bereitstellungstyp Persistent 1.

Wählen Sie SSD-Cache, um einen SSD-Cache zu erstellen, der auf 20 Prozent Ihrer Festplattenspeicherkapazität ausgelegt ist und so Latenzen von unter einer Millisekunde und höhere IOPS für häufig aufgerufene Dateien bietet.

- Wählen Sie den Bereitstellungstyp Scratch, SSD für die temporäre Speicherung und die kurzfristige Verarbeitung von Daten. Scratch, SSD verwendet Scratch 2-Dateisysteme und bietet Verschlüsselung von Daten während der Übertragung.
- Wählen Sie den Durchsatz pro Speichereinheit, den Sie für Ihr Dateisystem benötigen. Diese Option ist nur für persistente Bereitstellungstypen gültig.

Der Durchsatz pro Speichereinheit ist der Lese- und Schreibdurchsatz für jedes bereitgestellte 1 Tebibyte (TiB) an Speicher in MB/s/TiB. Sie zahlen für den von Ihnen bereitgestellten Durchsatz:

- Wählen Sie für persistenten SSD-Speicher einen Wert von entweder 125, 250, 500 oder 1.000 MB/s/TiB.
- Wählen Sie für persistenten Festplattenspeicher einen Wert von 12 oder 40 MB/s/TiB.

Sie können den Durchsatz pro Speichereinheit nach Bedarf erhöhen oder verringern, nachdem Sie das Dateisystem erstellt haben. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

- Stellen Sie unter Speicherkapazität die Speicherkapazität für Ihr Dateisystem in TiB ein:
 - Für einen dauerhaften SSD-Bereitstellungstyp legen Sie diesen Wert auf einen Wert von 1,2 TiB, 2,4 TiB oder in Schritten von 2,4 TiB fest.
 - Bei einem dauerhaften HDD-Bereitstellungstyp kann dieser Wert um 6,0 TiB für Dateisysteme mit 12 MB/s/TiB und für Dateisysteme mit 40 MB/s/TiB um 1,8 TiB erhöht werden.

Sie können die Speicherkapazität nach Bedarf erhöhen, nachdem Sie das Dateisystem erstellt haben. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#).

- Für die Metadatenkonfiguration haben Sie zwei Optionen, um die Anzahl der Metadaten-IOPS für Ihr Dateisystem bereitzustellen:
 - Wählen Sie Automatisch (Standardeinstellung), wenn Amazon FSx die Metadaten-IOPS auf Ihrem Dateisystem basierend auf der Speicherkapazität Ihres Dateisystems automatisch bereitstellen und skalieren soll.

- Wählen Sie Vom Benutzer bereitgestellt, wenn Sie die Anzahl der Metadaten-IOPS angeben möchten, die für Ihr Dateisystem bereitgestellt werden sollen. Gültige Werte sind 1500, 3000, 6000, 12000, und Vielfache von 12000, bis zu einem Maximum von 192000

Weitere Informationen zu Metadaten-IOPS finden Sie unter [Leistungskonfiguration für Lustre-Metadaten](#)

- Wählen Sie als Datenkomprimierungstyp NONE aus, um die Datenkomprimierung zu deaktivieren, oder wählen Sie LZ4, um die Datenkomprimierung mit dem LZ4-Algorithmus zu aktivieren. Weitere Informationen finden Sie unter [Lustre-Datenkomprimierung](#).

Alle FSx for Lustre-Dateisysteme basieren auf Lustre-Version 2.15, wenn sie mit der Amazon FSx-Konsole erstellt wurden.

5. Geben Sie im Bereich Netzwerk und Sicherheit die folgenden Netzwerk- und Sicherheitsgruppeninformationen an:

- Wählen Sie für Virtual Private Cloud (VPC) die VPC aus, die Sie Ihrem Dateisystem zuordnen möchten. Wählen Sie für diese Übung „Erste Schritte“ dieselbe VPC aus, die Sie für Ihre Amazon EC2 EC2-Instance ausgewählt haben.
- Für VPC-Sicherheitsgruppen sollte die ID für die Standardsicherheitsgruppe für Ihre VPC bereits hinzugefügt sein. Wenn Sie nicht die Standardsicherheitsgruppe verwenden, stellen Sie sicher, dass der Sicherheitsgruppe, die Sie für diese Übung mit den ersten Schritten verwenden, die folgende Regel für eingehende Nachrichten hinzugefügt wird.

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
Alle TCP	TCP	0-65535	Benutzerdefiniert <i>the_ID_of_this_security_group</i>	Regel für eingehenden Lustre-Verkehr

Die folgende Bildschirmaufnahme zeigt ein Beispiel für die Bearbeitung von Regeln für eingehenden Datenverkehr.

Edit inbound rules [X]

Type	Protocol	Port Range	Source	Description
All traffic	All	0 - 65535	Custom	sg- [redacted]

[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

Stellen Sie sicher, dass die von Ihnen verwendete Sicherheitsgruppe den Konfigurationsanweisungen unter folgt. [Zugriffskontrolle für Dateisysteme mit Amazon VPC](#) Sie müssen die Sicherheitsgruppe so einrichten, dass eingehender Datenverkehr über die Ports 988 und 1018-1023 von der Sicherheitsgruppe selbst oder vom vollständigen Subnetz-CIDR zugelassen wird, was erforderlich ist, damit die Dateisystem-Hosts miteinander kommunizieren können.

- Wählen Sie für Subnetz einen beliebigen Wert aus der Liste der verfügbaren Subnetze aus.
6. Für den Bereich Verschlüsselung hängen die verfügbaren Optionen davon ab, welchen Dateisystemtyp Sie erstellen:
- Für ein persistentes Dateisystem können Sie einen AWS Key Management Service (AWS KMS) Verschlüsselungsschlüssel wählen, um die Daten in Ihrem Dateisystem im Ruhezustand zu verschlüsseln.
 - Bei einem Scratch-Dateisystem werden Daten im Ruhezustand mit Schlüsseln verschlüsselt, die von verwaltet werden AWS.
 - Bei Scratch-2-Dateisystemen und persistenten Dateisystemen werden übertragene Daten automatisch verschlüsselt, wenn von einem unterstützten Amazon EC2 EC2-Instance-Typ auf das Dateisystem zugegriffen wird. Weitere Informationen finden Sie unter [Verschlüsseln von Daten während der Übertragung](#).
7. Für den Abschnitt Datenrepository-Import/Export — optional ist die Verknüpfung Ihres Dateisystems mit Amazon S3 S3-Datenrepositorys standardmäßig deaktiviert. Informationen zur Aktivierung dieser Option und zum Erstellen einer Datenrepository-Zuordnung zu einem vorhandenen S3-Bucket finden Sie unter. [Um einen S3-Bucket beim Erstellen eines Dateisystems \(Konsole\) zu verknüpfen](#)

⚠ Important

- Wenn Sie diese Option auswählen, werden auch Backups deaktiviert, sodass Sie während der Erstellung des Dateisystems keine Backups aktivieren können.
- Wenn Sie ein oder mehrere Amazon FSx for Lustre-Dateisysteme mit einem Amazon S3 S3-Bucket verknüpfen, löschen Sie den Amazon S3 S3-Bucket erst, wenn alle verknüpften Dateisysteme gelöscht wurden.

8. Für Protokollierung — optional, ist die Protokollierung standardmäßig aktiviert. Wenn diese Option aktiviert ist, werden Fehler und Warnungen für Datenrepository-Aktivitäten in Ihrem Dateisystem in Amazon CloudWatch Logs protokolliert. Informationen zur Konfiguration der Protokollierung finden Sie unter [Verwaltung der Protokollierung](#).
9. Unter Backup und Wartung — optional können Sie Folgendes tun.

Für tägliche automatische Backups:

- Deaktivieren Sie das tägliche automatische Backup. Diese Option ist standardmäßig aktiviert, sofern Sie den Import/Export von Data Repository nicht aktiviert haben.
- Legen Sie die Startzeit für das tägliche automatische Backup-Fenster fest.
- Legen Sie den Aufbewahrungszeitraum für automatische Backups auf 1 bis 35 Tage fest.

Weitere Informationen finden Sie unter [Arbeiten mit Backups](#).

10. Legen Sie die Startzeit für das wöchentliche Wartungsfenster fest, oder behalten Sie die Standardeinstellung Keine Präferenz bei.
11. Für Root Squash — optional, ist Root Squash standardmäßig deaktiviert. Informationen zur Aktivierung und Konfiguration von Root-Squash finden Sie unter [Um Root Squash beim Erstellen eines Dateisystems \(Konsole\) zu aktivieren](#)
12. Erstellen Sie alle Tags, die Sie auf Ihr Dateisystem anwenden möchten.
13. Wählen Sie Weiter, um die Übersichtsseite „Dateisystem erstellen“ aufzurufen.
14. Überprüfen Sie die Einstellungen für Ihr Amazon FSx for Lustre-Dateisystem und wählen Sie Dateisystem erstellen.

Nachdem Sie Ihr Dateisystem erstellt haben, notieren Sie sich den vollqualifizierten Domainnamen und den Mount-Namen für einen späteren Schritt. Sie können den vollqualifizierten Domänennamen

und den Mount-Namen für ein Dateisystem finden, indem Sie den Namen des Dateisystems im Cache-Dashboard auswählen und dann Anhängen wählen.

Installieren und konfigurieren Sie den Lustre-Client

Bevor Sie von Ihrer Amazon EC2-Instance aus auf Ihr Amazon FSx for Lustre-Dateisystem zugreifen können, müssen Sie wie folgt vorgehen:

- Stellen Sie sicher, dass Ihre EC2-Instance die Mindestanforderungen an den Kernel erfüllt.
- Aktualisieren Sie den Kernel bei Bedarf.
- Laden Sie den Lustre-Client herunter und installieren Sie ihn.

Um die Kernel-Version zu überprüfen und den Lustre-Client herunterzuladen

1. Öffnen Sie ein Terminalfenster auf Ihrer EC2-Instance.
2. Ermitteln Sie, welcher Kernel derzeit auf Ihrer Compute-Instance läuft, indem Sie den folgenden Befehl ausführen.

```
uname -r
```

3. Führen Sie eine der folgenden Aktionen aus:

- Wenn der Befehl `6.1.79-99.167.amzn2023.x86_64` für x86-basierte EC2-Instances `6.1.79-99.167.amzn2023.aarch64` oder höher für Graviton2-basierte EC2-Instances zurückgegeben wird, laden Sie den Lustre-Client mit dem folgenden Befehl herunter und installieren Sie ihn.

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

- Wenn der Befehl weniger als `6.1.79-99.167.amzn2023.x86_64` für x86-basierte EC2-Instances oder weniger als `6.1.79-99.167.amzn2023.aarch64` für Graviton2-basierte EC2-Instances zurückgibt, aktualisieren Sie den Kernel und starten Sie Ihre Amazon EC2 EC2-Instance neu, indem Sie den folgenden Befehl ausführen.

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

Bestätigen Sie mit dem Befehl, dass der Kernel aktualisiert wurde. `uname -r` Laden Sie dann den Lustre-Client herunter und installieren Sie ihn wie oben beschrieben.

Informationen zur Installation des Lustre-Clients auf anderen Linux-Distributionen finden Sie unter. [Den Lustre-Client installieren](#)

Hängen Sie das Dateisystem ein

Um Ihr Dateisystem einzuhängen, erstellen Sie ein Bereitstellungsverzeichnis oder einen Einhängpunkt, hängen das Dateisystem dann auf Ihrem Client ein und stellen sicher, dass Ihr Client auf das Dateisystem zugreifen kann.

Um Ihr Dateisystem zu mounten

1. Erstellen Sie ein Verzeichnis für den Mountingpunkt mit dem folgenden Befehl.

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

2. Hängen Sie das Amazon FSx for Lustre-Dateisystem in das Verzeichnis ein, das Sie erstellt haben. Verwenden Sie den folgenden Befehl und ersetzen Sie die folgenden Elemente:

- *file_system_dns_name* Ersetzen Sie es durch den tatsächlichen DNS-Namen (Domain Name System) des Dateisystems.
- *mountname* Ersetzen Sie ihn durch den Mount-Namen des Dateisystems, den Sie erhalten können, indem Sie den describe-file-systems AWS CLI Befehl oder die [DescribeFileSystems-API-Operation](#) ausführen.

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

Dieser Befehl mountet Ihr Dateisystem mit zwei Optionen: `-o relatime flock`

- `relatime`— Die `atime` Option verwaltet zwar Daten `atime` (Inode-Zugriffszeiten) für jeden Dateizugriff, aber die `relatime` Option verwaltet auch `atime` Daten, jedoch nicht für jeden Dateizugriff. Wenn die `relatime` Option aktiviert ist, `atime` werden Daten nur dann auf die Festplatte geschrieben, wenn die Datei seit der `atime` letzten Aktualisierung (`mtime`) geändert wurde oder wenn der letzte Zugriff auf die Datei vor mehr als einer bestimmten Zeit (standardmäßig 6 Stunden) stattgefunden hat. Wenn Sie entweder die `atime` Option `relatime` oder verwenden, werden die [Dateifreigabeprozesse](#) optimiert.

Note

Wenn Ihr Workload eine genaue Genauigkeit der Zugriffszeit erfordert, können Sie das Mounten mit der Option `atime mount` durchführen. Dies kann sich jedoch negativ auf die Leistung der Arbeitslast auswirken, da der Netzwerkverkehr erhöht wird, der zur Einhaltung genauer Werte für die Zugriffszeit erforderlich ist.

Wenn Ihr Workload keine Zugriffszeit für Metadaten erfordert, kann die Verwendung der `noatime` Mount-Option zur Deaktivierung von Aktualisierungen der Zugriffszeit zu einer Leistungssteigerung führen. Beachten Sie, dass `atime` zielgerichtete Prozesse wie die Freigabe von Dateien oder die Freigabe von Datenvalidität bei ihrer Veröffentlichung ungenau sein können.

- `flock`— Aktiviert das Sperren von Dateien für Ihr Dateisystem. Wenn Sie nicht möchten, dass das Sperren von Dateien aktiviert wird, verwenden Sie den `mount` Befehl `ohneflock`.
3. Stellen Sie sicher, dass der Befehl `mount` erfolgreich war, indem Sie den Inhalt des Verzeichnisses `ls /mnt/fsx`, in dem Sie das Dateisystem bereitgestellt haben. Verwenden Sie dazu den folgenden Befehl.

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

Sie können auch den folgenden `df` Befehl verwenden.

```
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% /mnt/fsx
tmpfs                       203956         0     203956  0% /run/user/1000
```

Die Ergebnisse zeigen das Amazon FSx-Dateisystem, das auf `/mnt/fsx` gemountet ist.

Führen Sie Ihren Workflow aus

Nachdem Ihr Dateisystem nun erstellt und auf einer Recheninstanz bereitgestellt wurde, können Sie es verwenden, um Ihren Hochleistungs-Rechen-Workload auszuführen.

Sie können eine Datenrepository-Zuordnung erstellen, um Ihr Dateisystem mit einem Amazon S3 S3-Daten-Repository zu verknüpfen. Weitere Informationen finden Sie unter [Ihr Dateisystem mit einem S3-Bucket verknüpfen](#).

Nachdem Sie Ihr Dateisystem mit einem Amazon S3 S3-Daten-Repository verknüpft haben, können Sie Daten, die Sie in Ihr Dateisystem geschrieben haben, jederzeit wieder in Ihren Amazon S3 S3-Bucket exportieren. Führen Sie von einem Terminal auf einer Ihrer Compute-Instances aus den folgenden Befehl aus, um eine Datei in Ihren Amazon S3 S3-Bucket zu exportieren.

```
sudo lfs hsm_archive file_name
```

Weitere Informationen darüber, wie Sie diesen Befehl schnell für einen Ordner oder eine große Sammlung von Dateien ausführen können, finden Sie unter [Exportieren von Dateien mithilfe von HSM-Befehlen](#).

Bereinigen von -Ressourcen

Nachdem Sie diese Übung abgeschlossen haben, sollten Sie die folgenden Schritte ausführen, um Ihre Ressourcen zu bereinigen und Ihr AWS Konto zu schützen.

So bereinigen Sie Ressourcen

1. Wenn Sie einen endgültigen Export durchführen möchten, führen Sie den folgenden Befehl aus.

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

2. Beenden Sie Ihre Instance auf der Amazon EC2 EC2-Konsole. Weitere Informationen finden Sie unter [Terminate Your Instance](#) im Amazon EC2 EC2-Benutzerhandbuch.
3. Löschen Sie Ihr Dateisystem auf der Amazon FSx for Lustre-Konsole wie folgt:
 - a. Wählen Sie im Navigationsbereich Dateisysteme aus.
 - b. Wählen Sie das Dateisystem, das Sie löschen möchten, aus der Liste der Dateisysteme im Dashboard aus.

- c. Klicken Sie bei Aktionen auf Dateisystem löschen.
 - d. Wählen Sie im daraufhin angezeigten Dialogfeld aus, ob Sie eine endgültige Sicherungskopie des Dateisystems erstellen möchten. Geben Sie dann die Dateisystem-ID ein, um den Löschvorgang zu bestätigen. Wählen Sie Dateisystem löschen.
4. Wenn Sie für diese Übung einen Amazon S3 S3-Bucket erstellt haben und die exportierten Daten nicht beibehalten möchten, können Sie ihn jetzt löschen. Weitere Informationen finden Sie unter [Löschen eines Buckets](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Bereitstellungsoptionen für FSx for Lustre-Dateisysteme

FSx for Lustre bietet ein leistungsstarkes, paralleles Dateisystem, das Daten auf mehreren Netzwerk-Dateiservern speichert, um die Leistung zu maximieren und Engpässe zu reduzieren. Diese Server haben mehrere Festplatten. Um die Last zu verteilen, zerlegt Amazon FSx Dateisystemdaten in kleinere Blöcke und verteilt sie mithilfe eines als Striping bezeichneten Prozesses auf Festplatten und Server. Weitere Hinweise zu FSx for Lustre Data Striping finden Sie unter [Daten in Ihrem Dateisystem entfernen](#)

Es hat sich bewährt, ein äußerst langlebiges Langzeitdaten-Repository, das sich auf Amazon S3 befindet, mit Ihrem FSx for Lustre-Hochleistungsdateisystem zu verknüpfen.

In diesem Szenario speichern Sie Ihre Datensätze im verknüpften Amazon S3 S3-Daten-Repository. Wenn Sie Ihr FSx for Lustre-Dateisystem erstellen, verknüpfen Sie es mit Ihrem S3-Daten-Repository. Zu diesem Zeitpunkt werden die Objekte in Ihrem S3-Bucket als Dateien und Verzeichnisse in Ihrem FSx-Dateisystem aufgeführt. Amazon FSx kopiert dann automatisch den Dateiinhalt von S3 in Ihr Lustre-Dateisystem, wenn zum ersten Mal auf eine Datei im Amazon FSx-Dateisystem zugegriffen wird. Nachdem Ihr Rechen-Workload ausgeführt wurde, oder zu einem beliebigen Zeitpunkt, können Sie eine Datenrepository-Aufgabe verwenden, um Änderungen zurück nach S3 zu exportieren. Weitere Informationen finden Sie unter [Verwenden von Datenrepositorys mit Amazon FSx for Lustre](#) und [Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen](#).

Optionen zur Dateisystembereitstellung für FSx for Lustre

Amazon FSx for Lustre bietet zwei Bereitstellungsoptionen für Dateisysteme: Scratch und Persistent.

Note

Beide Bereitstellungsoptionen unterstützen Solid-State-Drive-Speicher (SSD). Festplattenspeicher (HDD) wird jedoch nur in einem der persistenten Bereitstellungstypen unterstützt.

Sie wählen den Bereitstellungstyp des Dateisystems, wenn Sie ein neues Dateisystem mit der AWS Management Console AWS Command Line Interface (AWS CLI) oder der Amazon FSx for Lustre-API erstellen. Weitere Informationen finden Sie unter [Erstellen Sie Ihr FSx for Lustre-Dateisystem](#) und [CreateFileSystem](#) in der Amazon FSx API-Referenz.

Die Verschlüsselung ruhender Daten wird automatisch aktiviert, wenn Sie ein Amazon FSx for Lustre-Dateisystem erstellen, unabhängig vom verwendeten Bereitstellungstyp. Scratch 2- und persistente Dateisysteme verschlüsseln automatisch Daten während der Übertragung, wenn auf sie von Amazon EC2 EC2-Instances zugegriffen wird, die Verschlüsselung bei der Übertragung unterstützen. Weitere Informationen zur Verschlüsselung finden Sie unter [Datenverschlüsselung in Amazon FSx for Lustre](#)

Scratch-Dateisysteme

Scratch-Dateisysteme sind für die temporäre Speicherung und die kurzfristige Verarbeitung von Daten konzipiert. Daten werden nicht repliziert und bleiben auch dann nicht erhalten, wenn ein Dateiserver ausfällt. Scratch-Dateisysteme bieten einen hohen Burst-Durchsatz, der bis zum Sechsfachen des Basisdurchsatzes von 200 MBps pro TiB Speicherkapazität beträgt. Weitere Informationen finden Sie unter [Aggregierte Dateisystemleistung](#).

Verwenden Sie Scratch-Dateisysteme, wenn Sie kostenoptimierten Speicher für kurzfristige, verarbeitungsintensive Workloads benötigen.

In einem Scratch-Dateisystem werden Dateiserver nicht ersetzt, wenn sie ausfallen und Daten nicht repliziert werden. Wenn ein Dateiserver oder eine Speicherfestplatte in einem Scratch-Dateisystem nicht mehr verfügbar ist, sind Dateien, die auf anderen Servern gespeichert sind, weiterhin zugänglich. Wenn Clients versuchen, auf Daten zuzugreifen, die sich auf dem nicht verfügbaren Server oder der Festplatte befinden, kommt es bei den Clients sofort zu einem I/O-Fehler.

Die folgende Tabelle zeigt die Verfügbarkeit oder Beständigkeit, für die Scratch-Dateisysteme mit Beispielgrößen im Laufe eines Tages und einer Woche konzipiert sind. Da größere Dateisysteme über mehr Dateiserver und mehr Festplatten verfügen, steigt die Ausfallwahrscheinlichkeit.

Dateisystemgröße (TiB)	Anzahl der Dateiserver	Verfügbarkeit/Haltbarkeit über einen Tag	Verfügbarkeit/Haltbarkeit über eine Woche
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%

Dateisystemgröße (TiB)	Anzahl der Dateiserver	Verfügbarkeit/Haltbarkeit über einen Tag	Verfügbarkeit/Haltbarkeit über eine Woche
50,4	22	99,1%	93,9%

Persistente Dateisysteme

Persistente Dateisysteme sind für längerfristige Speicherung und Workloads konzipiert. Die Dateiserver sind hochverfügbar, und Daten werden automatisch innerhalb derselben Availability Zone repliziert, in der sich das Dateisystem befindet. Die an die Dateiserver angeschlossenen Datenvolumen werden unabhängig von den Dateiservern repliziert, an die sie angeschlossen sind.

Amazon FSx überwacht persistente Dateisysteme kontinuierlich auf Hardwarefehler und ersetzt bei einem Ausfall automatisch Infrastrukturkomponenten. Wenn in einem persistenten Dateisystem ein Dateiserver nicht verfügbar ist, wird er innerhalb von Minuten nach dem Ausfall automatisch ersetzt. Während dieser Zeit werden Anfragen von Clients nach Daten auf diesem Server transparent wiederholt und sind schließlich erfolgreich, nachdem der Dateiserver ersetzt wurde. Daten auf persistenten Dateisystemen werden auf Festplatten repliziert, und ausgefallene Festplatten werden automatisch und transparent ersetzt.

Verwenden Sie persistente Dateisysteme für die längerfristige Speicherung und für durchsatzorientierte Workloads, die über einen längeren Zeitraum oder unbegrenzt ausgeführt werden und die empfindlich auf Verfügbarkeitsunterbrechungen reagieren können.

Persistente Bereitstellungstypen verschlüsseln automatisch Daten während der Übertragung, wenn auf sie von Amazon EC2 EC2-Instances zugegriffen wird, die Verschlüsselung bei der Übertragung unterstützen.

Amazon FSx for Lustre unterstützt zwei persistente Bereitstellungstypen: Persistent_1 und Persistent_2.

Bereitstellungstyp Persistent_2

Persistent_2 ist die neueste Generation des Bereitstellungstyps Persistent und eignet sich am besten für Anwendungsfälle, die eine längerfristige Speicherung erfordern und latenzempfindliche Workloads haben, die ein Höchstmaß an IOPS und Durchsatz erfordern. Die Bereitstellungstypen Persistent_2 unterstützen im Vergleich zu Persistent_1-Dateisystemen einen höheren Durchsatz pro

Speichereinheit und bieten vier Durchsatzstufen pro Speichereinheit: 125, 250, 500 und 1000 MB/s/TiB.

Wenn Sie bei der Erstellung eines Persistent_2-Dateisystems eine Metadatenkonfiguration angeben, können Sie die Leistung Ihrer Metadaten unabhängig von der Speicherkapazität Ihres Dateisystems im Laufe der Zeit erhöhen, um den steigenden Leistungsanforderungen gerecht zu werden und größere Workloads zu unterstützen.

Mithilfe der Amazon FSx-Konsole und der API können Sie persistent_2-Dateisysteme mit einem Metadaten-Konfigurationsmodus erstellen. AWS Command Line Interface

Bereitstellungstyp Persistent_1

Die Bereitstellungstypen Persistent_1 können auf Lustre 2.10 oder 2.12 basieren und unterstützen die Speichertypen SSD (Solid State Drive) und HDD (Hard Disk Drive). Der Bereitstellungstyp Persistent_1 eignet sich gut für Anwendungsfälle, in denen längerfristiger Speicher erforderlich ist und bei denen Workloads auf den Durchsatz ausgerichtet sind und nicht latenzempfindlich sind.

Für ein Persistent_1-Dateisystem mit SSD-Speicher beträgt der Durchsatz pro Speichereinheit entweder 50, 100 oder 200 MB/s pro Tebibyte (TiB). Für Festplattenspeicher beträgt der Persistent_1-Durchsatz pro Speichereinheit 12 oder 40 MB/s pro TiB.

Sie können Persistent_1-Bereitstellungstypen nur mithilfe der AWS CLI und der Amazon FSx-API erstellen.

Verfügbare Regionen

Persistente Bereitstellungstypen sind in den folgenden Ländern verfügbar AWS-Regionen:

AWS-Region	Persistent_1	Persistent_2
US East (Ohio)	✓	✓
USA Ost (Nord-Virginia)	✓	✓
Lokale Zone USA Ost (Atlanta)		✓ (Nur Persistent t 125 und 250)
USA West (Nordkalifornien)	✓	

AWS-Region	Persistent_1	Persistent_2
Lokale Zone USA West (Los Angeles)	✓	
USA West (Oregon)	✓	✓
Africa (Cape Town)	✓	
Asien-Pazifik (Hongkong)	✓	✓
Asien-Pazifik (Hyderabad)	✓	
Asien-Pazifik (Jakarta)	✓	
Asien-Pazifik (Melbourne)	✓	
Asien-Pazifik (Mumbai)	✓	✓
Asia Pacific (Osaka)	✓	
Asia Pacific (Seoul)	✓	✓
Asien-Pazifik (Singapur)	✓	✓
Asien-Pazifik (Sydney)	✓	✓
Asien-Pazifik (Tokio)	✓	✓
Canada (Central)	✓	✓
Kanada West (Calgary)		✓
		(Nur Persisten t 125 und 250)
Europe (Frankfurt)	✓	✓
Europa (Irland)	✓	✓
Europa (London)	✓	✓
Europa (Milan)	✓	

AWS-Region	Persistent_1	Persistent_2
Europa (Paris)	✓	
Europa (Spain)	✓	
Europa (Stockholm)	✓	✓
Europa (Zürich)	✓	
Israel (Tel Aviv)		✓ (Nur Persistent 125 und 250)
Naher Osten (Bahrain)	✓	
Naher Osten (VAE)	✓	
Südamerika (São Paulo)	✓	
AWS GovCloud (US-Ost)	✓	
AWS GovCloud (US-West)	✓	

Weitere Informationen zur Leistung von FSx for Lustre finden Sie unter [Aggregierte Dateisystemleistung](#)

Verwenden von Datenrepositories mit Amazon FSx for Lustre

Amazon FSx for Lustre bietet leistungsstarke Dateisysteme, die für eine schnelle Workload-Verarbeitung optimiert sind. Es kann Workloads wie maschinelles Lernen, Hochleistungsrechnen (HPC), Videoverarbeitung, Finanzmodellierung und elektronische Konstruktionsautomatisierung (EDA) unterstützen. Bei diesen Workloads müssen Daten in der Regel über eine skalierbare Hochgeschwindigkeits-Dateisystemschnittstelle für den Datenzugriff präsentiert werden. Oft werden die für diese Workloads verwendeten Datensätze in langfristigen Datenrepositories in Amazon S3 gespeichert. FSx for Lustre ist nativ in Amazon S3 integriert, was die Verarbeitung von Datensätzen mit dem Lustre-Dateisystem erleichtert.

Note

Dateisystem-Backups werden auf Dateisystemen, die mit einem Daten-Repository verknüpft sind, nicht unterstützt. Weitere Informationen finden Sie unter [Arbeiten mit Backups](#).


Themen

- [Überblick über Datenrepositories](#)
- [Unterstützung von POSIX-Metadaten für Daten-Repositories](#)
- [Ihr Dateisystem mit einem S3-Bucket verknüpfen](#)
- [Änderungen aus Ihrem Daten-Repository importieren](#)
- [Änderungen in das Daten-Repository exportieren](#)
- [Datenrepository-Aufgaben](#)
- [Dateien werden freigegeben](#)
- [Amazon FSx mit Ihren lokalen Daten verwenden](#)
- [Datenrepository-Ereignisprotokolle](#)
- [Mit älteren Bereitstellungstypen arbeiten](#)

Überblick über Datenrepositories

Wenn Sie Amazon FSx for Lustre mit Datenrepositories verwenden, können Sie große Mengen an Dateidaten in einem Hochleistungsdateisystem aufnehmen und verarbeiten, indem Sie automatische Import- und Import-Daten-Repository-Aufgaben verwenden. Gleichzeitig können Sie mithilfe von

Aufgaben zum automatischen Export oder Export von Datenrepositorys Ergebnisse in Ihre Daten-Repositorys schreiben. Mit diesen Funktionen können Sie Ihren Workload jederzeit neu starten und dabei die neuesten Daten verwenden, die in Ihrem Daten-Repository gespeichert sind.


 Note

Datenrepository-Verknüpfungen, automatischer Export und Unterstützung für mehrere Datenrepositorien sind auf FSx for Lustre 2.10-Dateisystemen oder Dateisystemen nicht verfügbar. Scratch 1

FSx for Lustre ist tief in Amazon S3 integriert. Diese Integration bedeutet, dass Sie über Anwendungen, die Ihr FSx for Lustre-Dateisystem mounten, nahtlos auf die in Ihren Amazon S3 S3-Buckets gespeicherten Objekte zugreifen können. Sie können Ihre rechenintensiven Workloads auch auf Amazon EC2 EC2-Instances in der ausführen AWS Cloud und die Ergebnisse nach Abschluss Ihrer Arbeitslast in Ihr Daten-Repository exportieren.

Um auf Objekte im Amazon S3 S3-Daten-Repository als Dateien und Verzeichnisse im Dateisystem zugreifen zu können, müssen Datei- und Verzeichnismetadaten in das Dateisystem geladen werden. Sie können Metadaten aus einem verknüpften Datenrepository laden, wenn Sie eine Datenrepository-Zuordnung erstellen.

Darüber hinaus können Sie Datei- und Verzeichnismetadaten mithilfe des automatischen Imports oder mithilfe einer Aufgabe zum Importieren eines Datenrepositorys aus Ihren verknüpften Datenrepositorys in das Dateisystem importieren. Wenn Sie den automatischen Import für eine Datenrepository-Zuordnung aktivieren, importiert Ihr Dateisystem automatisch Dateimetadaten, wenn Dateien im S3-Datenrepository erstellt, geändert und/oder gelöscht werden. Alternativ können Sie Metadaten für neue oder geänderte Dateien und Verzeichnisse mithilfe einer Aufgabe zum Importieren eines Datenrepositorys importieren.

 Note

Aufgaben zum automatischen Importieren und Importieren von Datenrepositorys können gleichzeitig in einem Dateisystem verwendet werden.

Sie können Dateien und die zugehörigen Metadaten in Ihrem Dateisystem auch mithilfe des automatischen Exports oder mithilfe einer Aufgabe zum Exportieren eines Datenrepositorys in

Ihr Datenrepository exportieren. Wenn Sie den automatischen Export für eine Datenrepository-Zuordnung aktivieren, exportiert Ihr Dateisystem automatisch Dateidaten und Metadaten, wenn Dateien erstellt, geändert oder gelöscht werden. Alternativ können Sie Dateien oder Verzeichnisse mithilfe einer Aufgabe zum Exportieren eines Datenrepositorys exportieren. Wenn Sie eine Aufgabe zum Exportieren eines Datenrepositorys verwenden, werden Dateidaten und Metadaten exportiert, die seit der letzten Aufgabe erstellt oder geändert wurden.

Note

- Aufgaben zum automatischen Exportieren und Exportieren von Datenrepositorys können nicht gleichzeitig in einem Dateisystem ausgeführt werden.
- Datenrepository-Verknüpfungen exportieren nur reguläre Dateien, Symlinks und Verzeichnisse. Das bedeutet, dass alle anderen Dateitypen (FIFO Special, Block Special, Character Special und Socket) nicht im Rahmen von Exportprozessen wie automatischem Export und Export von Datenrepositorys exportiert werden.

FSx for Lustre unterstützt auch Cloud-Bursting-Workloads mit lokalen Dateisystemen, indem es Ihnen ermöglicht, Daten von lokalen Clients mithilfe von VPN zu kopieren. AWS Direct Connect

Important

Wenn Sie ein oder mehrere FSx for Lustre-Dateisysteme mit einem Daten-Repository auf Amazon S3 verknüpft haben, löschen Sie den Amazon S3 S3-Bucket erst, wenn Sie alle verknüpften Dateisysteme gelöscht oder die Verknüpfung aufgehoben haben.

Unterstützung von POSIX-Metadaten für Daten-Repositorys

Amazon FSx for Lustre überträgt automatisch POSIX-Metadaten (Portable Operating System Interface) für Dateien, Verzeichnisse und symbolische Links (Symlinks), wenn Daten in und aus einem Linked Data Repository auf Amazon S3 importiert und exportiert werden. Wenn Sie Änderungen in Ihrem Dateisystem in das verknüpfte Daten-Repository exportieren, exportiert FSx for Lustre auch POSIX-Metadatenänderungen als S3-Objektmetadaten. Das bedeutet, dass, wenn ein anderes FSx for Lustre-Dateisystem dieselben Dateien aus S3 importiert, die Dateien dieselben POSIX-Metadaten in diesem Dateisystem haben, einschließlich Eigentum und Berechtigungen.

FSx for Lustre importiert nur S3-Objekte, die POSIX-konforme Objektschlüssel haben, wie die folgenden.

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

FSx for Lustre speichert Verzeichnisse und Symlinks als separate Objekte im Linked Data Repository auf S3. Für Verzeichnisse erstellt FSx for Lustre ein S3-Objekt mit einem Schlüsselnamen, der mit einem Schrägstrich („/“) endet, wie folgt:


- Der S3-Objektschlüssel `mydir/` ist dem Verzeichnis FSx for Lustre zugeordnet. `mydir/`
- Der S3-Objektschlüssel `mydir/mysubdir/` ist dem Verzeichnis FSx for Lustre zugeordnet. `mydir/mysubdir/`

Für Symlinks verwendet FSx for Lustre das folgende Amazon S3 S3-Schema:

- S3-Objektschlüssel — Der Pfad zum Link, relativ zum FSx for Lustre-Mount-Verzeichnis
- S3-Objektdatei — Der Zielpfad dieses Symlinks
- S3-Objektmetadaten — Die Metadaten für den Symlink

FSx for Lustre speichert POSIX-Metadaten, einschließlich Besitz, Berechtigungen und Zeitstempel für Dateien, Verzeichnisse und symbolische Links, in S3-Objekten wie folgt:

- Content-Type— Der HTTP-Entity-Header, der verwendet wird, um den Medientyp der Ressource für Webbrowser anzugeben.
- `x-amz-meta-file-permissions`— Der Dateityp und die Berechtigungen in dem Format `<octal file type><octal permission mask>`, das mit `st_mode` der [Linux-Manpage stat \(2\)](#) übereinstimmt.

 Note

FSx for Lustre importiert oder speichert `setuid` keine Informationen.

- `x-amz-meta-file-owner`— Die Benutzer-ID (UID) des Besitzers, ausgedrückt als Ganzzahl.
- `x-amz-meta-file-group`— Die Gruppen-ID (GID), ausgedrückt als Ganzzahl.

- `x-amz-meta-file-atime`— Die Zeit des letzten Zugriffs in Nanosekunden seit Beginn der Unix-Epoche. Beenden Sie den Zeitwert mit `ns`; andernfalls interpretiert FSx for Lustre den Wert als Millisekunden.
- `x-amz-meta-file-mtime`— Die letzte Änderung in Nanosekunden seit Beginn der Unix-Epoche. Beenden Sie den Zeitwert mit `ns`; andernfalls interpretiert FSx for Lustre den Wert als Millisekunden.
- `x-amz-meta-user-agent`— Der Benutzeragent, der beim Import von FSx for Lustre ignoriert wurde. Während des Exports setzt FSx for Lustre diesen Wert auf `aws-fsx-lustre`

Beim Import von Objekten aus S3, denen keine POSIX-Berechtigungen zugeordnet sind, lautet die POSIX-Standardberechtigung, die FSx for Lustre einer Datei zuweist. Diese Berechtigung ermöglicht Lese- und Ausführungszugriff für alle Benutzer und Schreibzugriff für den Eigentümer der Datei.

Note

FSx for Lustre speichert keine benutzerdefinierten benutzerdefinierten Metadaten für S3-Objekte.

Harte Links und Export nach S3

Wenn der automatische Export (mit NEUEN und GEÄNDERTEN Richtlinien) für einen DRA in Ihrem Dateisystem aktiviert ist, wird jeder im DRA enthaltene Hardlink als separates S3-Objekt für jeden Hardlink nach Amazon S3 exportiert. Wenn eine Datei mit mehreren Hardlinks im Dateisystem geändert wird, werden alle Kopien in S3 aktualisiert, unabhängig davon, welcher Hardlink beim Ändern der Datei verwendet wurde.

Wenn Hardlinks mithilfe von Data Repository Tasks (DRTs) nach S3 exportiert werden, wird jeder Hardlink, der in den für das DRT angegebenen Pfaden enthalten ist, als separates S3-Objekt für jeden Hardlink nach S3 exportiert. Wenn eine Datei mit mehreren Hardlinks im Dateisystem geändert wird, wird jede Kopie in S3 zum Zeitpunkt des Exports des jeweiligen Hardlinks aktualisiert, unabhängig davon, welcher Hardlink beim Ändern der Datei verwendet wurde.

⚠ Important

Wenn ein neues FSx for Lustre-Dateisystem mit einem S3-Bucket verknüpft wird, in den Hardlinks zuvor von einem anderen FSx for Lustre-Dateisystem oder Amazon FSx File Gateway exportiert wurden, werden die Hardlinks anschließend als separate Dateien in das neue Dateisystem importiert. AWS DataSync

Harte Links und veröffentlichte Dateien

Eine veröffentlichte Datei ist eine Datei, deren Metadaten im Dateisystem vorhanden sind, deren Inhalt jedoch nur in S3 gespeichert ist. Weitere Informationen zu veröffentlichten Dateien finden Sie unter [Dateien werden freigegeben](#).

⚠ Important

Die Verwendung von Hardlinks in einem Dateisystem mit Data Repository Associations (DRAs) unterliegt den folgenden Einschränkungen:

- Das Löschen und Neuerstellen einer veröffentlichten Datei mit mehreren Hardlinks kann dazu führen, dass der Inhalt aller Hardlinks überschrieben wird.
- Durch das Löschen einer veröffentlichten Datei werden Inhalte von allen Hardlinks gelöscht, die sich außerhalb einer Datenrepository-Zuordnung befinden.
- Durch das Erstellen eines Hardlinks zu einer veröffentlichten Datei, deren entsprechendes S3-Objekt sich in einer der Speicherklassen S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive befindet, wird in S3 kein neues Objekt für den Hardlink erstellt.

Exemplarische Vorgehensweise: Anhängen von POSIX-Berechtigungen beim Hochladen von Objekten in einen Amazon S3 S3-Bucket

Das folgende Verfahren führt Sie durch den Prozess des Hochladens von Objekten in Amazon S3 mit POSIX-Berechtigungen. Auf diese Weise können Sie die POSIX-Berechtigungen importieren, wenn Sie ein Amazon FSx-Dateisystem erstellen, das mit diesem S3-Bucket verknüpft ist.

Um Objekte mit POSIX-Berechtigungen auf Amazon S3 hochzuladen

1. Verwenden Sie von Ihrem lokalen Computer oder Computer aus die folgenden Beispielbefehle, um ein Testverzeichnis (`s3cptestdir`) und eine Datei (`s3cptest.txt`) zu erstellen, die in den S3-Bucket hochgeladen werden.

```
$ 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
```

Die neu erstellte Datei und das neu erstellte Verzeichnis haben eine Benutzer-ID (UID) des Dateibesitzers und eine Gruppen-ID (GID) von 500 sowie Berechtigungen, wie im vorherigen Beispiel gezeigt.

2. Rufen Sie die Amazon S3 S3-API auf, um das Verzeichnis `s3cptestdir` mit Metadatenberechtigungen zu erstellen. Sie müssen den Verzeichnisnamen mit einem abschließenden Schrägstrich (`/`) angeben. Hinweise zu unterstützten POSIX-Metadaten finden Sie unter [Unterstützung von POSIX-Metadaten für Daten-Repositorys](#)

bucket_name Ersetzen Sie es durch den tatsächlichen Namen Ihres S3-Buckets.

```
$ 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. Stellen Sie sicher, dass die POSIX-Berechtigungen mit S3-Objektmetadaten gekennzeichnet sind.

```
$ 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": "1595002920000000000ns",
    "file-owner": "500",
    "file-permissions": "0100664",
    "file-group": "500",
    "file-mtime": "1595002920000000000ns"
  }
}

```

4. Laden Sie die Testdatei (erstellt in Schritt 1) von Ihrem Computer in den S3-Bucket mit Metadatenberechtigungen hoch.

```

$ aws s3 cp s3cptestdir/s3cptest.txt s3://bucket_name/s3cptestdir/s3cptest.txt \
  --metadata '{"user-agent":"aws-fsx-lustre" , "file-
atime":"1595002920000000000ns" , \
  "file-owner":"500" , "file-permissions":"0100664","file-group":"500" , "file-
mtime":"1595002920000000000ns"}'

```

5. Stellen Sie sicher, dass die POSIX-Berechtigungen mit den Metadaten des S3-Objekts gekennzeichnet sind.

```

$ 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": "1595002920000000000ns",
    "file-owner": "500",
    "file-permissions": "0100664",
    "file-group": "500",
    "file-mtime": "1595002920000000000ns"
  }
}

```

6. Überprüfen Sie die Berechtigungen für das Amazon FSx-Dateisystem, das mit dem S3-Bucket verknüpft ist.

```

$ 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

```

Sowohl für das `s3cptestdir` Verzeichnis als auch für die `s3cptest.txt` Datei wurden POSIX-Berechtigungen importiert.

Ihr Dateisystem mit einem S3-Bucket verknüpfen

Sie können Ihr Amazon FSx for Lustre-Dateisystem mit Datenrepositoys in Amazon S3 verknüpfen. Sie können den Link bei der Erstellung des Dateisystems oder zu einem beliebigen Zeitpunkt nach der Erstellung des Dateisystems erstellen.

Eine Verbindung zwischen einem Verzeichnis im Dateisystem und einem S3-Bucket oder -Präfix wird als Data Repository Association (DRA) bezeichnet. Sie können maximal 8 Datenrepository-Verknüpfungen auf einem FSx for Lustre-Dateisystem konfigurieren. Es können maximal 8 DRA-Anfragen in die Warteschlange gestellt werden, es kann jedoch jeweils nur eine Anfrage für das Dateisystem bearbeitet werden. Jeder DRA muss über ein eindeutiges FSx for Lustre-Dateisystemverzeichnis und einen eindeutigen S3-Bucket oder -Präfix verfügen, der diesem zugeordnet ist.

Note

Datenrepository-Verknüpfungen, automatischer Export und Unterstützung für mehrere Datenrepositorien sind auf FSx for Lustre 2.10-Dateisystemen oder Dateisystemen nicht verfügbar. [Scratch 1](#)

Um auf Objekte im S3-Datenrepository als Dateien und Verzeichnisse im Dateisystem zugreifen zu können, müssen Datei- und Verzeichnismetadaten in das Dateisystem geladen werden. Sie

können Metadaten aus einem verknüpften Datenrepository laden, wenn Sie den DRA erstellen, oder Metadaten für Batches von Dateien und Verzeichnissen laden, auf die Sie zu einem späteren Zeitpunkt mit dem FSx for Lustre-Dateisystem zugreifen möchten, oder den automatischen Export verwenden, um Metadaten automatisch zu laden, wenn Objekte zum Datenrepository hinzugefügt, darin geändert oder gelöscht werden.

Sie können ein DRA nur für den automatischen Import, nur für den automatischen Export oder für beide konfigurieren. Eine Datenrepository-Zuordnung, die sowohl für den automatischen Import als auch für den automatischen Export konfiguriert ist, überträgt Daten in beide Richtungen zwischen dem Dateisystem und dem verknüpften S3-Bucket. Wenn Sie Änderungen an Daten in Ihrem S3-Datenrepository vornehmen, erkennt FSx for Lustre die Änderungen und importiert die Änderungen dann automatisch in Ihr Dateisystem. Wenn Sie Dateien erstellen, ändern oder löschen, exportiert FSx for Lustre die Änderungen automatisch asynchron nach Amazon S3, sobald Ihre Anwendung die Änderung der Datei abgeschlossen hat.

Important

- Wenn Sie dieselbe Datei sowohl im Dateisystem als auch im S3-Bucket ändern, sollten Sie die Koordination auf Anwendungsebene sicherstellen, um Konflikte zu vermeiden. FSx for Lustre verhindert nicht widersprüchliche Schreibvorgänge an mehreren Standorten.
- Bei Dateien, die mit einem unveränderlichen Attribut gekennzeichnet sind, kann FSx for Lustre keine Änderungen zwischen Ihrem FSx for Lustre-Dateisystem und einem mit dem Dateisystem verknüpften S3-Bucket synchronisieren. Das Setzen einer unveränderlichen Markierung für einen längeren Zeitraum kann dazu führen, dass sich die Leistung der Datenbewegung zwischen Amazon FSx und S3 verschlechtert.

Wenn Sie eine Datenrepository-Zuordnung erstellen, können Sie die folgenden Eigenschaften konfigurieren:

- Dateisystempfad — Geben Sie einen lokalen Pfad im Dateisystem ein, der auf ein Verzeichnis (z. B. /ns1/) oder ein Unterverzeichnis (z. B. /ns1/subdir/) verweist, das one-to-one dem unten angegebenen Datenrepository-Pfad zugeordnet wird. Der führende Schrägstrich im Namen ist erforderlich. Zwei Daten-Repository-Verknüpfungen dürfen keine überlappenden Dateisystempfade haben. Wenn beispielsweise ein Daten-Repository dem Dateisystempfad /ns1 zugeordnet ist, können Sie kein anderes Daten-Repository mit dem Dateisystempfad /ns1/ns2 verknüpfen.

Note

Wenn Sie als Dateisystempfad nur einen Schrägstrich (/) angeben, können Sie nur ein Daten-Repository mit dem Dateisystem verknüpfen. Sie können „/“ nur als Dateisystempfad für das erste Daten-Repository angeben, das einem Dateisystem zugeordnet ist.

- **Datenrepository-Pfad** — Geben Sie einen Pfad im S3-Datenrepository ein. Der Pfad kann ein S3-Bucket oder ein Präfix im Format `s3://myBucket/myPrefix/` sein. Diese Eigenschaft gibt an, aus welchem Bereich des S3-Datenrepositorys Dateien importiert oder exportiert werden. FSx for Lustre hängt ein abschließendes „/“ an Ihren Datenrepository-Pfad an, falls Sie keinen angeben. Wenn Sie beispielsweise einen Datenrepository-Pfad von `angebens3://myBucket/myPrefix`, interpretiert FSx for Lustre ihn als `s3://myBucket/myPrefix/`

Zwei Datenrepository-Assoziationen dürfen sich nicht überlappen. Wenn beispielsweise ein Datenrepository mit Pfad mit dem Dateisystem verknüpft `s3://myBucket/myPrefix/` ist, können Sie keine weitere Datenrepository-Assoziation mit dem Datenrepository-Pfad `s3://myBucket/myPrefix/mySubPrefix` erstellen.

- **Metadaten aus dem Repository importieren** — Sie können diese Option auswählen, um Metadaten aus dem gesamten Datenrepository unmittelbar nach der Erstellung der Datenrepository-Zuordnung zu importieren. Alternativ können Sie jederzeit, nachdem die Datenrepository-Zuordnung erstellt wurde, eine Aufgabe zum Importieren des Datenrepositorys ausführen, um alle oder einen Teil der Metadaten aus dem verknüpften Datenrepository in das Dateisystem zu laden.
- **Einstellungen importieren** — Wählen Sie eine Importrichtlinie, die den Typ der aktualisierten Objekte (eine beliebige Kombination aus neuen, geänderten und gelöschten Objekten) festlegt, die automatisch aus dem verknüpften S3-Bucket in Ihr Dateisystem importiert werden. Der automatische Import (neu, geändert, gelöscht) ist standardmäßig aktiviert, wenn Sie ein Daten-Repository über die Konsole hinzufügen, ist jedoch standardmäßig deaktiviert, wenn Sie die AWS CLI oder Amazon FSx-API verwenden.
- **Exporteinstellungen** — Wählen Sie eine Exportrichtlinie, die den Typ der aktualisierten Objekte (eine beliebige Kombination aus neuen, geänderten und gelöschten Objekten) festlegt, die automatisch in den S3-Bucket exportiert werden. Der automatische Export (neu, geändert, gelöscht) ist standardmäßig aktiviert, wenn Sie ein Daten-Repository über die Konsole hinzufügen, ist jedoch standardmäßig deaktiviert, wenn Sie die AWS CLI oder Amazon FSx-API verwenden.

Die Einstellungen Dateisystempfad und Datenrepository-Pfad bieten eine 1:1 -Zuordnung zwischen Pfaden in Amazon FSx und Objektschlüsseln in S3.

Regions- und Kontounterstützung für verknüpfte S3-Buckets

Beachten Sie beim Erstellen von Links zu S3-Buckets die folgenden Einschränkungen der Regions- und Kontounterstützung:

- Der automatische Export unterstützt regionsübergreifende Konfigurationen. Das Amazon FSx-Dateisystem und der verknüpfte S3-Bucket können sich im selben AWS-Region oder in einem anderen AWS-Regionen befinden.
- Der automatische Import unterstützt keine regionsübergreifenden Konfigurationen. Sowohl das Amazon FSx-Dateisystem als auch der verknüpfte S3-Bucket müssen sich im selben AWS-Region befinden.
- Sowohl der automatische Export als auch der automatische Import unterstützen kontoübergreifende Konfigurationen. Das Amazon FSx-Dateisystem und der verknüpfte S3-Bucket können zu demselben AWS-Konto oder zu einem anderen AWS-Konten gehören.

Einen Link zu einem S3-Bucket erstellen

Die folgenden Verfahren führen Sie durch den Prozess der Erstellung einer Datenrepository-Zuordnung für ein FSx for Lustre-Dateisystem zu einem vorhandenen S3-Bucket mithilfe von AWS Management Console und AWS Command Line Interface (AWS CLI). Informationen zum Hinzufügen von Berechtigungen zu einem S3-Bucket, um ihn mit Ihrem Dateisystem zu verknüpfen, finden Sie unter [Hinzufügen von Berechtigungen zur Verwendung von Datenrepositorys in Amazon S3](#)

Note

Datenrepositorys können nicht mit Dateisystemen verknüpft werden, für die Dateisystem-Backups aktiviert sind. Deaktivieren Sie Backups, bevor Sie eine Verbindung zu einem Daten-Repository herstellen.

Um einen S3-Bucket beim Erstellen eines Dateisystems (Konsole) zu verknüpfen

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, das [Erstellen Sie Ihr FSx for Lustre-Dateisystem](#) im Abschnitt Erste Schritte beschrieben ist.

3. Öffnen Sie den Abschnitt Datenrepository-Import/Export — optional. Die Funktion ist standardmäßig deaktiviert.
4. Wählen Sie Daten importieren aus und exportieren Sie Daten nach S3.
5. Geben Sie im Dialogfeld Informationen zur Datenrepository-Zuordnung Informationen für die folgenden Felder ein.
 - Dateisystempfad: Geben Sie den Namen eines Verzeichnisses auf hoher Ebene (z. B./ns1) oder eines Unterverzeichnisses (z. B./ns1/subdir) innerhalb des Amazon FSx-Dateisystems ein, das mit dem S3-Daten-Repository verknüpft wird. Der führende Schrägstrich im Pfad ist erforderlich. Zwei Daten-Repository-Verknüpfungen dürfen keine überlappenden Dateisystempfade haben. Wenn beispielsweise ein Daten-Repository dem Dateisystempfad /ns1 zugeordnet ist, können Sie kein anderes Daten-Repository mit dem Dateisystempfad /ns1/ns2 verknüpfen. Die Einstellung für den Dateisystempfad muss für alle Datenrepository-Verknüpfungen für das Dateisystem eindeutig sein.
 - Datenrepository-Pfad: Geben Sie den Pfad eines vorhandenen S3-Buckets oder ein Präfix ein, das Sie Ihrem Dateisystem zuordnen möchten (z. B.s3://my-bucket/my-prefix/). Zwei Datenrepository-Verknüpfungen dürfen sich nicht überlappen. Wenn beispielsweise ein Datenrepository mit dem Pfad mit dem Dateisystem verknüpft s3://myBucket/myPrefix/ ist, können Sie keine weitere Datenrepository-Assoziation mit dem Datenrepository-Pfad s3://myBucket/myPrefix/mySubPrefix erstellen. Die Einstellung für den Datenrepository-Pfad muss für alle Datenrepository-Verknüpfungen für das Dateisystem eindeutig sein.
 - Metadaten aus dem Repository importieren: Wählen Sie diese Eigenschaft, um optional eine Aufgabe zum Importieren eines Datenrepositorys auszuführen, um Metadaten unmittelbar nach der Erstellung des Links zu importieren.

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. Legen Sie für Importeinstellungen — optional — eine Importrichtlinie fest, die festlegt, wie Ihre Datei- und Verzeichnislisten auf dem neuesten Stand gehalten werden, wenn Sie Objekte in Ihrem S3-Bucket hinzufügen, ändern oder löschen. Wählen Sie beispielsweise Neu aus, um Metadaten für neue Objekte, die im S3-Bucket erstellt wurden, in Ihr Dateisystem zu importieren. Weitere Informationen zu Importrichtlinien finden Sie unter [Automatisches Importieren von Updates aus Ihrem S3-Bucket](#).

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. Legen Sie unter Exportrichtlinie eine Exportrichtlinie fest, die festlegt, wie Ihre Dateien in Ihren verknüpften S3-Bucket exportiert werden, wenn Sie Objekte in Ihrem Dateisystem hinzufügen,

ändern oder löschen. Wählen Sie beispielsweise Geändert, um Objekte zu exportieren, deren Inhalt oder Metadaten in Ihrem Dateisystem geändert wurden. Weitere Informationen zu Exportrichtlinien finden Sie unter [Exportieren Sie Updates automatisch in Ihren S3-Bucket](#).

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	<input checked="" type="checkbox"/>
Export new files and directories to the repository as they are added to the file system	
Changed	<input checked="" type="checkbox"/>
Export changes to files and directories on the file system to the repository	
Deleted	<input checked="" type="checkbox"/>
Delete files and directories on the data repository when they are deleted from the file system	

8. Fahren Sie mit dem nächsten Abschnitt des Assistenten zum Erstellen von Dateisystemen fort.

Um einen S3-Bucket mit einem vorhandenen Dateisystem (Konsole) zu verknüpfen

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Dashboard Dateisysteme und dann das Dateisystem aus, für das Sie eine Datenrepository-Zuordnung erstellen möchten.
3. Wählen Sie die Registerkarte Datenrepository.
4. Wählen Sie im Bereich Datenrepository-Verknüpfungen die Option Datenrepository-Zuordnung erstellen aus.
5. Geben Sie im Dialogfeld Informationen zur Datenrepository-Zuordnung Informationen für die folgenden Felder ein.
 - Dateisystempfad: Geben Sie den Namen eines Verzeichnisses auf hoher Ebene (z. B./ns1) oder eines Unterverzeichnisses (z. B./ns1/subdir) innerhalb des Amazon FSx-Dateisystems ein, das mit dem S3-Daten-Repository verknüpft wird. Der führende Schrägstrich im Pfad ist erforderlich. Zwei Daten-Repository-Verknüpfungen dürfen keine überlappenden

Dateisystempfade haben. Wenn beispielsweise ein Daten-Repository dem Dateisystempfad `/ns1` zugeordnet ist, können Sie kein anderes Daten-Repository mit dem Dateisystempfad `/ns1/ns2` verknüpfen. Die Einstellung für den Dateisystempfad muss für alle Datenrepository-Verknüpfungen für das Dateisystem eindeutig sein.

- **Datenrepository-Pfad:** Geben Sie den Pfad eines vorhandenen S3-Buckets oder ein Präfix ein, das Sie Ihrem Dateisystem zuordnen möchten (z. B. `s3://my-bucket/my-prefix/`). Zwei Datenrepository-Verknüpfungen dürfen sich nicht überlappen. Wenn beispielsweise ein Datenrepository mit Pfad mit dem Dateisystem verknüpft `s3://myBucket/myPrefix/` ist, können Sie keine weitere Datenrepository-Assoziation mit dem Datenrepository-Pfad `s3://myBucket/myPrefix/mySubPrefix` erstellen. Die Einstellung für den Datenrepository-Pfad muss für alle Datenrepository-Verknüpfungen für das Dateisystem eindeutig sein.
- **Metadaten aus dem Repository importieren:** Wählen Sie diese Eigenschaft, um optional eine Aufgabe zum Importieren eines Datenrepositorys auszuführen, um Metadaten unmittelbar nach der Erstellung des Links zu importieren.

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. Legen Sie für Importeinstellungen — optional — eine Importrichtlinie fest, die festlegt, wie Ihre Datei- und Verzeichnislisten auf dem neuesten Stand gehalten werden, wenn Sie Objekte in Ihrem S3-Bucket hinzufügen, ändern oder löschen. Wählen Sie beispielsweise Neu aus, um Metadaten für neue Objekte, die im S3-Bucket erstellt wurden, in Ihr Dateisystem zu importieren.

Weitere Informationen zu Importrichtlinien finden Sie unter [Automatisches Importieren von Updates aus Ihrem S3-Bucket](#).

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

- Legen Sie unter Exportrichtlinie eine Exportrichtlinie fest, die festlegt, wie Ihre Dateien in Ihren verknüpften S3-Bucket exportiert werden, wenn Sie Objekte in Ihrem Dateisystem hinzufügen, ändern oder löschen. Wählen Sie beispielsweise Geändert, um Objekte zu exportieren, deren Inhalt oder Metadaten in Ihrem Dateisystem geändert wurden. Weitere Informationen zu Exportrichtlinien finden Sie unter [Exportieren Sie Updates automatisch in Ihren S3-Bucket](#).

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 <input checked="" type="checkbox"/> Export new files and directories to the repository as they are added to the file system	Changed <input checked="" type="checkbox"/> Export changes to files and directories on the file system to the repository	Deleted <input checked="" type="checkbox"/> Delete files and directories on the data repository when they are deleted from the file system
---	--	--

- Wählen Sie Erstellen.

Um ein Dateisystem mit einem S3-Bucket zu verknüpfen (AWS CLI)

Das folgende Beispiel erstellt eine Datenrepository-Zuordnung, die ein Amazon FSx-Dateisystem mit einem S3-Bucket verknüpft, mit einer Importrichtlinie, die alle neuen oder geänderten Dateien in das Dateisystem importiert, und einer Exportrichtlinie, die neue, geänderte oder gelöschte Dateien in den verknüpften S3-Bucket exportiert.

- Um eine Datenrepository-Zuordnung zu erstellen, verwenden Sie den Amazon FSx CLI-Befehl `create-data-repository-association`, wie im Folgenden gezeigt.

```
$ 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 gibt die JSON-Beschreibung des DRA sofort zurück. Der DRA wird asynchron erstellt.

Sie können diesen Befehl verwenden, um eine Datenrepository-Verknüpfung zu erstellen, noch bevor das Dateisystem die Erstellung abgeschlossen hat. Die Anfrage wird in die Warteschlange gestellt und die Datenrepository-Zuordnung wird erstellt, sobald das Dateisystem verfügbar ist.

Einstellungen für die Datenrepository-Zuordnung werden aktualisiert

Sie können die Einstellungen einer bestehenden Datenrepository-Verknüpfung mithilfe der AWS Management Console AWS CLI, der und der Amazon FSx-API aktualisieren, wie in den folgenden Verfahren gezeigt.

Note

Sie können das `file system path` oder `Data repository path` eines DRA nicht aktualisieren, nachdem es erstellt wurde. Wenn Sie das `file system path` Oder ändern möchten `Data repository path`, müssen Sie das DRA löschen und erneut erstellen.

So aktualisieren Sie die Einstellungen für eine bestehende Datenrepository-Zuordnung (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Dashboard Dateisysteme und dann das Dateisystem aus, das Sie verwalten möchten.
3. Wählen Sie die Registerkarte Daten-Repository.
4. Wählen Sie im Bereich Datenrepository-Verknüpfungen die Datenrepository-Zuordnung aus, die Sie ändern möchten.

5. Wählen Sie Aktualisieren. Für die Datenrepository-Zuordnung wird ein Bearbeitungsdiaologfeld angezeigt.
6. Unter Importeinstellungen — optional können Sie Ihre Importrichtlinie aktualisieren. Weitere Informationen zu Importrichtlinien finden Sie unter [Automatisches Importieren von Updates aus Ihrem S3-Bucket](#).
7. Unter Exporteinstellungen — optional können Sie Ihre Exportrichtlinie aktualisieren. Weitere Informationen zu Exportrichtlinien finden Sie unter [Exportieren Sie Updates automatisch in Ihren S3-Bucket](#).
8. Wählen Sie Aktualisieren.

So aktualisieren Sie die Einstellungen für eine bestehende Datenrepository-Zuordnung (CLI)

- Um eine Datenrepository-Zuordnung zu aktualisieren, verwenden Sie den Amazon FSx CLI-Befehl `update-data-repository-association`, wie im Folgenden gezeigt.

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

Nach erfolgreicher Aktualisierung der Import- und Exportrichtlinien der Daten-Repository-Verknüpfung gibt Amazon FSx die Beschreibung der aktualisierten Daten-Repository-Zuordnung als JSON zurück.

Löschen einer Zuordnung zu einem S3-Bucket

Die folgenden Verfahren führen Sie durch den Prozess des Löschens einer Datenrepository-Zuordnung von einem vorhandenen Amazon FSx-Dateisystem zu einem vorhandenen S3-Bucket mithilfe von AWS Management Console und AWS Command Line Interface (AWS CLI). Durch das Löschen der Datenrepository-Zuordnung wird die Verknüpfung des Dateisystems mit dem S3-Bucket aufgehoben.

Um einen Link von einem Dateisystem zu einem S3-Bucket (Konsole) zu löschen

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Dashboard Dateisysteme und dann das Dateisystem aus, aus dem Sie eine Datenrepository-Zuordnung löschen möchten.
3. Wählen Sie die Registerkarte Datenrepository.

4. Wählen Sie im Bereich Datenrepository-Verknüpfungen die Datenrepository-Zuordnung aus, die Sie löschen möchten.
5. Wählen Sie für Aktionen die Option Verknüpfung löschen aus.
6. (Optional) Im Dialogfeld Löschen können Sie Daten im Dateisystem löschen auswählen, um die Daten im Dateisystem, die der Datenrepository-Zuordnung entsprechen, physisch zu löschen.
7. Wählen Sie Löschen, um die Datenrepository-Zuordnung aus dem Dateisystem zu entfernen.

Um einen Link von einem Dateisystem zu einem S3-Bucket zu löschen (AWS CLI)

Das folgende Beispiel löscht eine Datenrepository-Zuordnung, die ein Amazon FSx-Dateisystem mit einem S3-Bucket verknüpft. Der `--association-id` Parameter gibt die ID der Datenrepository-Zuordnung an, die gelöscht werden soll.

- Um eine Datenrepository-Zuordnung zu löschen, verwenden Sie den Amazon FSx CLI-Befehl `delete-data-repository-association`, wie im Folgenden gezeigt.

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

Nach dem erfolgreichen Löschen der Datenrepository-Zuordnung gibt Amazon FSx die Beschreibung als JSON zurück.

Details zur Datenrepository-Zuordnung anzeigen

Sie können die Details einer Datenrepository-Zuordnung mithilfe der FSx for Lustre-Konsole, der AWS CLI, der API anzeigen. Zu den Details gehören die Zuordnungs-ID des DRA, der Dateisystempfad, der Datenrepository-Pfad, die Importeinstellungen, die Exporteinstellungen, der Status und die ID des zugehörigen Dateisystems.

Um DRA-Details anzuzeigen (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Dashboard Dateisysteme und dann das Dateisystem aus, für das Sie die Details einer Datenrepository-Zuordnung anzeigen möchten.
3. Wählen Sie die Registerkarte Daten-Repository.

4. Wählen Sie im Bereich Datenrepository-Verknüpfungen die Datenrepository-Zuordnung aus, die Sie anzeigen möchten. Die Übersichtsseite mit den DRA-Details wird angezeigt.

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

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

So zeigen Sie DRA-Details an (CLI)

- Um die Details einer bestimmten Datenrepository-Zuordnung anzuzeigen, verwenden Sie den Amazon FSx CLI-Befehl `describe-data-repository-associations`, wie im Folgenden dargestellt.

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

Amazon FSx gibt die Beschreibung der Datenrepository-Zuordnung als JSON zurück.

Lebenszyklusstatus der Datenrepository-Zuordnung

Der Lebenszyklusstatus der Datenrepository-Zuordnung enthält Statusinformationen zu einem bestimmten DRA. Eine Datenrepository-Zuordnung kann die folgenden Lebenszyklusstatus haben:

- **Erstellen** — Amazon FSx erstellt die Datenrepository-Zuordnung zwischen dem Dateisystem und dem verknüpften Daten-Repository. Das Daten-Repository ist nicht verfügbar.
- **Verfügbar** — Die Datenrepository-Verknüpfung kann verwendet werden.
- **Aktualisierung** — Die Datenrepository-Verknüpfung wird derzeit einem vom Kunden initiierten Update unterzogen, was sich auf die Verfügbarkeit auswirken kann.
- **Löschen** — Die Datenrepository-Zuordnung wird vom Kunden initiiert gelöscht.

- Falsch konfiguriert — Amazon FSx kann Updates nicht automatisch aus dem S3-Bucket importieren oder Updates automatisch in den S3-Bucket exportieren, bis die Konfiguration der Daten-Repository-Zuordnung korrigiert ist.
- Fehlgeschlagen — Die Datenrepository-Zuordnung befindet sich in einem Terminalstatus, der nicht wiederhergestellt werden kann (z. B. weil ihr Dateisystempfad gelöscht wurde oder der S3-Bucket gelöscht wurde).

Sie können den Lebenszyklusstatus einer Datenrepository-Verknüpfung mithilfe der Amazon FSx-Konsole, der AWS Command Line Interface, der und der Amazon FSx-API anzeigen. Weitere Informationen finden Sie unter [Details zur Datenrepository-Zuordnung anzeigen](#).

Arbeiten mit serverseitig verschlüsselten Amazon S3 S3-Buckets

FSx for Lustre unterstützt Amazon S3 S3-Buckets, die serverseitige Verschlüsselung mit S3-verwalteten Schlüsseln (SSE-S3) und mit gespeicherten Schlüsseln (SSE-KMS) verwenden. AWS KMS keys AWS Key Management Service

Wenn Sie möchten, dass Amazon FSx Daten beim Schreiben in Ihren S3-Bucket verschlüsselt, müssen Sie die Standardverschlüsselung in Ihrem S3-Bucket entweder auf SSE-S3 oder SSE-KMS festlegen. Weitere Informationen finden Sie unter [Konfiguration der Standardverschlüsselung](#) im Amazon S3 S3-Benutzerhandbuch. Beim Schreiben von Dateien in Ihren S3-Bucket folgt Amazon FSx der Standardverschlüsselungsrichtlinie Ihres S3-Buckets.

Standardmäßig unterstützt Amazon FSx mit SSE-S3 verschlüsselte S3-Buckets. Wenn Sie Ihr Amazon FSx-Dateisystem mit einem S3-Bucket verknüpfen möchten, der mit SSE-KMS-Verschlüsselung verschlüsselt wurde, müssen Sie Ihrer Richtlinie für vom Kunden verwaltete Schlüssel eine Erklärung hinzufügen, die es Amazon FSx ermöglicht, Objekte in Ihrem S3-Bucket mit Ihrem KMS-Schlüssel zu verschlüsseln und zu entschlüsseln.

Die folgende Anweisung ermöglicht es einem bestimmten Amazon FSx-Dateisystem, Objekte für einen bestimmten S3-Bucket, bucket_name, zu verschlüsseln und zu entschlüsseln.

```
{
  "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

Wenn Sie einen KMS mit CMK verwenden, um Ihren S3-Bucket mit aktivierten S3-Bucket-Schlüsseln EncryptionContext zu verschlüsseln, setzen Sie den auf den Bucket-ARN, nicht auf den Objekt-ARN, wie in diesem Beispiel:

```

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

```

Die folgende Richtlinienerklärung ermöglicht es allen Amazon FSx-Dateisystemen in Ihrem Konto, eine Verknüpfung mit einem bestimmten S3-Bucket herzustellen.

```

{
  "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/*"
    }
  }
}

```

Zugreifen auf serverseitig verschlüsselte Amazon S3 S3-Buckets in einem anderen AWS-Konto

Nachdem Sie ein FSx for Lustre-Dateisystem erstellt haben, das mit einem verschlüsselten Amazon S3 S3-Bucket verknüpft ist, müssen Sie der `AWSServiceRoleForFSxS3Access_fs-01234567890` Service-Linked Role (SLR) Zugriff auf den KMS-Schlüssel gewähren, mit dem der S3-Bucket verschlüsselt wurde, bevor Sie Daten aus dem verknüpften S3-Bucket lesen oder schreiben. Sie können eine IAM-Rolle verwenden, die bereits über Berechtigungen für den KMS-Schlüssel verfügt.

Note

Diese IAM-Rolle muss sich in dem Konto befinden, in dem das FSx for Lustre-Dateisystem erstellt wurde (das ist dasselbe Konto wie die S3-SLR), nicht in dem Konto, zu dem der KMS-Schlüssel/der S3-Bucket gehört.

Sie verwenden die IAM-Rolle, um die folgende AWS KMS API aufzurufen, um einen Zuschuss für die S3-Spiegelreflexkamera zu erstellen, sodass die Spiegelreflexkamera Berechtigungen für die S3-

Objekte erhält. Um den mit Ihrer SLR verknüpften ARN zu finden, durchsuchen Sie Ihre IAM-Rollen mit Ihrer Dateisystem-ID als Suchzeichenfolge.

```
$ 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"
```

Weitere Informationen zu serviceverknüpften Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#).

Änderungen aus Ihrem Daten-Repository importieren

Sie können Änderungen an Daten und POSIX-Metadaten aus einem verknüpften Daten-Repository in Ihr Amazon FSx-Dateisystem importieren. Zu den zugehörigen POSIX-Metadaten gehören Eigentum, Berechtigungen und Zeitstempel.

Verwenden Sie eine der folgenden Methoden, um Änderungen in das Dateisystem zu importieren:

- Konfigurieren Sie Ihr Dateisystem so, dass neue, geänderte oder gelöschte Dateien automatisch aus Ihrem verknüpften Datenrepository importiert werden. Weitere Informationen finden Sie unter [Automatisches Importieren von Updates aus Ihrem S3-Bucket](#).
- Wählen Sie die Option zum Importieren von Metadaten aus, wenn Sie eine Datenrepository-Zuordnung erstellen. Dadurch wird unmittelbar nach der Erstellung der Datenrepository-Zuordnung eine Aufgabe zum Importieren des Datenrepositorys gestartet.
- Verwenden Sie eine On-Demand-Aufgabe zum Importieren von Datenrepositorys. Weitere Informationen finden Sie unter [Verwenden von Datenrepository-Aufgaben zum Importieren von Änderungen](#).

Aufgaben zum automatischen Import und Import von Datenrepositorys können gleichzeitig ausgeführt werden.

Wenn Sie den automatischen Import für eine Datenrepository-Zuordnung aktivieren, aktualisiert Ihr Dateisystem automatisch Dateimetadaten, wenn Objekte in S3 erstellt, geändert oder gelöscht werden. Wenn Sie beim Erstellen einer Datenrepository-Zuordnung die Option zum Importieren von

Metadaten auswählen, importiert Ihr Dateisystem Metadaten für alle Objekte im Datenrepository. Wenn Sie mithilfe einer Aufgabe zum Importieren eines Datenrepositorys importieren, importiert Ihr Dateisystem nur Metadaten für Objekte, die seit dem letzten Import erstellt oder geändert wurden.

FSx for Lustre kopiert automatisch den Inhalt einer Datei aus Ihrem Daten-Repository und lädt ihn in das Dateisystem, wenn Ihre Anwendung zum ersten Mal auf die Datei im Dateisystem zugreift. Diese Datenbewegung wird von FSx for Lustre verwaltet und ist für Ihre Anwendungen transparent. Nachfolgende Lesevorgänge dieser Dateien werden direkt vom Dateisystem aus mit Latenzen von unter einer Millisekunde bereitgestellt.

Sie können auch Ihr gesamtes Dateisystem oder ein Verzeichnis innerhalb Ihres Dateisystems vorab laden. Weitere Informationen finden Sie unter [Vorladen von Dateien in Ihr Dateisystem](#). Wenn Sie das gleichzeitige Vorladen mehrerer Dateien anfordern, lädt FSx for Lustre Dateien parallel aus Ihrem Amazon S3 S3-Daten-Repository.

FSx for Lustre importiert nur S3-Objekte, die POSIX-konforme Objektschlüssel haben. Sowohl automatische Import- als auch Import-Daten-Repository-Aufgaben importieren POSIX-Metadaten. Weitere Informationen finden Sie unter [Unterstützung von POSIX-Metadaten für Daten-Repositorys](#).

Note

FSx for Lustre unterstützt nicht den Import von Metadaten für symbolische Links (Symlinks) aus den Speicherklassen S3 Glacier Flexible Retrieval und S3 Glacier Deep Archive. Metadaten für S3 Glacier Flexible Retrieval- oder S3 Glacier Deep Archive Archive-Objekte, die keine Symlinks sind, können importiert werden (d. h., es wird ein Inode auf dem FSx for Lustre-Dateisystem mit den richtigen Metadaten erstellt). Um diese Daten aus dem Dateisystem zu lesen, müssen Sie jedoch zuerst das Objekt S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive wiederherstellen. Der direkte Import von Dateidaten aus Amazon S3 S3-Objekten in der Speicherklasse S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive in FSx for Lustre wird nicht unterstützt.

Automatisches Importieren von Updates aus Ihrem S3-Bucket

Sie können FSx for Lustre so konfigurieren, dass Metadaten im Dateisystem automatisch aktualisiert werden, wenn Objekte zu Ihrem S3-Bucket hinzugefügt, darin geändert oder gelöscht werden. FSx for Lustre erstellt, aktualisiert oder löscht die Datei- und Verzeichnisliste entsprechend der Änderung in S3. Wenn das geänderte Objekt im S3-Bucket seine Metadaten nicht mehr enthält, behält FSx for Lustre die aktuellen Metadatenwerte der Datei bei, einschließlich der aktuellen Berechtigungen.

Note

Das FSx for Lustre-Dateisystem und der verknüpfte S3-Bucket müssen sich im selben befinden, um Updates automatisch AWS-Region zu importieren.

Sie können den automatischen Import konfigurieren, wenn Sie die Datenrepository-Zuordnung erstellen, und Sie können die Einstellungen für den automatischen Import jederzeit über die FSx-Managementkonsole AWS CLI, die oder die AWS API aktualisieren.

Note

Sie können sowohl den automatischen Import als auch den automatischen Export für dieselbe Datenrepository-Zuordnung konfigurieren. In diesem Thema wird nur die automatische Importfunktion beschrieben.

⚠ Important

- Wenn ein Objekt in S3 geändert wird, wobei alle automatischen Importrichtlinien aktiviert und der automatische Export deaktiviert sind, wird der Inhalt dieses Objekts immer in eine entsprechende Datei im Dateisystem importiert. Wenn am Zielort bereits eine Datei vorhanden ist, wird die Datei überschrieben.
- Wenn eine Datei sowohl im Dateisystem als auch in S3 geändert wird und alle automatischen Import- und Exportrichtlinien aktiviert sind, kann entweder die Datei im Dateisystem oder das Objekt in S3 durch die andere überschrieben werden. Es ist nicht garantiert, dass eine spätere Bearbeitung an einem Ort eine frühere Bearbeitung an einem anderen Ort überschreibt. Wenn Sie dieselbe Datei sowohl im Dateisystem als auch im S3-Bucket ändern, sollten Sie die Koordination auf Anwendungsebene sicherstellen, um solche Konflikte zu vermeiden. FSx for Lustre verhindert nicht widersprüchliche Schreibvorgänge an mehreren Standorten.

Die Importrichtlinie legt fest, wie FSx for Lustre Ihr Dateisystem aktualisieren soll, wenn sich der Inhalt im verknüpften S3-Bucket ändert. Eine Datenrepository-Zuordnung kann eine der folgenden Importrichtlinien haben:

- **Neu** — FSx for Lustre aktualisiert Datei- und Verzeichnismetadaten automatisch nur, wenn dem verknüpften S3-Datenrepository neue Objekte hinzugefügt werden.
- **Geändert** — FSx for Lustre aktualisiert Datei- und Verzeichnismetadaten nur dann automatisch, wenn ein vorhandenes Objekt im Datenrepository geändert wird.
- **Gelöscht** — FSx for Lustre aktualisiert Datei- und Verzeichnismetadaten nur dann automatisch, wenn ein Objekt im Datenrepository gelöscht wird.
- **Beliebige Kombination aus Neu, Geändert und Gelöscht** — FSx for Lustre aktualisiert automatisch Datei- und Verzeichnismetadaten, wenn eine der angegebenen Aktionen im S3-Datenrepository stattfindet. Sie können beispielsweise angeben, dass das Dateisystem aktualisiert wird, wenn ein Objekt zum S3-Repository hinzugefügt (Neu) oder aus dem S3-Repository entfernt (gelöscht) wird, aber nicht aktualisiert wird, wenn ein Objekt geändert wird.
- **Keine Richtlinie konfiguriert** — FSx for Lustre aktualisiert keine Datei- und Verzeichnismetadaten im Dateisystem, wenn Objekte zum S3-Daten-Repository hinzugefügt, darin geändert oder gelöscht werden. Wenn Sie keine Importrichtlinie konfigurieren, ist der automatische Import für die Datenrepository-Zuordnung deaktiviert. Sie können Metadatenänderungen immer noch manuell importieren, indem Sie eine Aufgabe zum Importieren eines Datenrepositories verwenden, wie unter [beschrieben](#) [Verwenden von Datenrepository-Aufgaben zum Importieren von Änderungen](#).

Wichtig

Beim automatischen Import werden die folgenden S3-Aktionen nicht mit Ihrem verknüpften FSx for Lustre-Dateisystem synchronisiert:

- Löschen eines Objekts mit Ablauf des S3-Objektlebenszyklus
- Dauerhaftes Löschen der aktuellen Objektversion in einem Bucket mit aktivierter Versionierung
- Das Löschen eines Objekts in einem Bucket mit aktivierter Versionierung rückgängig machen

Für die meisten Anwendungsfälle empfehlen wir, die Importrichtlinie „Neu“, „Geändert“ und „Gelöscht“ zu konfigurieren. Diese Richtlinie stellt sicher, dass alle Aktualisierungen, die in Ihrem verknüpften S3-Datenrepository vorgenommen wurden, automatisch in Ihr Dateisystem importiert werden.

Wenn Sie eine Importrichtlinie festlegen, um Ihre Dateisystemdatei und Verzeichnismetadaten auf der Grundlage von Änderungen im verknüpften S3-Datenrepository zu aktualisieren, erstellt FSx

for Lustre eine Konfiguration für Ereignisbenachrichtigungen auf dem verknüpften S3-Bucket. Die Konfiguration für die Ereignisbenachrichtigung hat einen Namen. FSx Ändern oder löschen Sie die Konfiguration der FSx Ereignisbenachrichtigung im S3-Bucket nicht. Dadurch wird der automatische Import aktualisierter Datei- und Verzeichnismetadaten in Ihr Dateisystem verhindert.

Wenn FSx for Lustre eine Dateiliste aktualisiert, die sich im verknüpften S3-Datenrepository geändert hat, überschreibt es die lokale Datei mit der aktualisierten Version, auch wenn die Datei schreibgesperrt ist.

FSx for Lustre bemüht sich nach besten Kräften, Ihr Dateisystem zu aktualisieren. FSx for Lustre kann das Dateisystem in den folgenden Situationen nicht aktualisieren:

- Wenn FSx for Lustre nicht berechtigt ist, das geänderte oder neue S3-Objekt zu öffnen. In diesem Fall überspringt FSx for Lustre das Objekt und fährt fort. Der DRA-Lebenszyklusstatus ist nicht betroffen.
- Wenn FSx for Lustre keine Berechtigungen auf Bucket-Ebene hat, wie zum Beispiel für `GetBucketAcl`. Dies führt dazu, dass der Lebenszyklusstatus des Datenrepositorys auf „Fehlkonfiguriert“ zurückgeht. Weitere Informationen finden Sie unter [Lebenszyklusstatus der Datenrepository-Zuordnung](#).
- Wenn die Konfiguration der FSx Ereignisbenachrichtigung im verknüpften S3-Bucket gelöscht oder geändert wird. Dies führt dazu, dass der Lebenszyklusstatus des Datenrepositorys falsch konfiguriert wird. Weitere Informationen finden Sie unter [Lebenszyklusstatus der Datenrepository-Zuordnung](#).

Wir empfehlen, die [Protokollierung in CloudWatch Logs zu aktivieren](#), um Informationen zu Dateien oder Verzeichnissen zu protokollieren, die nicht automatisch importiert werden konnten. Warnungen und Fehler im Protokoll enthalten Informationen zur Fehlerursache. Weitere Informationen finden Sie unter [Datenrepository-Ereignisprotokolle](#).

Voraussetzungen

Die folgenden Bedingungen sind erforderlich, damit FSx for Lustre automatisch neue, geänderte oder gelöschte Dateien aus dem verknüpften S3-Bucket importiert:

- Das Dateisystem und der verknüpfte S3-Bucket befinden sich in derselben AWS-Region.
- Der S3-Bucket hat keinen falsch konfigurierten Lifecycle-Status. Weitere Informationen finden Sie unter [Lebenszyklusstatus der Datenrepository-Zuordnung](#).

- Ihr Konto verfügt über die erforderlichen Berechtigungen, um Ereignisbenachrichtigungen für den verknüpften S3-Bucket zu konfigurieren und zu empfangen.

Unterstützte Arten von Dateiänderungen

FSx for Lustre unterstützt den Import der folgenden Änderungen an Dateien und Verzeichnissen, die im verknüpften S3-Bucket auftreten:

- Änderungen am Dateiinhalt.
- Änderungen an Datei- oder Verzeichnismetadaten.
- Änderungen am Symlink-Ziel oder an den Metadaten.
- Löschungen von Dateien und Verzeichnissen. Wenn Sie ein Objekt im verknüpften S3-Bucket löschen, das einem Verzeichnis im Dateisystem entspricht (d. h. ein Objekt mit einem Schlüsselnamen, der mit einem Schrägstrich endet), löscht FSx for Lustre das entsprechende Verzeichnis im Dateisystem nur, wenn es leer ist.

Importeinstellungen werden aktualisiert

Sie können die Importeinstellungen eines Dateisystems für einen verknüpften S3-Bucket festlegen, wenn Sie die Datenrepository-Zuordnung erstellen. Weitere Informationen finden Sie unter [Einen Link zu einem S3-Bucket erstellen](#).

Sie können auch die Importeinstellungen, einschließlich der Importrichtlinie, jederzeit aktualisieren. Weitere Informationen finden Sie unter [Einstellungen für die Datenrepository-Zuordnung werden aktualisiert](#).

Überwachung des automatischen Imports

Wenn die Änderungsrate in Ihrem S3-Bucket die Geschwindigkeit übersteigt, mit der der automatische Import diese Änderungen verarbeiten kann, werden die entsprechenden Metadatenänderungen, die in Ihr FSx for Lustre-Dateisystem importiert werden, verzögert. In diesem Fall können Sie anhand der `AgeOfOldestQueuedMessage` Metrik das Alter der ältesten Änderung überwachen, die darauf wartet, vom automatischen Import verarbeitet zu werden. Weitere Informationen zu dieser Metrik finden Sie unter [AutoImport AutoExport und Metriken](#).

Wenn die Verzögerung beim Import von Metadatenänderungen 14 Tage überschreitet (gemessen anhand der `AgeOfOldestQueuedMessage` Metrik), werden Änderungen in Ihrem S3-Bucket, die

nicht durch automatischen Import verarbeitet wurden, nicht in Ihr Dateisystem importiert. Darüber hinaus ist der Zuordnungszyklus Ihres Daten-Repositorys als FALSCH KONFIGURIERT markiert und der automatische Import wird gestoppt. Wenn Sie den automatischen Export aktiviert haben, überwacht der automatische Export weiterhin Ihr FSx for Lustre-Dateisystem auf Änderungen. Zusätzliche Änderungen werden jedoch nicht von Ihrem FSx for Lustre-Dateisystem mit S3 synchronisiert.

Um Ihre Datenrepository-Zuordnung vom Lebenszyklusstatus MISCONFIGURED in den Lebenszyklusstatus AVAILABLE zurückzusetzen, müssen Sie Ihre Datenrepository-Zuordnung aktualisieren. Sie können Ihre Datenrepository-Zuordnung mit dem CLI-Befehl [update-data-repository-association](#) (oder der entsprechenden API-Operation) aktualisieren. [UpdateDataRepositoryAssociation](#) Der einzige Anforderungsparameter, den Sie benötigen, ist der der AssociationID Datenrepository-Zuordnung, die Sie aktualisieren möchten.

Nachdem der Lebenszyklusstatus der Datenrepository-Zuordnung auf VERFÜGBAR geändert wurde, wird der automatische Import (und der automatische Export, falls aktiviert) neu gestartet. Nach dem Neustart setzt der automatische Export die Synchronisierung der Dateisystemänderungen mit S3 fort. Um die Metadaten neuer und geänderter Objekte in S3 mit Ihrem FSx for Lustre-Dateisystem zu synchronisieren, die nicht importiert wurden oder aus einer Zeit stammen, in der sich die Datenrepository-Zuordnung in einem falsch konfigurierten Zustand befand, führen Sie eine Aufgabe zum [Importieren eines Datenrepositorys](#) aus. Beim Importieren von Datenrepository-Aufgaben werden Löschungen in Ihrem S3-Bucket nicht mit Ihrem FSx for Lustre-Dateisystem synchronisiert. Wenn Sie S3 vollständig mit Ihrem Dateisystem synchronisieren möchten (einschließlich Löschungen), müssen Sie Ihr Dateisystem neu erstellen.

Um sicherzustellen, dass Verzögerungen beim Import von Metadatenänderungen 14 Tage nicht überschreiten, empfehlen wir Ihnen, einen Alarm für die `AgeOfOldestQueuedMessage` Metrik einzurichten und die Aktivität in Ihrem S3-Bucket zu reduzieren, falls die `AgeOfOldestQueuedMessage` Metrik Ihren Alarmschwellenwert überschreitet. Für ein FSx for Lustre-Dateisystem, das mit einem S3-Bucket verbunden ist, wobei ein einziger Shard kontinuierlich die maximale Anzahl möglicher Änderungen von S3 sendet, wobei nur der automatische Import auf dem FSx for Lustre-Dateisystem ausgeführt wird, kann der automatische Import einen 7-stündigen Backlog von S3-Änderungen innerhalb von 14 Tagen verarbeiten.

Darüber hinaus können Sie mit einer einzigen S3-Aktion mehr Änderungen generieren, als der automatische Import jemals in 14 Tagen verarbeiten würde. Beispiele für diese Arten von Aktionen sind unter anderem AWS Snowball Uploads auf S3 und umfangreiche Löschungen. Wenn Sie eine umfangreiche Änderung an Ihrem S3-Bucket vornehmen, die Sie mit Ihrem FSx for Lustre-

Dateisystem synchronisieren möchten, sollten Sie Ihr Dateisystem löschen und neu erstellen, sobald die S3-Änderung abgeschlossen ist, um zu verhindern, dass automatische Importänderungen länger als 14 Tage dauern.

Wenn Ihre `AgeOfOldestQueuedMessage` Kennzahl wächst, überprüfen Sie Ihren `S3-BucketGetRequests`, `PutRequests` `PostRequests`, und die `DeleteRequests` Metriken auf Aktivitätsänderungen, die zu einer Erhöhung der Geschwindigkeit und/oder Anzahl der Änderungen führen würden, die an den automatischen Import gesendet werden. Informationen zu verfügbaren S3-Metriken finden Sie unter [Monitoring Amazon S3](#) im Amazon S3 S3-Benutzerhandbuch.

Eine Liste aller verfügbaren FSx for Lustre-Metriken finden Sie unter [Überwachung mit Amazon CloudWatch](#)

Verwenden von Datenrepository-Aufgaben zum Importieren von Änderungen

Die Aufgabe zum Importieren von Datenrepositorien importiert Metadaten von Objekten, die in Ihrem S3-Datenrepository neu sind oder geändert wurden, und erstellt so eine neue Datei- oder Verzeichnisliste für jedes neue Objekt im S3-Datenrepository. Für jedes Objekt, das im Datenrepository geändert wurde, wird die entsprechende Datei- oder Verzeichnisliste mit den neuen Metadaten aktualisiert. Für Objekte, die aus dem Datenspeicher gelöscht wurden, werden keine Maßnahmen ergriffen.

Gehen Sie wie folgt vor, um Metadatenänderungen mithilfe der Amazon FSx-Konsole und CLI zu importieren. Beachten Sie, dass Sie eine Datenrepository-Aufgabe für mehrere DRAs verwenden können.

Um Metadatenänderungen zu importieren (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Navigationsbereich Dateisysteme und anschließend Ihr Lustre-Dateisystem aus.
3. Wählen Sie die Registerkarte Daten-Repository.
4. Wählen Sie im Bereich Datenrepository-Verknüpfungen die Datenrepository-Verknüpfungen aus, für die Sie die Importaufgabe erstellen möchten.
5. Wählen Sie im Menü Aktionen die Option Aufgabe importieren aus. Diese Option ist nicht verfügbar, wenn das Dateisystem nicht mit einem Datenrepository verknüpft ist. Die Aufgabenseite Import-Daten-Repository erstellen wird angezeigt.

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

- (Optional) Geben Sie bis zu 32 Verzeichnisse oder Dateien an, die aus Ihren verknüpften S3-Buckets importiert werden sollen, indem Sie die Pfade zu diesen Verzeichnissen oder Dateien unter Zu importierende Datenrepository-Pfade angeben.

 Note

Wenn ein von Ihnen angegebener Pfad nicht gültig ist, schlägt die Aufgabe fehl.

- (Optional) Wählen Sie unter Abschlussbericht die Option Aktivieren aus, um nach Abschluss der Aufgabe einen Bericht über den Abschluss der Aufgabe zu erstellen. Ein Bericht über den Abschluss der Aufgabe enthält Details zu den Dateien, die von der Aufgabe verarbeitet wurden und die dem unter Berichtsbereich angegebenen Umfang entsprechen. Um den Ort anzugeben, an dem Amazon FSx den Bericht liefern soll, geben Sie einen relativen Pfad in einem verknüpften S3-Datenrepository als Berichtspfad ein.
- Wählen Sie Erstellen.

Eine Benachrichtigung oben auf der Seite Dateisysteme zeigt, dass die Aufgabe, die Sie gerade erstellt haben, in Bearbeitung ist.

Um den Status und die Details der Aufgabe einzusehen, scrollen Sie auf der Registerkarte Daten-Repository für das Dateisystem nach unten zum Bereich Daten-Repository-Aufgaben. In der Standardsortierreihenfolge wird die neueste Aufgabe ganz oben in der Liste angezeigt.

Um auf dieser Seite eine Aufgabenzusammenfassung anzuzeigen, wählen Sie die Task-ID für die Aufgabe, die Sie gerade erstellt haben. Die Übersichtsseite für die Aufgabe wird angezeigt.

So importieren Sie Metadatenänderungen (CLI)

- Verwenden Sie den [create-data-repository-task](#) CLI-Befehl, um Metadatenänderungen in Ihr FSx for Lustre-Dateisystem zu importieren. Die entsprechende API-Operation ist [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
```

Nach erfolgreicher Erstellung der Datenrepository-Aufgabe gibt Amazon FSx die Aufgabenbeschreibung als JSON zurück.

Nachdem Sie die Aufgabe zum Importieren von Metadaten aus dem verknüpften Daten-Repository erstellt haben, können Sie den Status der Aufgabe zum Importieren des Daten-Repositorys überprüfen. Weitere Informationen zum Anzeigen von Datenrepository-Aufgaben finden Sie unter [Zugreifen auf Datenrepository-Aufgaben](#).

Vorladen von Dateien in Ihr Dateisystem

Amazon FSx kopiert Daten aus Ihrem Amazon S3 S3-Daten-Repository, wenn auf eine Datei zum ersten Mal zugegriffen wird. Aufgrund dieses Ansatzes kommt es beim ersten Lesen oder Schreiben in eine Datei zu einer geringen Latenz. Wenn Ihre Anwendung empfindlich auf diese Latenz reagiert und Sie wissen, auf welche Dateien oder Verzeichnisse Ihre Anwendung zugreifen muss, können

Sie optional Inhalte einzelner Dateien oder Verzeichnisse vorab laden. Dazu verwenden Sie den `hsm_restore` folgenden Befehl.

Sie können den `hsm_action` Befehl (der mit dem `lfs` Benutzerprogramm ausgegeben wird) verwenden, um zu überprüfen, ob der Inhalt der Datei vollständig in das Dateisystem geladen wurde. Der Rückgabewert von `N00P` gibt an, dass die Datei erfolgreich geladen wurde. Führen Sie die folgenden Befehle von einer Recheninstanz aus, auf der das Dateisystem eingehängt ist. Ersetzen Sie *path/to/file* durch den Pfad der Datei, die Sie vorab in Ihr Dateisystem laden.

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

Mit den folgenden Befehlen können Sie Ihr gesamtes Dateisystem oder ein ganzes Verzeichnis innerhalb Ihres Dateisystems vorab laden. (Das nachstehende Und-Zeichen sorgt dafür, dass ein Befehl als Hintergrundprozess ausgeführt wird.) Wenn Sie das gleichzeitige Vorladen mehrerer Dateien anfordern, lädt Amazon FSx Ihre Dateien parallel aus Ihrem Amazon S3 S3-Daten-Repository. Wenn eine Datei bereits in das Dateisystem geladen wurde, lädt der `hsm_restore` Befehl sie nicht erneut.

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

Note

Wenn Ihr verknüpfter S3-Bucket größer als Ihr Dateisystem ist, sollten Sie in der Lage sein, alle Dateimetadaten in Ihr Dateisystem zu importieren. Sie können jedoch nur so viele tatsächliche Dateidaten laden, wie in den verbleibenden Speicherplatz des Dateisystems passen. Sie erhalten eine Fehlermeldung, wenn Sie versuchen, auf Dateidaten zuzugreifen, obwohl im Dateisystem kein Speicherplatz mehr vorhanden ist. In diesem Fall können Sie die Speicherkapazität nach Bedarf erhöhen. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#).


Änderungen in das Daten-Repository exportieren

Sie können Änderungen an Daten und POSIX-Metadatenänderungen aus Ihrem FSx for Lustre-Dateisystem in ein verknüpftes Daten-Repository exportieren. Zu den zugehörigen POSIX-Metadaten gehören Besitz, Berechtigungen und Zeitstempel.

Verwenden Sie eine der folgenden Methoden, um Änderungen aus dem Dateisystem zu exportieren.

- Konfigurieren Sie Ihr Dateisystem so, dass neue, geänderte oder gelöschte Dateien automatisch in Ihr verknüpft Datenrepository exportiert werden. Weitere Informationen finden Sie unter [Exportieren Sie Updates automatisch in Ihren S3-Bucket](#).
- Verwenden Sie eine On-Demand-Aufgabe zum Exportieren von Datenrepositorys. Weitere Informationen finden Sie unter [Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen](#).

Aufgaben zum automatischen Exportieren und Exportieren von Datenrepositorys können nicht gleichzeitig ausgeführt werden.


 **Important**

Beim automatischen Export werden die folgenden Metadatenoperationen auf Ihrem Dateisystem nicht mit S3 synchronisiert, wenn die entsprechenden Objekte in S3 Glacier Flexible Retrieval gespeichert sind:

- chmod
- Chown
- umbenennen

Wenn Sie den automatischen Export für eine Datenrepository-Verknüpfung aktivieren, exportiert Ihr Dateisystem automatisch Dateidaten und Metadatenänderungen, wenn Dateien erstellt, geändert oder gelöscht werden. Wenn Sie Dateien oder Verzeichnisse mithilfe einer Aufgabe zum Exportieren eines Datenrepositorys exportieren, exportiert Ihr Dateisystem nur Datendateien und Metadaten, die seit dem letzten Export erstellt oder geändert wurden.

Sowohl beim automatischen Export als auch beim Exportieren von Datenrepositorys werden POSIX-Metadaten exportiert. Weitere Informationen finden Sie unter [Unterstützung von POSIX-Metadaten für Daten-Repositorys](#).

 **Important**

- Um sicherzustellen, dass FSx for Lustre Ihre Daten in Ihren S3-Bucket exportieren kann, müssen sie in einem UTF-8-kompatiblen Format gespeichert werden.

- S3-Objektschlüssel haben eine maximale Länge von 1.024 Byte. FSx for Lustre exportiert keine Dateien, deren entsprechender S3-Objektschlüssel länger als 1.024 Byte wäre.

Note

Alle Objekte, die durch automatische Export- und Export-Datenrepository-Aufgaben erstellt wurden, werden mit der Speicherklasse S3 Standard geschrieben.

Themen

- [Exportieren Sie Updates automatisch in Ihren S3-Bucket](#)
- [Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen](#)
- [Exportieren von Dateien mithilfe von HSM-Befehlen](#)

Exportieren Sie Updates automatisch in Ihren S3-Bucket

Sie können Ihr FSx for Lustre-Dateisystem so konfigurieren, dass der Inhalt eines verknüpften S3-Buckets automatisch aktualisiert wird, wenn Dateien im Dateisystem hinzugefügt, geändert oder gelöscht werden. FSx for Lustre erstellt, aktualisiert oder löscht das Objekt in S3 entsprechend der Änderung im Dateisystem.

Note

Automatischer Export ist auf FSx for Lustre 2.10-Dateisystemen oder Scratch 1 Dateisystemen nicht verfügbar.

Sie können in ein Daten-Repository exportieren, das sich im selben AWS-Region Dateisystem oder in einem anderen befindet. AWS-Region

Sie können den automatischen Export konfigurieren, wenn Sie die Datenrepository-Zuordnung erstellen, und die automatischen Exporteinstellungen jederzeit mithilfe der FSx-Managementkonsole AWS CLI, der und der AWS API aktualisieren.

Note

Sie können sowohl den automatischen Export als auch den automatischen Import für dieselbe Datenrepository-Zuordnung konfigurieren. In diesem Thema wird nur die automatische Exportfunktion beschrieben.

⚠ Important

- Wenn eine Datei im Dateisystem geändert wird, wobei alle automatischen Exportrichtlinien aktiviert und der automatische Import deaktiviert ist, wird der Inhalt dieser Datei immer in ein entsprechendes Objekt in S3 exportiert. Wenn am Zielort bereits ein Objekt vorhanden ist, wird das Objekt überschrieben.
- Wenn eine Datei sowohl im Dateisystem als auch in S3 geändert wird und alle automatischen Import- und Exportrichtlinien aktiviert sind, kann entweder die Datei im Dateisystem oder das Objekt in S3 durch die andere überschrieben werden. Es ist nicht garantiert, dass eine spätere Bearbeitung an einem Ort eine frühere Bearbeitung an einem anderen Ort überschreibt. Wenn Sie dieselbe Datei sowohl im Dateisystem als auch im S3-Bucket ändern, sollten Sie die Koordination auf Anwendungsebene sicherstellen, um solche Konflikte zu vermeiden. FSx for Lustre verhindert nicht widersprüchliche Schreibvorgänge an mehreren Standorten.

Die Exportrichtlinie legt fest, wie FSx for Lustre Ihren verknüpften S3-Bucket aktualisieren soll, wenn sich der Inhalt im Dateisystem ändert. Eine Datenrepository-Zuordnung kann eine der folgenden automatischen Exportrichtlinien haben:

- Neu — FSx for Lustre aktualisiert das S3-Daten-Repository nur dann automatisch, wenn eine neue Datei, ein neues Verzeichnis oder ein neuer Symlink im Dateisystem erstellt wird.
- Geändert — FSx for Lustre aktualisiert das S3-Daten-Repository nur dann automatisch, wenn eine bestehende Datei im Dateisystem geändert wird. Bei Änderungen des Dateiinhalts muss die Datei geschlossen werden, bevor sie in das S3-Repository übertragen wird. Metadatenänderungen (Umbenennung, Besitz, Berechtigungen und Zeitstempel) werden weitergegeben, wenn der Vorgang abgeschlossen ist. Beim Umbenennen von Änderungen (einschließlich Verschiebungen) wird das bestehende (zuvor umbenannte) S3-Objekt gelöscht und ein neues S3-Objekt mit dem neuen Namen erstellt.

- **Gelöscht** — FSx for Lustre aktualisiert das S3-Daten-Repository nur dann automatisch, wenn eine Datei, ein Verzeichnis oder ein Symlink im Dateisystem gelöscht wird.
- **Beliebige Kombination aus Neu, Geändert und Gelöscht** — FSx for Lustre aktualisiert das S3-Daten-Repository automatisch, wenn eine der angegebenen Aktionen im Dateisystem auftritt. Sie können beispielsweise angeben, dass das S3-Repository aktualisiert wird, wenn eine Datei zum Dateisystem hinzugefügt (Neu) oder aus dem Dateisystem entfernt (gelöscht) wird, aber nicht, wenn eine Datei geändert wird.
- **Keine Richtlinie konfiguriert** — FSx for Lustre aktualisiert das S3-Daten-Repository nicht automatisch, wenn Dateien zum Dateisystem hinzugefügt, geändert oder aus dem Dateisystem gelöscht werden. Wenn Sie keine Exportrichtlinie konfigurieren, ist der automatische Export deaktiviert. Sie können Änderungen immer noch manuell exportieren, indem Sie eine Aufgabe zum Exportieren eines Datenrepositorys verwenden, wie unter [beschrieben](#) [Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen](#).

Für die meisten Anwendungsfälle empfehlen wir, die Exportrichtlinie „Neu“, „Geändert“ und „Gelöscht“ zu konfigurieren. Diese Richtlinie stellt sicher, dass alle an Ihrem Dateisystem vorgenommenen Aktualisierungen automatisch in Ihr verknüpftes S3-Datenrepository exportiert werden.

Wir empfehlen, die [Protokollierung in CloudWatch Logs zu aktivieren](#), um Informationen zu Dateien oder Verzeichnissen zu protokollieren, die nicht automatisch exportiert werden konnten. Warnungen und Fehler im Protokoll enthalten Informationen zur Fehlerursache. Weitere Informationen finden Sie unter [Datenrepository-Ereignisprotokolle](#).

Die Exporteinstellungen werden aktualisiert

Sie können die Exporteinstellungen eines Dateisystems auf einen verknüpften S3-Bucket festlegen, wenn Sie die Datenrepository-Zuordnung erstellen. Weitere Informationen finden Sie unter [Einen Link zu einem S3-Bucket erstellen](#).

Sie können auch die Exporteinstellungen, einschließlich der Exportrichtlinie, jederzeit aktualisieren. Weitere Informationen finden Sie unter [Einstellungen für die Datenrepository-Zuordnung werden aktualisiert](#).

Überwachung des automatischen Exports

Sie können die Verknüpfungen von Datenrepositorys mit automatischem Export anhand einer Reihe von auf Amazon veröffentlichten Metriken überwachen CloudWatch. Die `AgeOfOldestQueuedMessage` Metrik gibt das Alter der ältesten Aktualisierung des Dateisystems

an, die noch nicht nach S3 exportiert wurde. Wenn der über einen längeren Zeitraum größer als `Null AgeOf01destQueuedMessage` ist, empfehlen wir, die Anzahl der Änderungen (insbesondere Verzeichnisumbenennungen), die aktiv am Dateisystem vorgenommen werden, vorübergehend zu reduzieren, bis die Nachrichtenwarteschlange reduziert wurde. Weitere Informationen finden Sie unter [AutoImport AutoExport und Metriken](#).

Important

Wenn Sie eine Datenrepository-Zuordnung oder ein Dateisystem mit aktiviertem automatischen Export löschen, sollten Sie zunächst sicherstellen, dass der Wert `Null AgeOf01destQueuedMessage` ist, d. h., dass es keine Änderungen gibt, die noch nicht exportiert wurden. Wenn der Wert größer als `Null AgeOf01destQueuedMessage` ist, wenn Sie Ihre Datenrepository-Zuordnung oder Ihr Dateisystem löschen, werden die Änderungen, die noch nicht exportiert wurden, Ihren verknüpften S3-Bucket nicht erreichen. Um dies zu vermeiden, warten `AgeOf01destQueuedMessage` Sie, bis Null erreicht ist, bevor Sie Ihre Datenrepository-Zuordnung oder Ihr Dateisystem löschen.

Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen

Die Aufgabe zum Exportieren von Datenrepositorien exportiert Dateien, die in Ihrem Dateisystem neu sind oder geändert wurden. Sie erstellt ein neues Objekt in S3 für jede neue Datei im Dateisystem. Für jede Datei, die im Dateisystem geändert wurde oder deren Metadaten geändert wurden, wird das entsprechende Objekt in S3 durch ein neues Objekt mit den neuen Daten und Metadaten ersetzt. Für Dateien, die aus dem Dateisystem gelöscht wurden, werden keine Maßnahmen ergriffen.

Note

Beachten Sie bei der Verwendung von Aufgaben zum Exportieren von Datenrepositorys Folgendes:

- Die Verwendung von Platzhaltern zum Ein- oder Ausschließen von Dateien für den Export wird nicht unterstützt.
- Bei der Ausführung von `mv` Vorgängen wird die Zielfeile nach dem Verschieben nach S3 exportiert, auch wenn keine UID, GID, Berechtigung oder Inhaltsänderung vorgenommen wurde.

Verwenden Sie die folgenden Verfahren, um Daten und Metadatenänderungen im Dateisystem mithilfe der Amazon FSx-Konsole und CLI in verknüpfte S3-Buckets zu exportieren. Beachten Sie, dass Sie eine Datenrepository-Aufgabe für mehrere DRAs verwenden können.

Um Änderungen zu exportieren (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Navigationsbereich Dateisysteme und anschließend Ihr Lustre-Dateisystem aus.
3. Wählen Sie die Registerkarte Daten-Repository.
4. Wählen Sie im Bereich Datenrepository-Verknüpfungen die Datenrepository-Zuordnung aus, für die Sie die Exportaufgabe erstellen möchten.
5. Wählen Sie für Aktionen die Option Aufgabe exportieren aus. Diese Option ist nicht verfügbar, wenn das Dateisystem nicht mit einem Daten-Repository auf S3 verknüpft ist. Das Aufgabendialogfeld Exportdaten-Repository erstellen wird angezeigt.

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

- (Optional) Geben Sie bis zu 32 Verzeichnisse oder Dateien an, die aus Ihrem Amazon FSx-Dateisystem exportiert werden sollen, indem Sie die Pfade zu diesen Verzeichnissen oder Dateien unter Zu exportierende Dateisystempfade angeben. Die Pfade, die Sie angeben, müssen sich auf den Bereitstellungspunkt des Dateisystems beziehen. Wenn der Einhängpunkt ein Verzeichnis oder eine Datei auf dem Dateisystem `/mnt/fsx/path1` ist `/mnt/fsx` und ist, das Sie exportieren möchten, dann ist der Pfad, den Sie angeben möchten `path1`.

 Note

Wenn ein von Ihnen angegebener Pfad nicht gültig ist, schlägt die Aufgabe fehl.

- (Optional) Wählen Sie unter Abschlussbericht die Option Aktivieren aus, um nach Abschluss der Aufgabe einen Bericht über den Abschluss der Aufgabe zu erstellen. Ein Bericht über den Abschluss der Aufgabe enthält Details zu den Dateien, die von der Aufgabe verarbeitet wurden und die dem unter Berichtsbereich angegebenen Umfang entsprechen. Um den Speicherort anzugeben, an den Amazon FSx den Bericht liefern soll, geben Sie als Berichtspfad einen relativen Pfad im verknüpften S3-Daten-Repository des Dateisystems ein.
- Wählen Sie Erstellen.

Eine Benachrichtigung oben auf der Seite Dateisysteme zeigt, dass die Aufgabe, die Sie gerade erstellt haben, noch in Bearbeitung ist.

Um den Status und die Details der Aufgabe einzusehen, scrollen Sie auf der Registerkarte Daten-Repository für das Dateisystem nach unten zum Bereich Daten-Repository-Aufgaben. In der Standardsortierreihenfolge wird die neueste Aufgabe ganz oben in der Liste angezeigt.

Um auf dieser Seite eine Aufgabenzusammenfassung anzuzeigen, wählen Sie die Task-ID für die Aufgabe, die Sie gerade erstellt haben. Die Übersichtsseite für die Aufgabe wird angezeigt.

Um Änderungen zu exportieren (CLI)

- Verwenden Sie den [create-data-repository-task](#) CLI-Befehl, um Daten und Metadatenänderungen auf Ihrem FSx for Lustre-Dateisystem zu exportieren. Die entsprechende API-Operation ist. [CreateDataRepositoryTask](#)

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

```
--report Enabled=true
```

Nach erfolgreicher Erstellung der Datenrepository-Aufgabe gibt Amazon FSx die Aufgabenbeschreibung als JSON zurück, wie im folgenden Beispiel gezeigt.

```
{
  "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"
  }
}
```

Nachdem Sie die Aufgabe zum Exportieren von Daten in das verknüpfte Daten-Repository erstellt haben, können Sie den Status der Aufgabe zum Exportieren des Daten-Repositorys überprüfen. Weitere Informationen zum Anzeigen von Datenrepository-Aufgaben finden Sie unter [Zugreifen auf Datenrepository-Aufgaben](#).

Exportieren von Dateien mithilfe von HSM-Befehlen

Note

Um Änderungen an den Daten und Metadaten Ihres FSx for Lustre-Dateisystems in ein dauerhaftes Daten-Repository auf Amazon S3 zu exportieren, verwenden Sie die unter beschriebene automatische Exportfunktion. [Exportieren Sie Updates automatisch in Ihren S3-Bucket](#) Sie können auch Aufgaben zum Exportieren von Datenrepositorys verwenden,

die unter beschrieben sind. [Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen](#)

Um eine einzelne Datei in Ihr Daten-Repository zu exportieren und zu überprüfen, ob die Datei erfolgreich in Ihr Daten-Repository exportiert wurde, können Sie die folgenden Befehle ausführen. Ein Rückgabewert von `states: (0x00000009) exists archived` gibt an, dass die Datei erfolgreich exportiert wurde.

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

Note

Sie müssen die HSM-Befehle (z. B. `hsm_archive`) als Root-Benutzer oder mithilfe von `sudo` ausführen.

Führen Sie die folgenden Befehle aus, um Ihr gesamtes Dateisystem oder ein ganzes Verzeichnis in Ihrem Dateisystem zu exportieren. Wenn Sie mehrere Dateien gleichzeitig exportieren, exportiert Amazon FSx for Lustre Ihre Dateien parallel in Ihr Amazon S3 S3-Daten-Repository.

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

Führen Sie den folgenden Befehl aus, um festzustellen, ob der Export abgeschlossen wurde.

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

Wenn der Befehl zurückkehrt und keine Dateien mehr übrig sind, ist der Export abgeschlossen.

Datenrepository-Aufgaben

Mithilfe von Aufgaben zum Importieren und Exportieren von Datenrepositorys können Sie die Übertragung von Daten und Metadaten zwischen Ihrem FSx for Lustre-Dateisystem und seinen dauerhaften Datenrepositorys auf Amazon S3 verwalten.

Datenrepository-Aufgaben optimieren Daten- und Metadatentransfers zwischen Ihrem FSx for Lustre-Dateisystem und einem Daten-Repository auf S3. Eine Möglichkeit, dies zu tun, besteht darin, Änderungen zwischen Ihrem Amazon FSx-Dateisystem und dem zugehörigen verknüpften Daten-Repository zu verfolgen. Sie tun dies auch, indem sie parallel Übertragungstechniken verwenden, um Daten mit Geschwindigkeiten von bis zu Hunderten von Gbit/s zu übertragen. Sie erstellen und zeigen Datenrepository-Aufgaben mit der Amazon FSx-Konsole AWS CLI, der und der Amazon FSx-API an.

Datenrepository-Aufgaben verwalten die POSIX-Metadaten (Portable Operating System Interface) des Dateisystems, einschließlich Eigentum, Berechtigungen und Zeitstempel. Da die Aufgaben diese Metadaten verwalten, können Sie Zugriffskontrollen zwischen Ihrem FSx for Lustre-Dateisystem und seinen verknüpften Datenrepositorys implementieren und verwalten.

Sie können eine Aufgabe zum Freigeben von Datenrepositorys verwenden, um Speicherplatz im Dateisystem für neue Dateien freizugeben, indem Sie nach Amazon S3 exportierte Dateien freigeben. Der Inhalt der veröffentlichten Datei wird entfernt, aber die Metadaten der veröffentlichten Datei verbleiben im Dateisystem. Benutzer und Anwendungen können weiterhin auf eine veröffentlichte Datei zugreifen, indem sie die Datei erneut lesen. Wenn der Benutzer oder die Anwendung die veröffentlichte Datei liest, ruft FSx for Lustre den Dateiinhalt transparent von Amazon S3 ab.

Arten von Datenrepository-Aufgaben

Es gibt drei Arten von Datenrepository-Aufgaben:

- Exportieren Sie Datenrepository-Aufgaben: Export aus Ihrem Lustre-Dateisystem in einen verknüpften S3-Bucket.
- Datenrepository-Aufgaben importieren Import aus einem verknüpften S3-Bucket in Ihr Lustre-Dateisystem.
- Aufgaben im Daten-Repository veröffentlichen Dateien, die aus Ihrem Lustre-Dateisystem in einen verknüpften S3-Bucket exportiert wurden.

Weitere Informationen finden Sie unter [Eine Datenrepository-Aufgabe erstellen](#).

Themen

- [Den Status und die Details einer Aufgabe verstehen](#)
- [Verwenden von Datenrepository-Aufgaben](#)
- [Arbeiten mit Berichten über den Abschluss von Aufgaben](#)

- [Behebung von Fehlern bei Datenrepository-Aufgaben](#)

Den Status und die Details einer Aufgabe verstehen

Eine Datenrepository-Aufgabe kann einen der folgenden Status haben:

- PENDING gibt an, dass Amazon FSx die Aufgabe nicht gestartet hat.
- EXECUTING gibt an, dass Amazon FSx die Aufgabe verarbeitet.
- FAILED bedeutet, dass Amazon FSx die Aufgabe nicht erfolgreich verarbeitet hat. Beispielsweise kann es Dateien geben, die die Aufgabe nicht verarbeiten konnte. Die Aufgabedetails enthalten weitere Informationen über den Fehler. Weitere Informationen zu fehlgeschlagenen Aufgaben finden Sie unter [Behebung von Fehlern bei Datenrepository-Aufgaben](#).
- SUCCEED gibt an, dass Amazon FSx die Aufgabe erfolgreich abgeschlossen hat.
- CANCELED gibt an, dass die Aufgabe storniert und nicht abgeschlossen wurde.
- CANCELING bedeutet, dass Amazon FSx gerade dabei ist, die Aufgabe abubrechen.

Nachdem eine Aufgabe erstellt wurde, können Sie die folgenden detaillierten Informationen für eine Datenrepository-Aufgabe mithilfe der Amazon FSx-Konsole, CLI oder API anzeigen:

- Der Aufgabentyp:
 - EXPORT_TO_REPOSITORY weist auf eine Exportaufgabe hin.
 - IMPORT_METADATA_FROM_REPOSITORY weist auf eine Importaufgabe hin.
 - RELEASE_DATA_FROM_FILESYSTEM weist auf eine Release-Aufgabe hin.
- Das Dateisystem, auf dem die Aufgabe ausgeführt wurde.
- Die Zeit, zu der die Aufgabe erstellt wurde.
- Der Status der Aufgabe.
- Die Gesamtzahl der Dateien, die von der Aufgabe verarbeitet wurden.
- Die Gesamtzahl der Dateien, die von der Aufgabe erfolgreich verarbeitet wurden.
- Die Gesamtzahl der Dateien, die die Aufgabe nicht verarbeiten konnte. Dieser Wert ist größer als Null, wenn der Aufgabenstatus FEHLGESCHLAGEN ist. Detaillierte Informationen zu Dateien, bei denen Fehler aufgetreten sind, sind in einem Bericht zum Abschluss der Aufgabe verfügbar. Weitere Informationen finden Sie unter [Arbeiten mit Berichten über den Abschluss von Aufgaben](#).
- Die Uhrzeit, zu der die Aufgabe gestartet wurde.

- Die Uhrzeit, zu der der Aufgabenstatus zuletzt aktualisiert wurde. Der Aufgabenstatus wird alle 30 Sekunden aktualisiert.

Weitere Informationen zum Zugriff auf bestehende Datenrepository-Aufgaben finden Sie unter [Zugreifen auf Datenrepository-Aufgaben](#).

Verwenden von Datenrepository-Aufgaben

Sie können Datenrepository-Aufgaben mithilfe der Amazon FSx-Konsole, CLI oder API erstellen, duplizieren, Details anzeigen und stornieren.

Themen

- [Eine Datenrepository-Aufgabe erstellen](#)
- [Eine Aufgabe duplizieren](#)
- [Zugreifen auf Datenrepository-Aufgaben](#)
- [Abbrechen einer Datenrepository-Aufgabe](#)

Eine Datenrepository-Aufgabe erstellen

Sie können eine Datenrepository-Aufgabe mithilfe der Amazon FSx-Konsole, CLI oder API erstellen. Nachdem Sie eine Aufgabe erstellt haben, können Sie den Fortschritt und den Status der Aufgabe mithilfe der Konsole, CLI oder API anzeigen.

Sie können drei Arten von Datenrepository-Aufgaben erstellen:

- Die Aufgabe Datenrepository exportieren exportiert aus Ihrem Lustre-Dateisystem in einen verknüpften S3-Bucket. Weitere Informationen finden Sie unter [Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen](#).
- Die Aufgabe Datenrepository importieren importiert aus einem verknüpften S3-Bucket in Ihr Lustre-Dateisystem. Weitere Informationen finden Sie unter [Verwenden von Datenrepository-Aufgaben zum Importieren von Änderungen](#).
- Die Aufgabe Datenrepository veröffentlichen gibt Dateien aus Ihrem Lustre-Dateisystem frei, die in einen verknüpften S3-Bucket exportiert wurden. Weitere Informationen finden Sie unter [Verwenden von Datenrepository-Aufgaben zur Freigabe von Dateien](#).

Eine Aufgabe duplizieren

Sie können eine bestehende Datenrepository-Aufgabe in der Amazon FSx-Konsole duplizieren. Wenn Sie eine Aufgabe duplizieren, wird eine exakte Kopie der vorhandenen Aufgabe auf der Aufgabenseite Import-Daten-Repository erstellen oder Daten-Repository erstellen angezeigt. Sie können die Pfade für den Export oder Import nach Bedarf ändern, bevor Sie die neue Aufgabe erstellen und ausführen.

Note

Eine Anforderung zur Ausführung einer doppelten Aufgabe schlägt fehl, wenn bereits eine exakte Kopie dieser Aufgabe ausgeführt wird. Eine exakte Kopie einer Aufgabe, die bereits ausgeführt wird, enthält denselben Dateisystempfad oder dieselben Dateisystempfade im Fall einer Exportaufgabe oder dieselben Datenrepository-Pfade im Fall einer Importaufgabe.

Sie können eine Aufgabe in der Aufgabendetailansicht, im Bereich Datenrepository-Aufgaben auf der Registerkarte Datenrepository für das Dateisystem oder auf der Seite mit den Datenrepository-Aufgaben duplizieren.

Um eine bestehende Aufgabe zu duplizieren

1. Wählen Sie im Bereich Datenrepository-Aufgaben auf der Registerkarte Daten-Repository für das Dateisystem eine Aufgabe aus.
2. Wählen Sie „Aufgabe duplizieren“. Je nachdem, welchen Aufgabentyp Sie ausgewählt haben, wird die Aufgabenseite Import-Daten-Repository erstellen oder Exportdaten-Repository erstellen angezeigt. Alle Einstellungen für die neue Aufgabe sind identisch mit denen für die Aufgabe, die Sie duplizieren.
3. Ändern Sie die Pfade, aus denen Sie importieren oder in die Sie exportieren möchten, oder fügen Sie sie hinzu.
4. Wählen Sie Erstellen.

Zugreifen auf Datenrepository-Aufgaben


Nachdem Sie eine Datenrepository-Aufgabe erstellt haben, können Sie über die Amazon FSx-Konsole, CLI und API auf die Aufgabe und alle vorhandenen Aufgaben in Ihrem Konto zugreifen. Amazon FSx bietet die folgenden detaillierten Aufgabeninformationen:


- Alle vorhandenen Aufgaben.
- Alle Aufgaben für ein bestimmtes Dateisystem.
- Alle Aufgaben für eine bestimmte Datenrepository-Zuordnung.
- Alle Aufgaben mit einem bestimmten Lebenszyklusstatus. Weitere Informationen zu Statuswerten für den Aufgabenlebenszyklus finden Sie unter [Den Status und die Details einer Aufgabe verstehen](#).

Sie können auf alle vorhandenen Datenrepository-Aufgaben in Ihrem Konto zugreifen, indem Sie die Amazon FSx-Konsole, CLI oder API verwenden, wie im Folgenden beschrieben.

Um Datenrepository-Aufgaben und Aufgabendetails anzuzeigen (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Navigationsbereich die Option Datenrepository-Aufgaben (Lustre) aus. Die Seite mit den Datenrepository-Aufgaben wird angezeigt, auf der die vorhandenen Aufgaben angezeigt werden.
3. Um die Details einer Aufgabe zu sehen, wählen Sie auf der Seite mit den Datenrepository-Aufgaben die Aufgaben-ID oder den Aufgabennamen aus. Die Seite mit den Aufgabendetails wird angezeigt.

Task status Info		
 Canceled	Total number of files to export Info 0	Task start time Info 2019-12-17T17:21:15-05:00
	Files successfully exported Info 0	Task end time Info 2019-12-17T17:22:13-05:00
	Files failed to export Info 0	Task last updated time Info 2019-12-17T17:21:36-05:00

Completion report		
 Enabled	Report format REPORT_CSV_20191124	Report path s3://completion-report-test/FSxLustre20191217T214233Z/.aws-fsx-data-repository-tasks
	Report scope FAILED_FILES_ONLY	

So rufen Sie Datenrepository-Aufgaben und Aufgabendetails ab (CLI)

Mit dem Amazon FSx [describe-data-repository-tasks](#) CLI-Befehl können Sie alle Datenrepository-Aufgaben und deren Details in Ihrem Konto anzeigen.

[DescribeDataRepositoryTasks](#) ist der entsprechende API-Befehl.

- Verwenden Sie den folgenden Befehl, um alle Datenrepository-Aufgabenobjekte in Ihrem Konto anzuzeigen.

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

Wenn der Befehl erfolgreich ist, gibt Amazon FSx die Antwort im JSON-Format zurück.

```
{
  "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"
  }
}

```

```
    }  
  ]  
}
```

Aufgaben nach Dateisystem anzeigen

Sie können alle Aufgaben für ein bestimmtes Dateisystem mithilfe der Amazon FSx-Konsole, CLI oder API anzeigen, wie im Folgenden beschrieben.

Um Aufgaben nach Dateisystem (Konsole) aufgeschlüsselt anzuzeigen

1. Wählen Sie im Navigationsbereich Dateisysteme aus. Die Seite Dateisysteme wird angezeigt.
2. Wählen Sie das Dateisystem aus, für das Sie Datenrepository-Aufgaben anzeigen möchten. Die Seite mit den Dateisystemdetails wird angezeigt.
3. Wählen Sie auf der Seite mit den Dateisystemdetails die Registerkarte Datenrepository aus. Alle Aufgaben für dieses Dateisystem werden im Bereich Datenrepository-Aufgaben angezeigt.

Um Aufgaben per Dateisystem (CLI) abzurufen

- Verwenden Sie den folgenden Befehl, um alle Datenrepository-Aufgaben für das Dateisystem anzuzeigen `fs-0123456789abcdef0`.

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

Wenn der Befehl erfolgreich ist, gibt Amazon FSx die Antwort im JSON-Format zurück.

```
{  
  "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,
      "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"
  }
]
}
```

Abbrechen einer Datenrepository-Aufgabe

Sie können eine Datenrepository-Aufgabe abbrechen, während sie sich entweder im Status AUSSTEHEND oder IN AUSFÜHRUNG befindet. Wenn Sie eine Aufgabe stornieren, passiert Folgendes:

- Amazon FSx verarbeitet keine Dateien, die sich in der zu verarbeitenden Warteschlange befinden.
- Amazon FSx setzt die Verarbeitung aller Dateien fort, die sich derzeit in Bearbeitung befinden.
- Amazon FSx setzt keine Dateien zurück, die die Aufgabe bereits verarbeitet hat.

Um eine Datenrepository-Aufgabe abzuberechnen (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Klicken Sie auf das Dateisystem, für das Sie eine Datenrepository-Aufgabe abbrechen möchten.
3. Öffnen Sie die Registerkarte Datenrepository und scrollen Sie nach unten, um den Bereich Datenrepository-Aufgaben aufzurufen.
4. Wählen Sie die Aufgaben-ID oder den Aufgabennamen für die Aufgabe, die Sie stornieren möchten.
5. Wählen Sie Aufgabe abbrechen, um die Aufgabe abzuberechnen.
6. Geben Sie die Aufgaben-ID ein, um die Stornierungsanfrage zu bestätigen.

Um eine Datenrepository-Aufgabe abzuberechnen (CLI)

Verwenden Sie den Amazon FSx [cancel-data-repository-task](#) CLI-Befehl, um eine Aufgabe abzuberechnen. [CancelDataRepositoryTask](#) ist der entsprechende API-Befehl.

- Verwenden Sie den folgenden Befehl, um eine Datenrepository-Aufgabe abzuberechnen.

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

Wenn der Befehl erfolgreich ist, gibt Amazon FSx die Antwort im JSON-Format zurück.

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

}

Arbeiten mit Berichten über den Abschluss von Aufgaben

Ein Bericht über den Abschluss einer Aufgabe enthält Einzelheiten zu den Ergebnissen einer Aufgabe zum Exportieren, Importieren oder Freigeben eines Datenrepositorys. Der Bericht enthält Ergebnisse für die von der Aufgabe verarbeiteten Dateien, die dem Umfang des Berichts entsprechen. Mithilfe des `Enabled` Parameters können Sie angeben, ob ein Bericht für eine Aufgabe generiert werden soll.

Amazon FSx übermittelt den Bericht an das verknüpfte Daten-Repository des Dateisystems in Amazon S3 und verwendet dabei den Pfad, den Sie angeben, wenn Sie den Bericht für eine Aufgabe aktivieren. Der Dateiname des Berichts ist `report.csv` für Importaufgaben und `failures.csv` für Export- oder Release-Aufgaben vorgesehen.

Das Berichtsformat ist eine Datei mit kommagetrennten Werten (CSV) mit drei Feldern: `FilePath`, `FileStatus`, und `ErrorCode`

Berichte werden mit der Kodierung im RFC-4180-Format wie folgt codiert:

- Pfade, die mit einem der folgenden Zeichen beginnen, sind in einfachen Anführungszeichen enthalten: `@ + - =`
- Zeichenfolgen, die mindestens eines der folgenden Zeichen enthalten, sind in doppelten Anführungszeichen enthalten: `" ,`
- Alle doppelten Anführungszeichen werden durch ein zusätzliches doppeltes Anführungszeichen maskiert.

Im Folgenden finden Sie einige Beispiele für die Berichtskodierung:

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

Weitere Informationen zur RFC-4180-Kodierung finden Sie unter [RFC-4180 — Common Format and MIME Type for Comma-Separated Values \(CSV\)](#) -Dateien auf der IETF-Website.

Im Folgenden finden Sie ein Beispiel für die Informationen in einem Bericht zum Abschluss einer Aufgabe, der nur fehlgeschlagene Dateien enthält.

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

Weitere Informationen zu Aufgabenfehlern und deren Behebung finden Sie unter [Behebung von Fehlern bei Datenrepository-Aufgaben](#).

Behebung von Fehlern bei Datenrepository-Aufgaben

Sie können die [Protokollierung in Logs aktivieren](#), um Informationen über Fehler zu CloudWatch protokollieren, die beim Import oder Export von Dateien mithilfe von Datenrepository-Tasks aufgetreten sind. Informationen zu CloudWatch Protokoll-Ereignisprotokollen finden Sie unter [Datenrepository-Ereignisprotokolle](#).

Wenn eine Datenrepository-Aufgabe fehlschlägt, finden Sie die Anzahl der Dateien, die Amazon FSx nicht verarbeiten konnte, unter Dateien konnten nicht exportiert werden auf der Task-Statusseite der Konsole. Oder Sie können die CLI oder API verwenden und die `Status: FailedCount` Eigenschaft der Aufgabe anzeigen. Informationen zum Zugriff auf diese Informationen finden Sie unter [Zugreifen auf Datenrepository-Aufgaben](#).

Für Datenrepository-Aufgaben stellt Amazon FSx optional auch Informationen zu den spezifischen Dateien und Verzeichnissen, bei denen Fehler aufgetreten sind, in einem Abschlussbericht bereit. Der Bericht über den Abschluss der Aufgabe enthält den Datei- oder Verzeichnispfad auf dem Lustre-Dateisystem, der ausgefallen ist, seinen Status und die Fehlerursache. Weitere Informationen finden Sie unter [Arbeiten mit Berichten über den Abschluss von Aufgaben](#).

Eine Datenrepository-Aufgabe kann aus verschiedenen Gründen fehlschlagen, unter anderem aus den unten aufgeführten Gründen.

Fehlercode	Erklärung
<code>FileSizeTooLarge</code>	Die maximale Objektgröße, die von Amazon S3 unterstützt wird, beträgt 5 TiB.
<code>InternalError</code>	Im Amazon FSx-Dateisystem ist bei einer Import-, Export- oder Release-Aufgabe ein

Fehlercode	Erklärung
	<p>Fehler aufgetreten. Im Allgemeinen bedeutet dieser Fehlercode, dass sich das Amazon FSx-Dateisystem, auf dem die fehlgeschlagene Aufgabe ausgeführt wurde, im Lebenszyklusstatus FAILED befindet. In diesem Fall können die betroffenen Dateien aufgrund von Datenverlust möglicherweise nicht wiederhergestellt werden. Andernfalls können Sie HSM-Befehle (Hierarchical Storage Management) verwenden, um die Dateien und Verzeichnisse in das Daten-Repository auf S3 zu exportieren. Weitere Informationen finden Sie unter Exportieren von Dateien mithilfe von HSM-Befehlen.</p>
OperationNotPermitted	<p>Amazon FSx konnte die Datei nicht veröffentlichen, da sie nicht in einen verknüpften S3-Bucket exportiert wurde. Sie müssen automatische Export- oder Export-Datenrepository-Aufgaben verwenden, um sicherzustellen, dass Ihre Dateien zuerst in Ihren verknüpften Amazon S3 S3-Bucket exportiert werden.</p>
PathSizeTooLong	<p>Der Exportpfad ist zu lang. Die maximale Länge des Objektschlüssels, die von S3 unterstützt wird, beträgt 1.024 Zeichen.</p>
ResourceBusy	<p>Amazon FSx konnte die Datei nicht exportieren oder veröffentlichen, da von einem anderen Client im Dateisystem auf sie zugegriffen wurde. Sie können es erneut versuchen, DataRepositoryTask nachdem Ihr Workflow das Schreiben in die Datei abgeschlossen hat.</p>

Fehlercode	Erklärung
S3AccessDenied	<p>Der Zugriff auf Amazon S3 wurde für eine Export- oder Importaufgabe des Datenrepositorys verweigert.</p> <p>Für Exportaufgaben muss das Amazon FSx-Dateisystem über die Berechtigung verfügen, den <code>S3:PutObject</code> Vorgang zum Exportieren in ein verknüpftes Daten-Repository auf S3 durchzuführen. Diese Berechtigung wird in der <code>AWSServiceRoleForFSxS3Access_fs-0123456789abcdef0</code> serviceverknüpften Rolle erteilt. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon FSx.</p> <p>Da bei Exportaufgaben Daten außerhalb der VPC eines Dateisystems fließen müssen, kann dieser Fehler auftreten, wenn das Ziel-Repository über eine Bucket-Richtlinie verfügt, die einen der globalen Bedingungsschlüssel <code>aws:SourceVpc</code> oder <code>aws:SourceVpcE</code> IAM-Bedingungsschlüssel enthält.</p> <p>Für Importaufgaben muss das Amazon FSx-Dateisystem über die Berechtigung verfügen, die <code>S3:GetObject</code> AND-Operationen für den <code>S3:HeadObject</code> Import aus einem verknüpften Daten-Repository auf S3 durchzuführen.</p> <p>Wenn Ihr S3-Bucket für Importaufgaben serverseitige Verschlüsselung mit in AWS Key Management Service (SSE-KMS) gespeicherten kundenverwalteten Schlüsseln verwendet, müssen Sie die Richtlinienkonfigurationen unter Arbeiten mit serverseitig verschlüsselten Amazon S3 S3-Buckets befolgen.</p>

Fehlercode	Erklärung
	<p>Wenn Ihr S3-Bucket Objekte enthält, die von einem anderen AWS-Konto als Ihrem mit dem Dateisystem verknüpften S3-Bucket-Konto hochgeladen wurden, können Sie sicherstellen, dass Ihre Datenrepository-Aufgaben S3-Metadaten ändern oder S3-Objekte überschreiben können, unabhängig davon, welches Konto sie hochgeladen hat. Wir empfehlen Ihnen, die Funktion S3-Objektbesitz für Ihren S3-Bucket zu aktivieren. Mit dieser Funktion können Sie die Verantwortung für neue Objekte übernehmen, die von anderen in Ihren Bucket AWS-Konten hochgeladen werden, indem Sie Uploads dazu zwingen, die gespeicherte ACL <code>-/-acl bucket-owner-full-control</code> bereitzustellen. Sie aktivieren S3 Object Ownership, indem Sie in Ihrem S3-Bucket die bevorzugte Option des Bucket-Besitzers auswählen. Weitere Informationen finden Sie unter Steuern des Eigentums an hochgeladenen Objekten mithilfe von S3 Object Ownership im Amazon S3 S3-Benutzerhandbuch.</p>
S3Error	<p>Amazon FSx ist auf einen S3-bezogenen Fehler gestoßen, der nicht aufgetreten ist.</p> <p>S3AccessDenied</p>
S3FileDeleted	<p>Amazon FSx konnte eine Hardlink-Datei nicht exportieren, da die Quelldatei nicht im Datenrepository existiert.</p>

Fehlercode	Erklärung
S3objectInUnsupportedTier	Amazon FSx hat erfolgreich ein Objekt ohne Symlink aus einer Speicherklasse S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive importiert. Das <code>FileStatus</code> wird im Bericht über den Abschluss der <code>succeeded with warning</code> Aufgabe enthalten sein. Die Warnung weist darauf hin, dass Sie zum Abrufen der Daten zuerst das Objekt S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive wiederherstellen und dann einen <code>hsm_restore</code> Befehl verwenden müssen, um das Objekt zu importieren.
S3objectNotFound	Amazon FSx konnte die Datei nicht importieren oder exportieren, da sie nicht im Daten-Repository existiert.
S3objectPathNotPosixCompliant	Das Amazon S3 S3-Objekt ist vorhanden, kann aber nicht importiert werden, da es kein POSIX-kompatibles Objekt ist. Informationen zu unterstützten POSIX-Metadaten finden Sie unter Unterstützung von POSIX-Metadaten für Daten-Repositorys
S3objectUpdateInProgressFromFileRename	Amazon FSx konnte die Datei nicht veröffentlichen, da der automatische Export eine Umbenennung der Datei verarbeitet. Der automatische Umbenennungsprozess für den Export muss abgeschlossen sein, bevor die Datei veröffentlicht werden kann.

Fehlercode	Erklärung
S3SymlinkInUnsupportedTier	Amazon FSx konnte ein Symlink-Objekt nicht importieren, da es sich in einer Amazon S3 S3-Speicherklasse befindet, die nicht unterstützt wird, wie z. B. einer S3 Glacier Flexible Retrieval- oder S3 Glacier Deep Archive Archive-Speicherklasse. Das FileStatus wird failed im Bericht über den Abschluss der Aufgabe stehen.
SourceObjectDeletedBeforeReleasing	Amazon FSx konnte die Datei nicht aus dem Dateisystem freigeben, da die Datei aus dem Daten-Repository gelöscht wurde, bevor sie veröffentlicht werden konnte.

Dateien werden freigegeben

Release-Datenrepository-Aufgaben geben Dateidaten aus Ihrem FSx for Lustre-Dateisystem frei, um Speicherplatz für neue Dateien freizugeben. Beim Freigeben einer Datei werden die Dateiliste und die Metadaten beibehalten, aber die lokale Kopie des Dateiinhalts wird entfernt. Wenn ein Benutzer oder eine Anwendung auf eine veröffentlichte Datei zugreift, werden die Daten automatisch und transparent aus Ihrem verknüpften Amazon S3 S3-Bucket wieder in Ihr Dateisystem geladen.

Note

Release-Datenrepository-Aufgaben sind auf FSx for Lustre 2.10-Dateisystemen nicht verfügbar.

Die Parameter Dateisystempfade bis zur Veröffentlichung und Mindestdauer seit dem letzten Zugriff legen fest, welche Dateien veröffentlicht werden.

- Dateisystempfade zur Veröffentlichung: Gibt den Pfad an, von dem aus Dateien veröffentlicht werden.
- Mindestdauer seit dem letzten Zugriff: Gibt die Dauer in Tagen an, sodass alle Dateien, auf die innerhalb dieser Zeit nicht zugegriffen wurde, veröffentlicht werden sollen. Die Dauer seit dem

letzten Zugriff auf eine Datei wird anhand der Differenz zwischen der Erstellungszeit der Release-Aufgabe und dem Zeitpunkt des letzten Zugriffs auf eine Datei berechnet (Maximalwert von `atimetime`, und `ctime`).

Dateien werden nur dann entlang des Dateipfads veröffentlicht, wenn sie nach S3 exportiert wurden und eine Dauer seit dem letzten Zugriff haben, die größer ist als der Wert für die Mindestdauer seit dem letzten Zugriff. Wenn Sie eine Mindestdauer seit dem letzten Zugriff von 0 Tagen angeben, werden Dateien unabhängig von ihrer Dauer seit dem letzten Zugriff veröffentlicht.

Note

Die Verwendung von Platzhaltern zum Ein- oder Ausschließen von Dateien für die Veröffentlichung wird nicht unterstützt.

Bei Aufgaben zur Freigabe von Datenrepositorien werden nur Daten aus Dateien freigegeben, die bereits in ein verknüpftes S3-Datenrepositorium exportiert wurden. Sie können Daten entweder mit der automatischen Exportfunktion, einer Aufgabe zum Exportieren eines Datenrepositoriums oder mit HSM-Befehlen nach S3 exportieren. Um zu überprüfen, ob eine Datei in Ihr Daten-Repositorium exportiert wurde, können Sie den folgenden Befehl ausführen. Ein Rückgabewert von `states : (0x00000009) exists archived` gibt an, dass die Datei erfolgreich exportiert wurde.

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

Note

Sie müssen den HSM-Befehl als Root-Benutzer oder mithilfe von `sudo` ausführen.

Um Dateidaten in regelmäßigen Intervallen freizugeben, können Sie mit Amazon EventBridge Scheduler eine wiederkehrende Aufgabe für das Release-Daten-Repositorium planen. Weitere Informationen finden Sie unter [Erste Schritte mit EventBridge Scheduler](#) im Amazon EventBridge Scheduler-Benutzerhandbuch.

Themen

- [Verwenden von Datenrepositorium-Aufgaben zur Freigabe von Dateien](#)

Verwenden von Datenrepository-Aufgaben zur Freigabe von Dateien

Gehen Sie wie folgt vor, um Aufgaben zu erstellen, die Dateien mithilfe der Amazon FSx-Konsole und CLI aus dem Dateisystem freigeben. Beim Freigeben einer Datei werden die Dateiliste und die Metadaten beibehalten, aber die lokale Kopie des Inhalts dieser Datei wird entfernt.

Um Dateien freizugeben (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im linken Navigationsbereich Dateisysteme und anschließend Ihr Lustre-Dateisystem aus.
3. Wählen Sie die Registerkarte Daten-Repository.
4. Wählen Sie im Bereich Datenrepository-Verknüpfungen die Datenrepository-Zuordnung aus, für die Sie die Release-Aufgabe erstellen möchten.
5. Wählen Sie für Aktionen die Option Veröffentlichungsaufgabe erstellen aus. Diese Option ist nur verfügbar, wenn das Dateisystem mit einem Daten-Repository auf S3 verknüpft ist. Das Aufgabendialogfeld Release-Daten-Repository erstellen wird angezeigt.

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

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

Report format

REPORT_CSV_20191124


Report scope

FAILED_FILES_ONLY

Cancel

Create data repository task

6. Geben Sie unter Dateisystempfade zur Veröffentlichung bis zu 32 Verzeichnisse oder Dateien an, die aus Ihrem Amazon FSx-Dateisystem freigegeben werden sollen, indem Sie die Pfade zu diesen Verzeichnissen oder Dateien angeben. Die Pfade, die Sie angeben, müssen sich auf den Einhängpunkt des Dateisystems beziehen. Wenn der Einhängpunkt beispielsweise eine Datei auf dem Dateisystem `/mnt/fsx/path1` ist `/mnt/fsx` und ist, die Sie veröffentlichen möchten, dann ist der bereitzustellende Pfad `path1`. Um alle Dateien im Dateisystem freizugeben, geben Sie einen Schrägstrich (`/`) als Pfad an.

 Note

Wenn ein von Ihnen angegebener Pfad nicht gültig ist, schlägt die Aufgabe fehl.

7. Geben Sie unter Mindestdauer seit letztem Zugriff die Dauer in Tagen an, sodass alle Dateien, auf die in dieser Zeit nicht zugegriffen wurde, freigegeben werden sollen. Die Zeit des letzten Zugriffs wird anhand des Maximalwerts von `atimemtime`, und berechnet `time`. Dateien, deren Dauer des letzten Zugriffs länger ist als die Mindestdauer seit dem letzten Zugriff (im Verhältnis zur Erstellungszeit der Aufgabe), werden veröffentlicht. Dateien mit einer Dauer des letzten Zugriffs unter dieser Anzahl von Tagen werden nicht veröffentlicht, auch wenn sie sich im Feld Dateisystempfade zur Veröffentlichung befinden. Geben Sie unabhängig von der Dauer seit dem letzten Zugriff eine Dauer von `0` Tagen für die Freigabe von Dateien an.
8. (Optional) Wählen Sie unter Abschlussbericht die Option Aktivieren aus, um einen Bericht zum Abschluss der Aufgabe zu erstellen, der Details zu den Dateien enthält, die den unter Berichtsbereich angegebenen Umfang erfüllen. Um einen Speicherort für Amazon FSx anzugeben, an dem der Bericht übermittelt werden soll, geben Sie als Berichtspfad einen relativen Pfad im verknüpften S3-Daten-Repository des Dateisystems ein.
9. Wählen Sie die Aufgabe „Datenrepository erstellen“.

Eine Benachrichtigung oben auf der Seite Dateisysteme zeigt an, dass die Aufgabe, die Sie gerade erstellt haben, in Bearbeitung ist.

Um den Status und die Details der Aufgabe einzusehen, scrollen Sie auf der Registerkarte Daten-Repository nach unten zu Datenrepository-Aufgaben. In der Standardsortierreihenfolge wird die neueste Aufgabe ganz oben in der Liste angezeigt.

Um auf dieser Seite eine Aufgabenzusammenfassung anzuzeigen, wählen Sie die Task-ID für die Aufgabe, die Sie gerade erstellt haben.

Um Dateien freizugeben (CLI)

- Verwenden Sie den [create-data-repository-task](#) CLI-Befehl, um eine Aufgabe zu erstellen, die Dateien auf Ihrem FSx for Lustre-Dateisystem veröffentlicht. Die entsprechende API-Operation ist [CreateDataRepositoryTask](#).

Legen Sie die folgenden Parameter fest:

- Geben `--file-system-id` Sie die ID des Dateisystems ein, aus dem Sie Dateien freigeben.
- Legt `--paths` die Pfade auf dem Dateisystem fest, aus dem die Daten veröffentlicht werden. Wenn ein Verzeichnis angegeben ist, werden die Dateien innerhalb des Verzeichnisses freigegeben. Wenn ein Dateipfad angegeben ist, wird nur diese Datei veröffentlicht. Um alle Dateien im Dateisystem freizugeben, die in einen verknüpften S3-Bucket exportiert wurden, geben Sie einen Schrägstrich (`/`) für den Pfad an.
- Setzen Sie `--type` auf `RELEASE_DATA_FROM_FILESYSTEM`.
- Stellen Sie die `--release-configuration` `DurationSinceLastAccess` Optionen wie folgt ein:
 - `Unit` – Eingestellt auf `DAYS`.
 - `Value`— Geben Sie eine Ganzzahl an, die die Dauer in Tagen angibt, sodass alle Dateien, auf die in dieser Zeit nicht zugegriffen wurde, veröffentlicht werden sollen. Dateien, auf die in einem Zeitraum von weniger als dieser Anzahl von Tagen zugegriffen wurde, werden nicht veröffentlicht, auch wenn sie im `--paths` Parameter enthalten sind. Geben Sie unabhängig von der Dauer seit dem letzten Zugriff eine Dauer von `0` Tagen für die Freigabe von Dateien an.

Dieser Beispielbefehl gibt an, dass Dateien, die in einen verknüpften S3-Bucket exportiert wurden und die `--release-configuration` Kriterien erfüllen, aus den Verzeichnissen in den angegebenen Pfaden veröffentlicht werden.

```
$ 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
```

Nach erfolgreicher Erstellung der Datenrepository-Aufgabe gibt Amazon FSx die Aufgabenbeschreibung als JSON zurück.

Nachdem Sie die Aufgabe zur Freigabe von Dateien erstellt haben, können Sie den Status der Aufgabe überprüfen. Weitere Informationen zum Anzeigen von Datenrepository-Aufgaben finden Sie unter [Zugreifen auf Datenrepository-Aufgaben](#).

Amazon FSx mit Ihren lokalen Daten verwenden

Sie können FSx for Lustre verwenden, um Ihre lokalen Daten mit In-Cloud-Recheninstanzen zu verarbeiten. FSx for Lustre unterstützt den Zugriff über AWS Direct Connect und VPN, sodass Sie Ihre Dateisysteme von lokalen Clients aus mounten können.

Um FSx for Lustre mit Ihren lokalen Daten zu verwenden

1. Erstellen eines Dateisystems. Weitere Informationen finden Sie [Erstellen Sie Ihr FSx for Lustre-Dateisystem](#) in der Übung Erste Schritte.
2. Mounten Sie das Dateisystem von lokalen Clients aus. Weitere Informationen finden Sie unter [Mounten von Amazon FSx-Dateisystemen vor Ort oder über eine Peering-Amazon VPC](#).
3. Kopieren Sie die Daten, die Sie verarbeiten möchten, in Ihr FSx for Lustre-Dateisystem.
4. Führen Sie Ihren rechenintensiven Workload auf Amazon EC2 EC2-Instances in der Cloud aus, die Ihr Dateisystem mounten.
5. Wenn Sie fertig sind, kopieren Sie die Endergebnisse aus Ihrem Dateisystem zurück an Ihren lokalen Datenspeicherort und löschen Sie Ihr FSx for Lustre-Dateisystem.

Datenrepository-Ereignisprotokolle

Sie können die Protokollierung in CloudWatch Logs aktivieren, um Informationen über Fehler beim Import oder Export von Dateien mithilfe von Aufgaben zum automatischen Import, automatischen Export und zur Datenablage zu protokollieren. Weitere Informationen finden Sie unter [Protokollierung mit Amazon CloudWatch Logs](#).

Note

Wenn eine Datenrepository-Aufgabe fehlschlägt, schreibt Amazon FSx auch Fehlerinformationen in den Aufgabenabschlussbericht. Weitere Informationen zu

Fehlerinformationen in Abschlussberichten finden Sie unter [Behebung von Fehlern bei Datenrepository-Aufgaben](#).

Automatische Import-, automatische Export- und Datenrepository-Aufgaben können aus verschiedenen Gründen fehlschlagen, darunter die unten aufgeführten. Informationen zum Anzeigen dieser Protokolle finden Sie unter [Anzeigen von -Protokollen](#).

Ereignisse importieren

Fehlercode	Protokollebene	Nachrichteinhalt	Ursache	Fehlercode im Abschlussbericht
S3ImportListObjectError	ERROR	<i>Fehler beim Auflisten von S3-Objekten im S3-Bucket bucket_name mit Präfixpräfix.</i>	Amazon FSx konnte S3-Objekte nicht im S3-Bucket auflisten. Dies kann passieren, wenn die S3-Bucket-Richtlinie Amazon FSx keine ausreichenden Berechtigungen gewährt.	N/A
S3ImportUnsupportedTierWarning	WARN	<i>Das S3-Objekt mit dem Schlüssel key_value konnte nicht in den S3-Bucket bucket_name</i>	Amazon FSx konnte ein S3-Objekt nicht importieren, da es sich in einer Amazon S3 S3-Speicherklasse befindet, die nicht unterstützt	S3ObjectUnsupportedTier

Fehlercode	Protokolebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
		<i>me importiert werden, da ein S3-Objekt der Stufe S3_Tier_N ame nicht unterstützt wird.</i>	zt wird, wie z. B. S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive.	
S3ImportSymlinkInUnsuportedTierWarning	WARN	<i>Das S3-Objekt mit dem Schlüssel key_value im S3-Bucket bucket_name konnte aufgrund eines S3-Symlink-Objekts in einer nicht unterstützten Stufe S3_Tier_N ame nicht importiert werden.</i>	Amazon FSx konnte ein Symlink-Objekt nicht importieren, da es sich in einer Amazon S3 S3-Speicherkategorie befindet, die nicht unterstützt wird, wie z. B. S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive.	S3SymlinkInUnsuportedTier

Fehlercode	Protokolebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ImportAccessDenied	ERROR	Das S3-Objekt mit dem Schlüssel <i>key_value in den S3-Bucket bucket_name</i> konnte nicht importiert werden, da der Zugriff auf das S3-Objekt verweigert wurde.	<p>Der Zugriff auf Amazon S3 wurde für eine Aufgabe zum Exportieren eines Datenrepositorys verweigert.</p> <p>Für Importaufgaben muss das Amazon FSx-Dateisystem über die Berechtigung verfügen, die <code>s3:GetObject</code> AND-Operationen für den <code>s3:HeadObject</code> Import aus einem verknüpften Daten-Repository auf S3 durchzuführen.</p> <p>Wenn Ihr S3-Bucket für Importauf</p>	S3AccessDenied

Fehlercode	Protokolebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
			gaben serverseitige Verschlüsselung mit in AWS Key Management Service (SSE-KMS) gespeicherten kundenverwalteten Schlüsseln verwendet, müssen Sie die Richtlinienkonfigurationen unter befolgen. Arbeiten mit serverseitig verschlüsselten Amazon S3 S3-Buckets	

Fehlercode	Protokolebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ImportDeleteAccessDenied	ERROR	Die lokale Datei für das S3-Objekt mit dem Schlüssel <i>key_value</i> im S3-Bucket <i>bucket_name</i> konnte nicht gelöscht werden, da der Zugriff auf das S3-Objekt verweigert wurde.	Dem automatischen Import wurde der Zugriff auf ein S3-Objekt verweigert.	N/A

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ImportObjectPathNotPosixCompliant	ERROR	Das S3-Objekt mit dem Schlüssel <i>key_value</i> konnte nicht in den S3-Bucket <i>bucket_name</i> importiert werden, da das S3-Objekt nicht POSIX-konform ist.	Das Amazon S3 S3-Objekt ist vorhanden, kann aber nicht importiert werden, da es kein POSIX-kompatibles Objekt ist. Informationen zu unterstützten POSIX-Metadaten finden Sie unter. Unterstützung von POSIX-Metadaten für Daten-Repositorys	S3objectPathNotPosixCompliant

Fehlercode	Protokolebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ImportObjectTypeMismatch	ERROR	Das S3-Objekt mit dem Schlüssel <i>key_value</i> konnte nicht in den S3-Bucket <i>bucket_name</i> importiert werden, da bereits ein S3-Objekt mit demselben Namen in das Dateisystem importiert wurde.	Das importierte S3-Objekt ist von einem anderen Typ (Datei oder Verzeichnis) als ein vorhandenes Objekt mit demselben Namen im Dateisystem.	S3objectTypeMismatch
S3ImportDirectoryMetadataUpdateError	ERROR	Die Metadaten des lokalen Verzeichnisses konnten aufgrund eines internen Fehlers nicht aktualisiert werden.	Verzeichnismetadaten konnten aufgrund eines internen Fehlers nicht importiert werden.	N/A

Fehlercode	Protokolebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ImportObjectDeleted	ERROR	<i>Das S3-Objekt mit dem Schlüssel <code>key_value</code> konnte nicht importiert werden, da es nicht im S3-Bucket <code>bucket_name</code> gefunden wurde.</i>	Amazon FSx konnte Dateimetadaten nicht importieren, da das entsprechende Objekt nicht im Daten-Repository existiert.	S3FileDeleted
S3ImportBucketDoesNotExist	ERROR	Das S3-Objekt mit dem Schlüssel <code>key_value</code> konnte nicht in den S3-Bucket <code>bucket_name</code> importiert werden, da der Bucket nicht existiert.	Amazon FSx kann ein S3-Objekt nicht automatisch in das Dateisystem importieren, da der S3-Bucket nicht mehr existiert.	N/A

Fehlercode	Protokolebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ImportDeleteBucketDoesNotExist	ERROR	Die lokale Datei für das S3-Objekt mit dem Schlüssel <i>key_value</i> im <i>S3-Bucket</i> <i>bucket_name</i> konnte nicht gelöscht werden, da der Bucket nicht existiert.	Amazon FSx kann eine mit einem S3-Objekt verknüpfte Datei im Dateisystem nicht löschen, da der S3-Bucket nicht mehr existiert.	N/A
S3ImportDirectoryCreateError	ERROR	Das lokale Verzeichnis konnte aufgrund eines internen Fehlers nicht erstellt werden.	Amazon FSx konnte eine Verzeichniserstellung aufgrund eines internen Fehlers nicht automatisch in das Dateisystem importieren.	N/A

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
NoDiskSpace	ERROR	Das S3-Objekt mit dem Schlüssel <i>key_value</i> konnte nicht in den S3-Bucket <i>bucket_name</i> importiert werden, da das Dateisystem voll ist.	Das Dateisystem hatte beim Erstellen der Datei oder des Verzeichnisses keinen Speicherplatz mehr auf den Metadaten servern.	N/A

Ereignisse exportieren

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ExportInternalError	ERROR	Das S3-Objekt mit dem Schlüssel <i>key_value</i> im S3-Bucket <i>bucket_name</i> konnte aufgrund eines internen Fehlers nicht exportiert werden.	Das Objekt wurde aufgrund eines internen Fehlers nicht exportiert.	INTERNAL_ERROR

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ExportAccessDenied	ERROR	<p><i>Die Datei konnte nicht exportiert werden, da der Zugriff auf das S3-Objekt mit dem Schlüssel <code>key_value</code> im S3-Bucket <code>bucket_name</code> verweigert wurde.</i></p>	<p>Der Zugriff auf Amazon S3 wurde für eine Datenrepository-Exportaufgabe verweigert.</p> <p>Für Exportaufgaben muss das Amazon FSx-Dateisystem über die Berechtigung verfügen, den <code>s3:PutObject</code> Vorgang zum Exportieren in ein verknüpft es Daten-Repository auf S3 durchzuführen. Diese Berechtigung wird in der <code>AWSServiceRoleForFSxS3Access_ fs-0123456789abcde f0</code> serviceverknüpften Rolle erteilt. Weitere Informationen finden Sie unter Verwenden</p>	S3AccessDenied

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
			<p>von serviceve rknüpften Rollen für Amazon FSx.</p> <p>Da für die Exportaufgabe Daten außerhalb der VPC eines Dateisystems fließen müssen, kann dieser Fehler auftreten , wenn das Ziel-Repository über eine Bucket-Richtlinie verfügt, die einen der globalen Bedingungsschlüssel <code>aws:SourceVpc</code> oder <code>aws:SourceVpc:IAM-Conditionsschlüssel</code> enthält.</p> <p>Wenn Ihr S3-Bucket Objekte enthält, die von einem anderen AWS-Konto als Ihrem mit dem Dateisystem</p>	

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
			<p>verknüpften S3-Bucket-Konto hochgeladen wurden, können Sie sicherstellen, dass Ihre Datenrepository-Aufgaben unabhängig davon, welches Konto sie hochgeladen hat, S3-Metadaten ändern oder S3-Objekte überschreiben können. Wir empfehlen Ihnen, die Funktion S3-Objektbesitz für Ihren S3-Bucket zu aktivieren. Mit dieser Funktion können Sie die Verantwortung für neue Objekte übernehmen, die von anderen in Ihren Bucket AWS-Konten hochgeladen werden, indem Sie Uploads</p>	

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
			<p>dazu zwingen, die gespeicherte ACL <code>--acl bucket-owner-full-control</code> bereitzustellen. Sie aktivieren S3 Object Ownership, indem Sie in Ihrem S3-Bucket die bevorzugte Option des Bucket-Besitzers auswählen. Weitere Informationen finden Sie unter Steuern des Eigentums an hochgeladenen Objekten mithilfe von S3 Object Ownership im Amazon S3 S3-Benutzerhandbuch.</p>	

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ExportPathSizeTooLong	ERROR	Die Datei konnte nicht exportiert werden, da die Größe des lokalen Dateipfads die von S3 unterstützte maximale Objektschlüssellänge überschreitet.	Der Exportpfad ist zu lang. Die von S3 unterstützte maximale Länge des Objektschlüssels beträgt 1.024 Zeichen.	PathSizeTooLong
S3ExportFileSizeTooLarge	ERROR	Die Datei konnte nicht exportiert werden, da die Dateigröße die maximal unterstützte Größe von S3-Objekten überschreitet.	Die maximale Objektgröße, die von Amazon S3 unterstützt wird, beträgt 5 TiB.	FileSizeTooLarge

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ExportKMSKeyNotFound	ERROR	Die Datei für das S3-Objekt mit dem Schlüssel <i>key_value</i> <i>im S3-Bucket</i> <i>bucket_name</i> konnte nicht exportiert werden, da der KMS-Schlüssel des Buckets nicht gefunden wurde.	Amazon FSx konnte die Datei nicht exportieren, da sie nicht gefunden werden konnte. Achten Sie darauf, einen Schlüssel zu verwenden, der sich im selben Ordner AWS-Region wie der S3-Bucket befindet. Weitere Informationen zum Erstellen von KMS-Schlüsseln finden Sie unter Creating Keys im AWS Key Management Service Developer Guide.	N/A

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ExportResourceBusy	ERROR	Die Datei konnte nicht exportiert werden, da sie von einem anderen Prozess verwendet wird.	Amazon FSx konnte die Datei nicht exportieren, da sie von einem anderen Client im Dateisystem geändert wurde. Sie können die Aufgabe erneut versuchen, nachdem Ihr Workflow das Schreiben in die Datei abgeschlossen hat.	ResourceBusy

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3ExportLocalObjectReleaseWithoutS3Source	WARN	<i>Export übersprungen: Die lokale Datei befindet sich im Status „Freigegeben“ und ein verknüpftes S3-Objekt mit dem Schlüssel key_value wurde im Bucket bucket_name nicht gefunden.</i>	Amazon FSx konnte die Datei nicht exportieren, da sie sich im Dateisystem in einem freigegebenen Zustand befand.	N/A
S3ExportLocalObjectNotMatchDra	WARN	Der Export wurde übersprungen: Die lokale Datei gehört nicht zu einem mit einem Daten-Repository verknüpften Dateisystempfad.	Amazon FSx konnte nicht exportieren, da das Objekt nicht zu einem Dateisystempfad gehört, der mit einem Daten-Repository verknüpft ist.	N/A

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
InternalAutoExportError	ERROR	Beim automatischen Export ist beim Export eines Dateisystemobjekts ein interner Fehler aufgetreten	Der Export ist aufgrund eines internen Fehlers (Autoexport oder Lustrebene) fehlgeschlagen.	N/A
S3CompletionReportUploadFailure	ERROR	<i>Der Bericht über den Abschluss der Datenrepository-Aufgabe konnte nicht in bucket_name hochgeladen werden</i>	Amazon FSx konnte den Abschlussbericht nicht hochladen.	N/A

Fehlercode	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3CompletionReportValidateFailure	ERROR	Der Bericht über den Abschluss von Aufgaben im Datenrepository konnte nicht in den Bucket <i>bucket_name</i> hochgeladen werden, da der Pfad des Abschlussberichts <i>report_path</i> nicht zu einem Daten-Repository gehört, das mit diesem Dateisystem verknüpft ist	Amazon FSx konnte den Abschlussbericht nicht hochladen, da der vom Kunden bereitgestellte S3-Pfad nicht zu einem verknüpften Daten-Repository gehört.	N/A

Mit älteren Bereitstellungstypen arbeiten

Dieser Abschnitt gilt für Dateisysteme mit dem Bereitstellungstyp Scratch 1 sowie für Dateisysteme mit Scratch 2 oder Persistent 1-Bereitstellungstypen, die keine Datenrepository-Zuordnungen verwenden.

Themen

- [Verknüpfen Sie Ihr Dateisystem mit einem Amazon S3-Bucket](#)
- [Automatisches Importieren von Updates aus Ihrem S3-Bucket](#)

Verknüpfen Sie Ihr Dateisystem mit einem Amazon S3-Bucket

Wenn Sie ein Amazon FSx for Lustre-Dateisystem erstellen, können Sie es mit einem dauerhaften Datenrepository in Amazon S3 verknüpfen. Bevor Sie Ihr Dateisystem erstellen, stellen Sie sicher, dass Sie den Amazon S3-Bucket, auf den Sie verlinken, bereits erstellt haben. In der Dateisystem erstellen Assistent, Sie legen die folgenden Eigenschaften der Datenrepository-Konfiguration im optionalen Feld fest Importieren/Exportieren von Datenrepository Fensterscheibe.

- Wählen Sie, wie Amazon FSx Ihre Datei- und Verzeichnisliste auf dem neuesten Stand hält, wenn Sie nach der Erstellung des Dateisystems Objekte in Ihrem S3-Bucket hinzufügen oder ändern. Weitere Informationen finden Sie unter [Automatisches Importieren von Updates aus Ihrem S3-Bucket](#).
- Bucket importieren: Geben Sie den Namen des S3-Buckets ein, den Sie für das verknüpfte Repository verwenden.
- Präfix importieren: Geben Sie ein optionales Importpräfix ein, wenn Sie nur einige Datei- und Verzeichnislisten mit Daten in Ihrem S3-Bucket in Ihr Dateisystem importieren möchten. Das Importpräfix definiert, aus welchem Teil Ihres S3-Buckets Daten importiert werden sollen.
- Präfix exportieren: Definiert, wo Amazon FSx den Inhalt Ihres Dateisystems in Ihren verknüpften S3-Bucket exportiert.

Sie können ein 1:1 -Mapping verwenden, bei dem Amazon FSx Daten aus Ihrem FSx for Lustre-Dateisystem zurück in dieselben Verzeichnisse im S3-Bucket exportiert, aus denen sie importiert wurden. Um ein 1:1 -Mapping zu erhalten, geben Sie bei der Erstellung Ihres Dateisystems einen Exportpfad zum S3-Bucket ohne Präfixe an.

- Wenn Sie das Dateisystem mit der Konsole erstellen, wählen Sie Präfix exportieren > Ein von Ihnen spezifiziertes Präfix Option, und lassen Sie das Präfixfeld leer.
- Wenn Sie ein Dateisystem mit dem erstellen AWSCLI oder API, geben Sie den Exportpfad als Namen des S3-Buckets ohne zusätzliche Präfixe an, z. B. `ExportPath=s3://lustre-export-test-bucket/`.

Mit dieser Methode können Sie bei der Angabe des Importpfads ein Importpräfix angeben, ohne dass sich dies auf eine 1:1 -Zuordnung für Exporte auswirkt.

Erstellen von Dateisystemen, die mit einem S3-Bucket verknüpft sind

Die folgenden Verfahren führen Sie durch den Prozess der Erstellung eines Amazon FSx-Dateisystems, das mit einem S3-Bucket verknüpft ist, mithilfe der AWS Management-Konsole und der AWS Befehlszeilenschnittstelle (AWS CLI).

Console

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Dashboard **Dateisystem erstellen**.
3. Wählen Sie für den Dateisystemtyp **FSx für Lustre**, und wählen Sie dann **Weiter**.
4. Geben Sie die erforderlichen Informationen für die **Dateisystemdetails** und **Netzwerk und Sicherheit** Abschnitte. Weitere Informationen finden Sie unter [Erstellen Sie Ihr FSx for Lustre-Dateisystem](#).
5. Du benutzt die **Importieren/Exportieren von Datenrepositorien** Panel zur Konfiguration eines verknüpften Datenrepositorys in Amazon S3. Wählen Sie **Daten aus S3 importieren** und nach S3 exportieren zur Erweiterung der **Importieren/Exportieren von Datenrepositorien** schneiden Sie die Einstellungen des Datenrepositorys ab und konfigurieren Sie sie.

▼ 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

The name of an existing S3 bucket

Import prefix - optional [Info](#)

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

6. Wählen Sie, wie Amazon FSx Ihre Datei- und Verzeichnisliste auf dem neuesten Stand hält, wenn Sie Objekte in Ihrem S3-Bucket hinzufügen oder ändern. (Optional) Wenn Sie Ihr Dateisystem erstellen, werden Ihre vorhandenen S3-Objekte als Datei- und Verzeichnislisten angezeigt.
 - Aktualisiere meine Datei- und Verzeichnisliste, wenn Objekte zu meinem S3-Bucket hinzugefügt werden: (Standard) Amazon FSx aktualisiert automatisch die Datei- und Verzeichnislisten aller neuen Objekte, die dem verknüpften S3-Bucket hinzugefügt wurden und die derzeit nicht im FSx-Dateisystem vorhanden sind. Amazon FSx aktualisiert keine Angebote für Objekte, die sich im S3-Bucket geändert haben. Amazon FSx löscht keine Auflistungen von Objekten, die im S3-Bucket gelöscht wurden.

Note

Die Standardeinstellung für die Importeinstellungen für den Import von Daten aus einem verknüpften S3-Bucket mithilfe der CLI und der API lautet NONE. Die Standardeinstellung für Importeinstellungen bei Verwendung der Konsole besteht darin, Lustre zu aktualisieren, wenn dem S3-Bucket neue Objekte hinzugefügt werden.

- Aktualisiere meine Datei- und Verzeichnisliste, wenn Objekte zu meinem S3-Bucket hinzugefügt oder geändert werden: Amazon FSx aktualisiert automatisch die Datei- und Verzeichnislisten aller neuen Objekte, die dem S3-Bucket hinzugefügt wurden, sowie aller vorhandenen Objekte, die im S3-Bucket geändert wurden, nachdem Sie diese Option ausgewählt haben. Amazon FSx löscht keine Auflistungen von Objekten, die im S3-Bucket gelöscht wurden.
 - Aktualisiere meine Datei- und Verzeichnisliste, wenn Objekte zu meinem S3-Bucket hinzugefügt, geändert oder daraus gelöscht werden: Amazon FSx aktualisiert automatisch die Datei- und Verzeichnislisten aller neuen Objekte, die dem S3-Bucket hinzugefügt wurden, aller vorhandenen Objekte, die im S3-Bucket geändert wurden, und aller vorhandenen Objekte, die im S3-Bucket gelöscht werden, nachdem Sie diese Option ausgewählt haben.
 - Meine Datei nicht aktualisieren und nicht direkt auflisten, wenn Objekte zu meinem S3-Bucket hinzugefügt, geändert oder aus meinem S3-Bucket gelöscht werden- Amazon FSx aktualisiert Datei- und Verzeichnislisten aus dem verknüpften S3-Bucket nur, wenn das Dateisystem erstellt wird. FSx aktualisiert keine Datei- und Verzeichnislisten für neue, geänderte oder gelöschte Objekte, nachdem Sie diese Option ausgewählt haben.
7. Geben Sie ein optionales Präfix importieren wenn Sie nur einige der Datei- und Verzeichnislisten der Daten in Ihrem S3-Bucket in Ihr Dateisystem importieren möchten. Das Importpräfix definiert, aus welchem Teil Ihres S3-Buckets Daten importiert werden sollen. Weitere Informationen finden Sie unter [Automatisches Importieren von Updates aus Ihrem S3-Bucket](#).
 8. Wählen Sie eine der verfügbaren Präfix exportieren Optionen:
 - Ein eindeutiges Präfix, das Amazon FSx in Ihrem Bucket erstellt: Wählen Sie diese Option, um neue und geänderte Objekte mit einem von FSx for Lustre generierten Präfix zu exportieren. Das Präfix sieht wie folgt aus: /FSxLustre*file-system-*

creation- timestamp. Der Zeitstempel weist das UTC-Format auf, z. B. FSxLustre20181105T222312Z.

- Das gleiche Präfix, aus dem Sie importiert haben (ersetzen Sie vorhandene Objekte durch aktualisierte): Wählen Sie diese Option, um bestehende Objekte durch aktualisierte zu ersetzen.
 - Ein Präfix, das Sie angeben: Wählen Sie diese Option, um Ihre importierten Daten beizubehalten und neue und geänderte Objekte mit einem von Ihnen angegebenen Präfix zu exportieren. Um beim Exportieren von Daten in Ihren S3-Bucket ein 1:1 -Mapping zu erreichen, wählen Sie diese Option und lassen Sie das Präfixfeld leer. FSx exportiert Daten in dieselben Verzeichnisse, aus denen sie importiert wurden.
9. (Optionales) SetWartungspräferenzen, oder verwenden Sie die Standardeinstellungen des Systems.
 10. Wählen Sie Weiter, und überprüfen Sie die Dateisystemeinstellungen. Nehmen Sie bei Bedarf Änderungen vor.
 11. Wählen Sie Create file system (Dateisystem erstellen) aus.

AWS CLI

Im folgenden Beispiel wird ein Amazon FSx-Dateisystem erstellt, das mit dem verknüpft ist `lustre-export-test-bucket`, mit einer Importeinstellung, die alle neuen, geänderten und gelöschten Dateien in das verknüpfte Datenrepository importiert, nachdem das Dateisystem erstellt wurde.

Note

Die Standardeinstellung für die Importeinstellungen für den Import von Daten aus einem verknüpften S3-Bucket mithilfe der CLI und der API lautet `NONE`, was sich vom Standardverhalten bei Verwendung der Konsole unterscheidet.

Verwenden Sie den Amazon FSx CLI-Befehl, um ein FSx for Lustre-Dateisystem zu erstellen [create-file-system](#), wie unten gezeigt. Die entsprechende API-Operation ist [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
```

Nachdem Sie das Dateisystem erfolgreich erstellt haben, gibt Amazon FSx die Dateisystembeschreibung als JSON zurück, wie im folgenden Beispiel gezeigt.

```
{  
  "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
}
]
```

Den Exportpfad eines Dateisystems anzeigen

Sie können den Exportpfad eines Dateisystems mithilfe der FSx for Lustre-Konsole einsehen, der AWS CLI und die API.

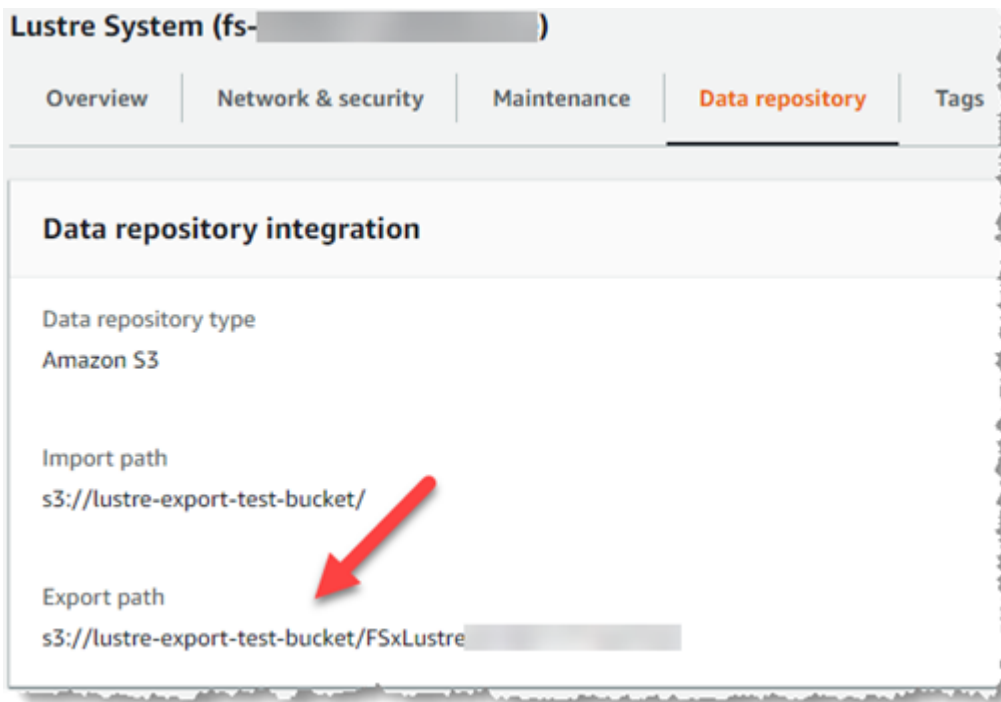
Console

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>
2. Wählen Sie `Name` des Dateisystems oder `Dateisystem-ID` für das FSx for Lustre-Dateisystem, für das Sie den Exportpfad anzeigen möchten.

Die Seite mit den Dateisystemdetails für dieses Dateisystem wird angezeigt.

3. Wählen Sie den `Datenspeicher`-Tab.

Das Fenster `Integration von Datenrepositorien` mit den Import- und Exportpfaden wird angezeigt.



CLI

Um den Exportpfad für Ihr Dateisystem zu ermitteln, verwenden Sie den [describe-file-systems](#) AWSCLI-Befehl.

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

Suchen Sie nach dem `ExportPath` Eigentum unter `LustreConfiguration` in der Antwort.

```
{
  "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"
}
```

Status des Lebenszyklus des Datenrepositorys

Der Lebenszyklusstatus des Datenrepositorys enthält Statusinformationen über das verknüpfte Datenrepository des Dateisystems. Ein Datenrepository kann die folgenden Lebenszyklusstatus haben.

- Erstellen: Amazon FSx erstellt die Datenrepository-Konfiguration zwischen dem Dateisystem und dem verknüpften Datenrepository. Das Datenrepository ist nicht verfügbar.
- Verfügbar: Das Datenrepository kann verwendet werden.
- Aktualisierung: Die Konfiguration des Datenrepositorys wird gerade einem vom Kunden initiierten Update unterzogen, das sich auf die Verfügbarkeit auswirken könnte.
- Falsch konfiguriert: Amazon FSx kann Updates nicht automatisch aus dem S3-Bucket importieren, bis die Konfiguration des Datenrepositorys korrigiert ist. Weitere Informationen finden Sie unter [Fehlerbehebung bei einem falsch konfigurierten verknüpften S3-Bucket](#).

Sie können den Lebenszyklusstatus eines verknüpften Datenrepositorys eines Dateisystems mithilfe der Amazon FSx-Konsole einsehen, der AWS-Befehlszeilenschnittstelle und die Amazon FSx-API. In

der Amazon FSx-Konsole können Sie auf das Datenrepository zugreifen. Status des Lebenszyklus in der Integration von Datenrepositorien. Bereich des DatenspeicherTab für das Dateisystem. Der LifecycleDie Immobilie befindet sich in der DataRepositoryConfiguration Objekt in der Antwort eines [describe-file-systems](#) CLI-Befehl (die entsprechende API-Aktion ist [DescribeFileSystems](#)).

Automatisches Importieren von Updates aus Ihrem S3-Bucket

Wenn Sie ein neues Dateisystem erstellen, importiert Amazon FSx standardmäßig die Dateimetadaten (Name, Eigentum, Zeitstempel und Berechtigungen) von Objekten im verknüpften S3-Bucket bei der Erstellung des Dateisystems. Sie können Ihr FSx for Lustre-Dateisystem so konfigurieren, dass es automatisch Metadaten von Objekten importiert, die nach der Erstellung des Dateisystems zu Ihrem S3-Bucket hinzugefügt, geändert oder aus diesem gelöscht wurden. FSx for Lustre aktualisiert die Datei- und Verzeichnisliste eines geänderten Objekts nach der Erstellung auf die gleiche Weise, wie es Dateimetadaten bei der Erstellung des Dateisystems importiert. Wenn Amazon FSx die Datei- und Verzeichnisliste eines geänderten Objekts aktualisiert und das geänderte Objekt im S3-Bucket seine Metadaten nicht mehr enthält, behält Amazon FSx die aktuellen Metadatenwerte der Datei bei, anstatt Standardberechtigungen zu verwenden.

Note


Importeinstellungen sind auf FSx for Lustre-Dateisystemen verfügbar, die nach 15:00 Uhr EDT am 23. Juli 2020 erstellt wurden.

Sie können Importeinstellungen festlegen, wenn Sie ein neues Dateisystem erstellen, und Sie können die Einstellung auf vorhandenen Dateisystemen mithilfe der FSx-Verwaltungskonsole aktualisieren, der AWS CLI und die AWS API. (Optional) Wenn Sie Ihr Dateisystem erstellen, werden Ihre vorhandenen S3-Objekte als Datei- und Verzeichnislisten angezeigt. Wie möchten Sie Ihr Dateisystem aktualisieren, nachdem Sie es erstellt haben, wenn der Inhalt Ihres S3-Buckets aktualisiert wird? Ein Dateisystem kann eine der folgenden Importeinstellungen haben:

Note

Das FSx for Lustre-Dateisystem und sein verknüpfter S3-Bucket müssen sich im selben Bucket befinden. AWS Region, um Updates automatisch zu importieren.

- Aktualisiere meine Datei- und Verzeichnisliste, wenn Objekte zu meinem S3-Bucket hinzugefügt werden: (Standard) Amazon FSx aktualisiert automatisch die Datei- und Verzeichnislisten aller neuen Objekte, die dem verknüpften S3-Bucket hinzugefügt wurden und die derzeit nicht im FSx-Dateisystem vorhanden sind. Amazon FSx aktualisiert keine Angebote für Objekte, die sich im S3-Bucket geändert haben. Amazon FSx löscht keine Auflistungen von Objekten, die im S3-Bucket gelöscht wurden.

 Note

Die Standardeinstellung für die Importeinstellungen für den Import von Daten aus einem verknüpften S3-Bucket mithilfe der CLI und der API lautet NONE. Die Standardeinstellung für Importeinstellungen bei Verwendung der Konsole besteht darin, Lustre zu aktualisieren, wenn dem S3-Bucket neue Objekte hinzugefügt werden.

- Aktualisiere meine Datei- und Verzeichnisliste, wenn Objekte zu meinem S3-Bucket hinzugefügt oder geändert werden: Amazon FSx aktualisiert automatisch die Datei- und Verzeichnislisten aller neuen Objekte, die dem S3-Bucket hinzugefügt wurden, sowie aller vorhandenen Objekte, die im S3-Bucket geändert wurden, nachdem Sie diese Option ausgewählt haben. Amazon FSx löscht keine Auflistungen von Objekten, die im S3-Bucket gelöscht wurden.
- Aktualisiere meine Datei- und Verzeichnisliste, wenn Objekte zu meinem S3-Bucket hinzugefügt, geändert oder aus meinem S3-Bucket gelöscht werden: Amazon FSx aktualisiert automatisch die Datei- und Verzeichnislisten aller neuen Objekte, die dem S3-Bucket hinzugefügt wurden, aller vorhandenen Objekte, die im S3-Bucket geändert wurden, und aller vorhandenen Objekte, die im S3-Bucket gelöscht werden, nachdem Sie diese Option ausgewählt haben.
- Meine Datei nicht aktualisieren und nicht direkt auflisten, wenn Objekte zu meinem S3-Bucket hinzugefügt, geändert oder aus meinem S3-Bucket gelöscht werden- Amazon FSx aktualisiert Datei- und Verzeichnislisten aus dem verknüpften S3-Bucket nur, wenn das Dateisystem erstellt wird. FSx aktualisiert keine Datei- und Verzeichnislisten für neue, geänderte oder gelöschte Objekte, nachdem Sie diese Option ausgewählt haben.

Wenn Sie die Importeinstellungen so festlegen, dass Ihre Dateisystemdateien und Verzeichnislisten auf der Grundlage von Änderungen im verknüpften S3-Bucket aktualisiert werden, erstellt Amazon FSx eine Konfiguration für die Ereignisbenachrichtigung für den verknüpften S3-Bucket mit dem Namen FSx. Ändern oder löschen Sie das nichtFSxKonfiguration der Ereignisbenachrichtigung im S3-Bucket. Dadurch wird der automatische Import neuer oder geänderter Datei- und Verzeichnislisten in Ihr Dateisystem verhindert.

Wenn Amazon FSx eine Dateiliste aktualisiert, die sich im verknüpften S3-Bucket geändert hat, überschreibt es die lokale Datei mit der aktualisierten Version, auch wenn die Datei schreibgeschützt ist. Wenn Amazon FSx eine Dateiliste aktualisiert, wenn das entsprechende Objekt im verknüpften S3-Bucket gelöscht wurde, löscht es in ähnlicher Weise die lokale Datei, selbst wenn die Datei schreibgesperrt ist.

Amazon FSx bemüht sich nach besten Kräften, Ihr Dateisystem zu aktualisieren. Amazon FSx kann das Dateisystem in den folgenden Situationen nicht mit Änderungen aktualisieren:

- Wenn Amazon FSx nicht berechtigt ist, das geänderte oder neue S3-Objekt zu öffnen.
- Wenn die Konfiguration der Ereignisbenachrichtigung im verknüpften S3-Bucket wurde gelöscht oder geändert.

Jede dieser Bedingungen führt dazu, dass der Lebenszyklusstatus des Datenrepositorys falsch konfiguriert. Weitere Informationen finden Sie unter [Status des Lebenszyklus des Datenrepositorys](#).

Voraussetzungen

Die folgenden Bedingungen sind erforderlich, damit Amazon FSx automatisch neue, geänderte oder gelöschte Dateien aus dem verknüpften S3-Bucket importieren kann:

- Das Dateisystem und sein verknüpfter S3-Bucket müssen sich im selben Bucket befindenAWSRegion.
- Der S3-Bucket hat keinen falsch konfigurierten Lifecycle-Status. Weitere Informationen finden Sie unter [Status des Lebenszyklus des Datenrepositorys](#).
- Ihr Konto muss über die erforderlichen Berechtigungen verfügen, um Ereignisbenachrichtigungen im verknüpften S3-Bucket zu konfigurieren und zu empfangen.

Unterstützte Arten von Dateiänderungen

Amazon FSx unterstützt den Import der folgenden Änderungen an Dateien und Ordnern, die im verknüpften S3-Bucket vorgenommen werden:

- Änderungen am Dateiinhalt
- Änderungen an Datei- oder Ordnermetadaten
- Änderungen am Symlink-Ziel oder an den Metadaten

Aktualisierung der Importeinstellungen

Sie können die Importeinstellungen eines Dateisystems festlegen, wenn Sie ein neues Dateisystem erstellen. Weitere Informationen finden Sie unter [Ihr Dateisystem mit einem S3-Bucket verknüpfen](#).

Sie können die Importeinstellungen eines Dateisystems auch aktualisieren, nachdem es erstellt wurde, indem Sie den AWS Management Console, die AWS CLI und die Amazon FSx-API, wie im folgenden Verfahren gezeigt.

Console

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Dashboard Dateisysteme.
3. Wählen Sie das Dateisystem aus, das Sie verwalten möchten, um die Dateisystemdetails anzuzeigen.
4. Wählen Sie Datenspeicherum die Einstellungen des Datenrepositorys einzusehen. Sie können die Importeinstellungen ändern, wenn der Lebenszyklusstatus lautet VERFÜGBAR oder FALSCH KONFIGURIERT. Weitere Informationen finden Sie unter [Status des Lebenszyklus des Datenrepositorys](#).
5. Wählen Sie Aktionen, und wählen Sie dann Importeinstellungen aktualisieren um die anzuzeigen Importeinstellungen aktualisieren Dialogfenster.
6. Wählen Sie die neue Einstellung aus und wählen Sie dann Aktualisieren um die Änderung vorzunehmen.

CLI

Um die Importeinstellungen zu aktualisieren, verwenden Sie den [update-file-system](#) CLI-Befehl. Die entsprechende API-Operation ist [UpdateFileSystem](#).

Nachdem Sie das Dateisystem erfolgreich aktualisiert haben `AutoImportPolicy`, Amazon FSx gibt die Beschreibung des aktualisierten Dateisystems als JSON zurück, wie hier gezeigt:

```
{
  "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"
}
}
]
```

Leistung von Amazon FSx for Lustre

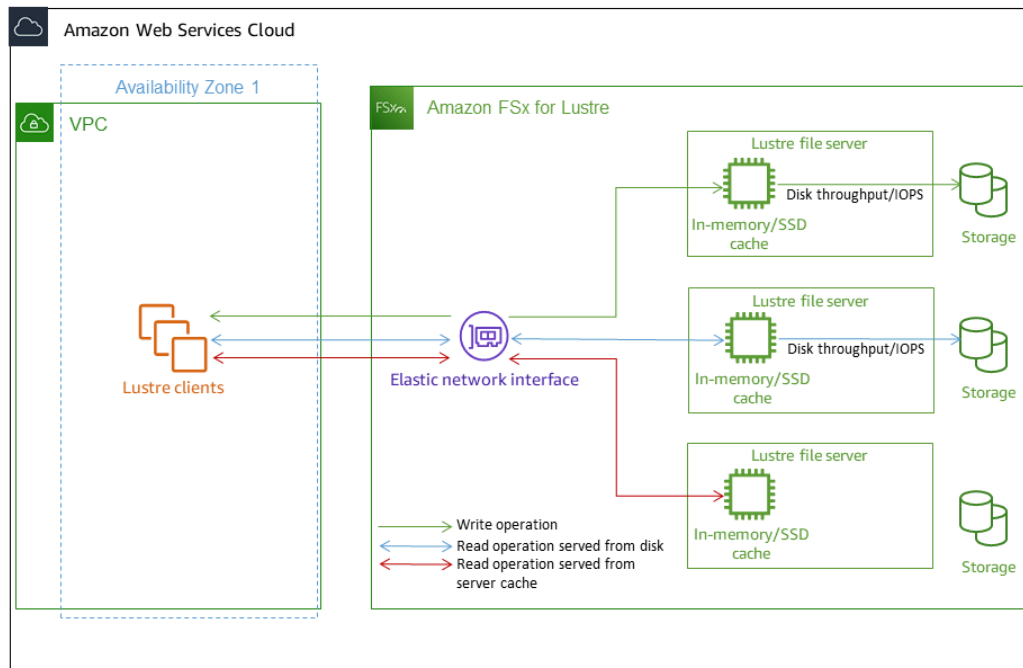
Amazon FSx for Lustre basiert auf Lustre, dem beliebten Hochleistungsdateisystem, und bietet Scale-Out-Leistung, die linear mit der Größe eines Dateisystems zunimmt. Lustre-Dateisysteme lassen sich horizontal auf mehrere Dateiserver und Festplatten skalieren. Diese Skalierung ermöglicht jedem Client direkten Zugriff auf die auf den einzelnen Festplatten gespeicherten Daten, wodurch viele der in herkömmlichen Dateisystemen vorhandenen Engpässe beseitigt werden. Amazon FSx for Lustre baut auf der skalierbaren Architektur von Lustre auf, um ein hohes Leistungsniveau bei einer großen Anzahl von Kunden zu unterstützen.

Themen

- [So funktionieren FSx for Lustre-Dateisysteme](#)
- [Aggregierte Dateisystemleistung](#)
- [Leistung der Metadaten des Dateisystems](#)
- [Speicherlayout des Dateisystems](#)
- [Daten in Ihrem Dateisystem entfernen](#)
- [Überwachung von Leistung und Nutzung](#)
- [Tipps zur Leistung](#)

So funktionieren FSx for Lustre-Dateisysteme

Jedes FSx for Lustre-Dateisystem besteht aus den Dateiservern, mit denen die Clients kommunizieren, und einem Satz von Festplatten, die an jeden Dateiserver angeschlossen sind und Ihre Daten speichern. Jeder Dateiserver verwendet einen schnellen In-Memory-Cache, um die Leistung für die am häufigsten aufgerufenen Daten zu verbessern. HDD-basierte Dateisysteme können auch mit einem SSD-basierten Lesecache ausgestattet werden, um die Leistung für die am häufigsten aufgerufenen Daten weiter zu verbessern. Wenn ein Client auf Daten zugreift, die im Arbeitsspeicher- oder SSD-Cache gespeichert sind, muss der Dateiserver sie nicht von der Festplatte lesen, was die Latenz reduziert und den Gesamtdurchsatz erhöht, den Sie steuern können. Das folgende Diagramm zeigt die Pfade eines Schreibvorgangs, eines Lesevorgangs, der von der Festplatte aus ausgeführt wird, und eines Lesevorgangs, der über den Arbeitsspeicher oder den SSD-Cache ausgeführt wird.



Wenn Sie Daten lesen, die im Arbeitsspeicher- oder SSD-Cache des Dateiservers gespeichert sind, wird die Leistung des Dateisystems durch den Netzwerkdurchsatz bestimmt. Wenn Sie Daten in Ihr Dateisystem schreiben oder wenn Sie Daten lesen, die nicht im In-Memory-Cache gespeichert sind, wird die Leistung des Dateisystems durch den jeweils niedrigeren Wert des Netzwerkdurchsatzes und des Festplattendurchsatzes bestimmt.

Wenn Sie ein HDD Lustre-Dateisystem mit einem SSD-Cache bereitstellen, erstellt Amazon FSx einen SSD-Cache, der automatisch auf 20 Prozent der Festplattenspeicherkapazität des Dateisystems skaliert wird. Dadurch werden Latenzen von unter einer Millisekunde und höhere IOPS für häufig aufgerufene Dateien erreicht.

Aggregierte Dateisystemleistung

Der Durchsatz, den ein FSx for Lustre-Dateisystem unterstützt, ist proportional zu seiner Speicherkapazität. Die Dateisysteme von Amazon FSx for Lustre lassen sich auf einen Durchsatz von Hunderten von Gbit/s und Millionen von IOPS skalieren. Amazon FSx for Lustre unterstützt auch den gleichzeitigen Zugriff auf dieselbe Datei oder dasselbe Verzeichnis von Tausenden von Recheninstanzen aus. Dieser Zugriff ermöglicht ein schnelles Prüfen von Daten vom Anwendungsspeicher zum Speicher, was eine gängige Technik im Hochleistungsrechnen (HPC)

ist. Sie können den Speicherplatz und die Durchsatzkapazität nach Bedarf jederzeit erhöhen, nachdem Sie das Dateisystem erstellt haben. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#).

FSx for Lustre-Dateisysteme bieten einen Burst-Lesedurchsatz mithilfe eines Netzwerk-I/O-Kreditmechanismus, um Netzwerkbandbreite auf der Grundlage der durchschnittlichen Bandbreitennutzung zuzuweisen. Die Dateisysteme sammeln Credits, wenn ihre Netzwerkbandbreitennutzung unter ihren Basisgrenzwerten liegt, und können diese Credits verwenden, wenn sie Netzwerkdatenübertragungen durchführen.

Die folgenden Tabellen zeigen die Leistung, für die die Bereitstellungsoptionen von FSx for Lustre konzipiert wurden.

Dateisystemleistung für SSD-Speicheroptionen

Art der Bereitstellung	Netzwerkdurchsatz (MB/s/TiB bereitgestellter Speicher)	Netzwerk-IOPS (IOPS/TiB des bereitgestellten Speichers)	Cache-Speicher (GiB RAM/TiB bereitgestellter Speicher)	Festplattenlatenz (ns pro Dateivorgang (Millisekunden, P50))	Festplattendurchsatz (Mbit/s/TiB bereitgestellter Speicher oder SSD-Cache)	
	Ausgangswert	Platzenwert			Grundlinie	Platzenwert
KRATZEN_2	200	1300	6.7	Metadaten: 200 Unter-MS (gelesen)	200	-
HARTNÄCKI G-125	320	1300	3.4	Daten: 100 Unter-MS (schreiben)	125	500
HARTNÄCKI G-250	640	1300	6.8		250	500
HARTNÄCKI G-500	1300	-	13,7		500	-
HARTNÄCKI G-1000	2600	-	27,3		1000	-

Dateisystemleistung für HDD-Speicheroptionen

Art der Bereitstellung	Netzwerkdurchsatz (MB/s/TiB bereitgestellter Speicher oder SSD-Cache)	Netzwerk-IOPS (IOPS/TiB des bereitgestellten Speichers)	Cache-Speicher (GiB RAM/TiB bereitgestellter Speicher)	Festplattenanzahl pro Dateivorgang (Millisekunden, P50)	Festplattendurchsatz (Mbit/s/TiB bereitgestellter Speicher oder SSD-Cache)	Ausgangswert	Platzen	Grundlinie	Platzen
HARTNÄCKIG-12									
HDD-Speicher	40	375*	0.4 Speicher	Metadaten: Sub-MS Daten: einstellige ms	12 80 (gelesen)				
SSD-Lese-ache	200	1.900	200 SSD-Cache	Daten: Sub-MS	-				
PERSISTENT-40									
HDD-Speicher	150	1.300*	1.5	Metadaten: Unter-MS Daten: einstellige ms	40 250 (gelesen)				
SSD-Lese-ache	750	6500	200 SSD-Cache	Daten: Sub-MS	-				

Leistung des Dateisystems für SSD-Speicheroptionen der vorherigen Generation

Art der Bereitstellung	Netzwerkdurchsatz (MB/s pro TiB bereitgestellten Speichers)	Netzwerk-IOPS (IOPS pro TiB bereitgestellten Speichers)	Cache-Speicher (GiB pro TiB bereitgestellten Speichers)	Festplattenanzahl pro Dateivorgang (Millisekunden, P50)	Festplattendurchsatz (MB/s pro TiB bereitgestellten Speicher oder SSD-Cache)	
	Ausgangswert	Platzen			Grundlinie	Platzen
HARTNÄCKI G-50	250	1.300*	2,2 RAM	Metadaten: Unter-MS	50	240
PERSISTENT T-100	500	1.300*	4,4 GRAMM	Daten: Unter-MS	100	240
PERSISTENT T-200	750	1.300*	8,8 GRAMM		200	240

Note

*Die folgenden persistenten Dateisysteme AWS-Regionen bieten Netzwerk-Bursts von bis zu 530 MB/s pro TiB Speicher: Afrika (Kapstadt), Asien-Pazifik (Hongkong), Asien-Pazifik (Osaka), Asien-Pazifik (Singapur), Kanada (Zentral), Europa (Frankfurt), Europa (London), Europa (Mailand), Europa (Stockholm), Naher Osten (Bahrain), Südamerika (São Paulo), China und USA West (Los Angeles).

Beispiel: Aggregierter Baseline- und Burst-Durchsatz

Das folgende Beispiel zeigt, wie sich Speicherkapazität und Festplattendurchsatz auf die Leistung des Dateisystems auswirken.

Ein persistentes Dateisystem mit einer Speicherkapazität von 4,8 TiB und 50 MB/s pro TiB Durchsatz pro Speichereinheit bietet einen aggregierten Basisdurchsatz von 240 MB/s und einen Burst-Festplattendurchsatz von 1,152 GB/s.

Unabhängig von der Größe des Dateisystems bietet Amazon FSx for Lustre konsistente Latenzen von unter einer Millisekunde für Dateioperationen.

Leistung der Metadaten des Dateisystems

I/O-Operationen pro Sekunde (IOPS) für Dateisystem-Metadaten bestimmen die Anzahl der Dateien und Verzeichnisse, die Sie pro Sekunde erstellen, auflisten, lesen und löschen können. Metadaten-IOPS werden automatisch auf FSx for Lustre-Dateisystemen bereitgestellt, basierend auf der von Ihnen bereitgestellten Speicherkapazität.

Persistent_2 Dateisysteme ermöglichen es Ihnen, Metadaten-IOPS unabhängig von der Speicherkapazität bereitzustellen und bieten einen besseren Einblick in die Anzahl und Art der Metadaten-IOPS-Client-Instances, die in Ihrem Dateisystem ausgeführt werden.

Bei FSx for Lustre Persistent_2 Dateisystemen bestimmen die Anzahl der von Ihnen bereitgestellten Metadaten-IOPS und die Art des Metadatenvorgangs die Rate der Metadatenoperationen, die Ihr Dateisystem unterstützen kann. Die Ebene der von Ihnen bereitgestellten Metadaten-IOPS bestimmt die Anzahl der IOPS, die für die Metadaten-Festplatten Ihres Dateisystems bereitgestellt werden.

Art des Vorgangs	Vorgänge, die Sie pro Sekunde für jede bereitgestellte Metadaten-IOPS ausführen können
Datei erstellen, öffnen	2
Datei löschen	1
Verzeichnis erstellen, umbenennen	0.1
Verzeichnis löschen	0.2

Sie können wählen, ob Sie Metadaten-IOPS im automatischen Modus oder im vom Benutzer bereitgestellten Modus bereitstellen möchten. Im automatischen Modus stellt Amazon FSx automatisch Metadaten-IOPS basierend auf der Speicherkapazität Ihres Dateisystems gemäß der folgenden Tabelle bereit:

Speicherkapazität des Dateisystems	Inklusive Metadaten-IOPS im automatischen Modus
1200 GiB	1500
2400 GiB	3000
4800—9600 GiB	6 000
12000—456,00 GiB	12000
≥48000 GiB	12000 IOPS pro 24000 GiB

Im vom Benutzer bereitgestellten Modus können Sie optional die Anzahl der bereitzustellenden Metadaten-IOPS angeben. Sie zahlen für bereitgestellte Metadaten-IOPS, die über der Standardanzahl an Metadaten-IOPS für Ihr Dateisystem liegen.

Speicherlayout des Dateisystems

Alle Dateidaten in Lustre werden auf Speichervolumen gespeichert, die als Object Storage Targets (OSTs) bezeichnet werden. Alle Dateimetadaten (einschließlich Dateinamen, Zeitstempel, Berechtigungen und mehr) werden auf Speichervolumen gespeichert, die als Metadatenziele (MDTs) bezeichnet werden. Amazon FSx for Lustre-Dateisysteme bestehen aus einem oder mehreren MDTs und mehreren OSTs. Jede OST-Datei hat eine Größe von etwa 1 bis 2 TiB, abhängig vom Bereitstellungstyp des Dateisystems. Amazon FSx for Lustre verteilt Ihre Dateidaten auf die OSTs, aus denen Ihr Dateisystem besteht, um die Speicherkapazität mit dem Durchsatz und der IOPS-Auslastung in Einklang zu bringen.

Um die Speichernutzung der MDT- und OSTs zu überprüfen, aus denen Ihr Dateisystem besteht, führen Sie den folgenden Befehl von einem Client aus, auf dem das Dateisystem gemountet ist.

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

Die Ausgabe dieses Befehls sieht wie folgt aus:

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

Daten in Ihrem Dateisystem entfernen

Mit File-Striping können Sie die Durchsatzleistung Ihres Dateisystems optimieren. Amazon FSx for Lustre verteilt Dateien automatisch auf alle OSTs, um sicherzustellen, dass Daten von allen Speicherservern bereitgestellt werden. Sie können dasselbe Konzept auf Dateiebene anwenden, indem Sie konfigurieren, wie Dateien auf mehrere OSTs verteilt werden.

Striping bedeutet, dass Dateien in mehrere Blöcke aufgeteilt werden können, die dann auf verschiedenen OSTs gespeichert werden. Wenn eine Datei über mehrere OSTs verteilt wird, werden Lese- oder Schreibanforderungen an die Datei auf diese OSTs verteilt, wodurch der Gesamtdurchsatz oder die IOPS, die Ihre Anwendungen verarbeiten können, erhöht wird.

Im Folgenden sind die Standardlayouts für Amazon FSx for Lustre-Dateisysteme aufgeführt.

- Für Dateisysteme, die vor dem 18. Dezember 2020 erstellt wurden, gibt das Standardlayout eine Stripe-Anzahl von 1 an. Das bedeutet, dass, sofern kein anderes Layout angegeben ist, jede in Amazon FSx for Lustre mit Standard-Linux-Tools erstellte Datei auf einer einzigen Festplatte gespeichert wird.
- Für Dateisysteme, die nach dem 18. Dezember 2020 erstellt wurden, ist das Standardlayout ein progressives Dateilayout, bei dem Dateien mit einer Größe von weniger als 1 GiB in einem Stripe gespeichert werden und größeren Dateien eine Stripe-Anzahl von 5 zugewiesen wird.
- Für Dateisysteme, die nach dem 25. August 2023 erstellt wurden, ist das Standardlayout ein progressives 4-Komponenten-Dateilayout, das unter erklärt wird. [Progressive Datei-Layouts](#)
- Für alle Dateisysteme, unabhängig von ihrem Erstellungsdatum, verwenden aus Amazon S3 importierte Dateien nicht das Standardlayout, sondern das Layout im ImportedFileChunkSize Dateisystemparameter. S3-importierte Dateien, die größer als die sind, ImportedFileChunkSize werden auf mehreren OSTs mit einer Stripe-Anzahl von gespeichert. $(\text{FileSize} / \text{ImportedFileChunksize}) + 1$ Der Standardwert von ImportedFileChunkSize ist 1 GiB.

Sie können die Layoutkonfiguration einer Datei oder eines Verzeichnisses mit dem `lfs getstripe` Befehl anzeigen.

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

Dieser Befehl meldet die Anzahl der Stripes, die Stripe-Größe und den Stripe-Offset einer Datei. Die Streifenanzahl gibt an, über wie viele OSTs die Datei gestreift ist. Die Stripe-Größe gibt an, wie viele kontinuierliche Daten auf einem OST gespeichert sind. Der Stripe-Offset ist der Index der ersten OST-Datei, über die die Datei gestreift wird.

Ändern Sie Ihre Striping-Konfiguration

Die Layoutparameter einer Datei werden festgelegt, wenn die Datei zum ersten Mal erstellt wird. Verwenden Sie den `lfs setstripe` Befehl, um eine neue, leere Datei mit einem bestimmten Layout zu erstellen.

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

Der `lfs setstripe` Befehl wirkt sich nur auf das Layout einer neuen Datei aus. Verwenden Sie ihn, um das Layout einer Datei festzulegen, bevor Sie sie erstellen. Sie können auch ein Layout für ein Verzeichnis definieren. Sobald es für ein Verzeichnis festgelegt ist, wird dieses Layout auf jede neue Datei angewendet, die diesem Verzeichnis hinzugefügt wird, jedoch nicht auf vorhandene Dateien. Jedes neue Unterverzeichnis, das Sie erstellen, erbt auch das neue Layout, das dann auf alle neuen Dateien oder Verzeichnisse angewendet wird, die Sie in diesem Unterverzeichnis erstellen.

Verwenden Sie den Befehl, um das Layout einer vorhandenen Datei zu ändern. `lfs migrate` Mit diesem Befehl wird die Datei nach Bedarf kopiert, um ihren Inhalt entsprechend dem Layout zu verteilen, das Sie im Befehl angeben. Beispielsweise ändern Dateien, die angehängt oder vergrößert werden, die Anzahl der Stripes nicht. Sie müssen sie also migrieren, um das Dateilayout zu ändern. Sie können auch eine neue Datei erstellen, indem Sie mit dem `lfs setstripe` Befehl ihr Layout angeben, den Originalinhalt in die neue Datei kopieren und dann die neue Datei umbenennen, um die Originaldatei zu ersetzen.

Es kann Fälle geben, in denen die Standard-Layoutkonfiguration nicht optimal für Ihre Arbeitslast ist. Beispielsweise kann in einem Dateisystem mit Dutzenden von OSTs und einer großen Anzahl von Dateien mit mehreren Gigabyte eine höhere Leistung erzielt werden, wenn die Dateien über mehr als den Standardwert für die Stripe-Anzahl von fünf OSTs verteilt werden. Das Erstellen großer Dateien mit einer niedrigen Stripe-Anzahl kann zu Engpässen bei der I/O-Leistung führen und auch dazu führen, dass OSTs voll werden. In diesem Fall können Sie ein Verzeichnis mit einer größeren Stripe-Anzahl für diese Dateien erstellen.

Die Einrichtung eines Streifenlayouts für große Dateien (insbesondere Dateien mit einer Größe von mehr als einem Gigabyte) ist aus folgenden Gründen wichtig:

- Verbessert den Durchsatz, indem mehrere OSTs und die zugehörigen Server beim Lesen und Schreiben großer Dateien IOPS, Netzwerkbandbreite und CPU-Ressourcen bereitstellen können.
- Reduziert die Wahrscheinlichkeit, dass ein kleiner Teil der OSTs zu Hotspots wird, die die Gesamtleistung der Arbeitslast einschränken.
- Verhindert, dass eine einzelne große Datei eine OST-Datei füllt, was möglicherweise zu Fehlern bei voller Festplatte führen kann.

Es gibt keine einzige optimale Layoutkonfiguration für alle Anwendungsfälle. Eine ausführliche Anleitung zu Datei-Layouts finden Sie unter [Managing File Layout \(Striping\) and Free Space](#) in der Lustre.org-Dokumentation. Im Folgenden finden Sie allgemeine Richtlinien:

- Das gestreifte Layout ist am wichtigsten für große Dateien, insbesondere für Anwendungsfälle, in denen Dateien routinemäßig Hunderte von Megabyte oder mehr groß sind. Aus diesem Grund weist das Standardlayout für ein neues Dateisystem Dateien mit einer Größe von mehr als 1 GiB eine Streifenanzahl von fünf zu.
- Die Anzahl der Stripes ist der Layoutparameter, den Sie für Systeme, die große Dateien unterstützen, anpassen sollten. Die Anzahl der Stripes gibt die Anzahl der OST-Volumes an, auf denen Teile einer Stripe-Datei gespeichert werden. Bei einer Stripe-Anzahl von 2 und einer Stripe-Größe von 1 MiB schreibt Lustre beispielsweise abwechselnd 1-MB-Chunks einer Datei in jedes von zwei OSTs.
- Die effektive Stripe-Anzahl ist der kleinere Wert aus der tatsächlichen Anzahl von OST-Volumes und dem von Ihnen angegebenen Wert für die Stripe-Anzahl. Sie können den speziellen Wert für die Stripe-Anzahl von verwenden, -1 um anzugeben, dass Stripes auf allen OST-Volumes platziert werden sollen.
- Die Einstellung einer großen Stripe-Anzahl für kleine Dateien ist nicht optimal, da Lustre für bestimmte Operationen einen Netzwerk-Roundtrip zu jedem OST-Objekt im Layout erfordert, auch wenn die Datei zu klein ist, um Speicherplatz auf allen OST-Volumes zu belegen.
- Sie können ein progressives Datei-Layout (PFL) einrichten, bei dem sich das Layout einer Datei mit der Größe ändern kann. Eine PFL-Konfiguration kann die Verwaltung eines Dateisystems mit einer Kombination aus großen und kleinen Dateien vereinfachen, ohne dass Sie für jede Datei explizit eine Konfiguration festlegen müssen. Weitere Informationen finden Sie unter [Progressive Datei-Layouts](#).
- Die Stripe-Größe beträgt standardmäßig 1 MiB. Das Einstellen eines Stripe-Offsets kann unter bestimmten Umständen nützlich sein, aber im Allgemeinen ist es am besten, ihn nicht anzugeben und die Standardeinstellung zu verwenden.

Progressive Datei-Layouts

Sie können eine PFL-Konfiguration (Progressive File Layout) für ein Verzeichnis angeben, um vor dem Auffüllen verschiedene Stripe-Konfigurationen für kleine und große Dateien festzulegen. Sie können beispielsweise eine PFL für das Verzeichnis der obersten Ebene festlegen, bevor Daten in ein neues Dateisystem geschrieben werden.

Um eine PFL-Konfiguration anzugeben, verwenden Sie den `lfs setstripe` Befehl mit `-E` Optionen, um Layoutkomponenten für Dateien unterschiedlicher Größe anzugeben, z. B. den folgenden Befehl:


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

Mit diesem Befehl werden vier Layoutkomponenten festgelegt:

- Die erste Komponente (-E 100M -c 1) gibt einen Wert für die Anzahl der Stripes von 1 für Dateien mit einer Größe von bis zu 100 MiB an.
- Die zweite Komponente (-E 10G -c 8) gibt eine Stripe-Anzahl von 8 für Dateien mit einer Größe von bis zu 10 GiB an.
- Die dritte Komponente (-E 100G -c 16) gibt eine Stripe-Anzahl von 16 für Dateien mit einer Größe von bis zu 100 GiB an.
- Die vierte Komponente (-E -1 -c 32) gibt eine Stripe-Anzahl von 32 für Dateien mit mehr als 100 GiB an.

Important

Durch das Anhängen von Daten an eine Datei, die mit einem PFL-Layout erstellt wurde, werden alle Layoutkomponenten aufgefüllt. Wenn Sie beispielsweise mit dem oben gezeigten 4-Komponenten-Befehl eine 1 MiB-Datei erstellen und dann Daten am Ende der Datei hinzufügen, wird das Layout der Datei auf eine Stripe-Anzahl von -1 erweitert, was alle OSTs im System bedeutet. Das bedeutet nicht, dass Daten in jedes OST geschrieben werden, aber ein Vorgang wie das Lesen der Dateilänge sendet parallel zu jedem OST eine Anfrage, was das Dateisystem erheblich belastet.

Achten Sie daher darauf, die Anzahl der Stripes für Dateien mit kleiner oder mittlerer Länge zu begrenzen, an die anschließend Daten angehängt werden können. Da Protokolldateien normalerweise wachsen, wenn neue Datensätze angehängt werden, weist Amazon FSx for Lustre jeder im Anfügemodus erstellten Datei eine Standard-Stripe-Anzahl von 1 zu, unabhängig von der im übergeordneten Verzeichnis angegebenen Standard-Stripe-Konfiguration.

Die Standard-PFL-Konfiguration auf Amazon FSx for Lustre-Dateisystemen, die nach dem 25. August 2023 erstellt wurden, wird mit diesem Befehl festgelegt:

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

Kunden mit Workloads, die in hohem Maße gleichzeitig auf mittlere und große Dateien zugreifen, profitieren wahrscheinlich von einem Layout mit mehr Stripes bei kleineren Größen und Striping über alle OSTs für die größten Dateien, wie im Beispiel-Layout mit vier Komponenten dargestellt.

Überwachung von Leistung und Nutzung

Jede Minute sendet Amazon FSx for Lustre Nutzungsmetriken für jede Festplatte (MDT und OST) an Amazon. CloudWatch

Um aggregierte Details zur Dateisystemnutzung anzuzeigen, können Sie sich die Summenstatistik jeder Metrik ansehen. Die Summe der `DataReadBytes` Statistik gibt beispielsweise den gesamten Lesedurchsatz an, der von allen OSTs in einem Dateisystem gemessen wurde. In ähnlicher Weise gibt die Summe der `FreeDataStorageCapacity` Statistik die gesamte verfügbare Speicherkapazität für Dateidaten im Dateisystem an.

Weitere Informationen zur Überwachung der Leistung Ihres Dateisystems finden Sie unter [Überwachung von Amazon FSx for Lustre](#).

Tipps zur Leistung

Beachten Sie bei der Verwendung von Amazon FSx for Lustre die folgenden Leistungstipps. Informationen zu Servicebeschränkungen finden Sie unter [Kontingente](#)

- **Durchschnittliche I/O-Größe** — Da es sich bei Amazon FSx for Lustre um ein Netzwerk-Dateisystem handelt, durchläuft jeder Dateivorgang einen Roundtrip zwischen dem Client und Amazon FSx for Lustre, wodurch ein geringer Latenz-Overhead entsteht. Aufgrund dieser vorgangsbasierten Latenz wird der Gesamtdurchsatz im Allgemeinen erhöht, wenn die durchschnittliche E/A-Größe steigt, da der Overhead über eine größere Menge von Daten amortisiert wird.
- **Anforderungsmodell** — Durch die Aktivierung asynchroner Schreibvorgänge in Ihr Dateisystem werden ausstehende Schreibvorgänge auf der Amazon EC2 EC2-Instance zwischengespeichert, bevor sie asynchron in Amazon FSx for Lustre geschrieben werden. Asynchrone Schreibvorgänge besitzen in der Regel niedrigere Latenzen. Bei der Ausführung asynchroner Schreibvorgänge verwendet der Kernel zusätzlichen Speicher zum Zwischenspeichern. Ein Dateisystem, das synchrone Schreibvorgänge aktiviert hat, sendet synchrone Anfragen an Amazon FSx for Lustre. Jeder Vorgang durchläuft einen Hin- und Rückweg zwischen dem Kunden und Amazon FSx for Lustre.

Note

Ihr Anforderungsmodell geht hinsichtlich Konsistenz (wenn Sie mehrere Amazon-EC2-Instances verwenden) und Geschwindigkeit Kompromisse ein.

- **Verzeichnisgröße begrenzen** — Um eine optimale Metadaten-Performance auf Persistent_2 FSx for Lustre-Dateisystemen zu erreichen, beschränken Sie jedes Verzeichnis auf weniger als 100.000 Dateien. Durch die Begrenzung der Anzahl der Dateien in einem Verzeichnis wird die Zeit reduziert, die das Dateisystem benötigt, um eine Sperre für das übergeordnete Verzeichnis zu erlangen.
- **Amazon EC2 EC2-Instances** — Anwendungen, die eine große Anzahl von Lese- und Schreibvorgängen ausführen, benötigen wahrscheinlich mehr Speicher oder Rechenkapazität als Anwendungen, die dies nicht tun. Wenn Sie Ihre Amazon EC2 EC2-Instances für Ihre rechenintensive Arbeitslast starten, wählen Sie Instance-Typen aus, die über die Menge dieser Ressourcen verfügen, die Ihre Anwendung benötigt. Die Leistungsmerkmale von Amazon FSx for Lustre-Dateisystemen hängen nicht von der Verwendung von Amazon EBS-optimierten Instances ab.
- **Empfohlenes Tuning von Client-Instances für optimale Leistung**

1. Für alle Client-Instance-Typen und -Größen empfehlen wir die folgende Optimierung:

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

2. Für Client-Instance-Typen mit einem Arbeitsspeicher von mehr als 64 GiB empfehlen wir die folgende Optimierung:

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

3. Für Client-Instance-Typen mit mehr als 64 vCPU-Kernen empfehlen wir die folgende Optimierung:

```
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
```

Nach dem Mounten des Clients muss die folgende Optimierung vorgenommen werden:

```
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
```

Beachten Sie, dass `lctl set_param` dies bekanntermaßen nach einem Neustart nicht bestehen bleibt. Da diese Parameter von der Clientseite aus nicht dauerhaft gesetzt werden können, wird empfohlen, einen Boot-Cron-Job zu implementieren, um die Konfiguration mit den empfohlenen Einstellungen festzulegen.

- Workload-Balance zwischen allen OSTs — In einigen Fällen bestimmt Ihre Arbeitslast nicht den Gesamtdurchsatz, den Ihr Dateisystem bereitstellen kann (200 MB/s pro TiB Speicher). Wenn ja, können Sie CloudWatch Metriken verwenden, um Fehler zu beheben, falls die Leistung durch ein Ungleichgewicht in den I/O-Mustern Ihres Workloads beeinträchtigt wird. Um herauszufinden, ob dies die Ursache ist, schauen Sie sich die CloudWatch Maximum-Metrik für Amazon FSx for Lustre an.

In einigen Fällen zeigt diese Statistik eine Last bei oder über 240 MBps Durchsatz (die Durchsatzkapazität einer einzelnen Amazon FSx for Lustre-Festplatte mit 1,2 TiB). In solchen Fällen ist Ihre Arbeitslast nicht gleichmäßig auf Ihre Festplatten verteilt. In diesem Fall können Sie den `lfs setstripe` Befehl verwenden, um das Striping der Dateien zu ändern, auf die Ihr Workload am häufigsten zugreift. Um eine optimale Leistung zu erzielen, sollten Sie Dateien mit hohen Durchsatzanforderungen auf alle OSTs verteilen, aus denen Ihr Dateisystem besteht.

Wenn Ihre Dateien aus einem Datenrepository importiert werden, können Sie einen anderen Ansatz wählen, um Ihre Dateien mit hohem Durchsatz gleichmäßig auf Ihre OSTs zu verteilen. Zu diesem Zweck können Sie den `ImportedFileChunkSize` Parameter ändern, wenn Sie Ihr nächstes Amazon FSx for Lustre-Dateisystem erstellen.

Nehmen wir zum Beispiel an, dass Ihr Workload ein 7,0-TiB-Dateisystem verwendet (das aus 6 x 1,17-TiB-OSTs besteht) und einen hohen Durchsatz für 2,4-GiB-Dateien erzielen muss. In diesem Fall können Sie den `ImportedFileChunkSize` Wert auf festlegen, $(2.4 \text{ GiB} / 6 \text{ OSTs}) = 400 \text{ MiB}$ sodass Ihre Dateien gleichmäßig auf die OSTs Ihres Dateisystems verteilt werden.

- Lustre-Client für Metadaten-IOPS — Wenn für Ihr Dateisystem eine Metadatenkonfiguration angegeben ist, empfehlen wir Ihnen, einen Lustre 2.15-Client oder einen Lustre 2.12-Client mit einer der folgenden Betriebssystemversionen zu installieren: Amazon Linux 2023, Amazon Linux 2, Red Hat/CentOS/Rocky Linux 8.9 oder 9.x, Ubuntu 22 mit 6.2-Kernel oder Ubuntu 20.

Zugreifen auf Dateisysteme

Mit Amazon FSx können Sie Ihre rechenintensiven Workloads von lokalen Standorten in die Amazon Web Services Cloud übertragen, indem Sie Daten über oder VPN importieren. AWS Direct Connect Sie können lokal auf Ihr Amazon FSx-Dateisystem zugreifen, Daten nach Bedarf in Ihr Dateisystem kopieren und rechenintensive Workloads auf In-Cloud-Instances ausführen.

Im folgenden Abschnitt erfahren Sie, wie Sie auf einer Linux-Instance auf Ihr Amazon FSx for Lustre-Dateisystem zugreifen. Dazu erfahren Sie, wie Sie mit der `dateifs` tab Ihr Dateisystem nach Systemneustarts automatisch erneut mounten.

Bevor Sie ein Dateisystem mounten können, müssen Sie Ihre zugehörigen AWS -Ressourcen erstellen, konfigurieren und starten. Detaillierte Anweisungen finden Sie unter [Erste Schritte mit Amazon FSx for Lustre](#). Als Nächstes können Sie den Lustre-Client auf Ihrer Compute-Instance installieren und konfigurieren.

Themen

- [Kompatibilität des Lustre-Dateisystems und des Client-Kernels](#)
- [Den Lustre-Client installieren](#)
- [Mounten von einer Amazon Elastic Compute Cloud-Instance](#)
- [Montage über Amazon Elastic Container Service](#)
- [Mounten von Amazon FSx-Dateisystemen vor Ort oder über eine Peering-Amazon VPC](#)
- [Automatisches Mounten Ihres Amazon FSx-Dateisystems](#)
- [Mounten bestimmter Dateisätze](#)
- [Aufheben des Mountings von Dateisystemen](#)
- [Arbeiten mit Amazon EC2-Spot-Instances](#)

Kompatibilität des Lustre-Dateisystems und des Client-Kernels

Wir empfehlen dringend, die Lustre-Version für Ihr FSx for Lustre-Dateisystem zu verwenden, die mit den Linux-Kernelversionen Ihrer Client-Instances kompatibel ist.

Amazon Linux-Kunden

Betriebssystem	Betriebssystemversion	Minimale Kernelversion	Maximale Kernelversion	Version des Dateisystems		
				2.10	2,12	2,15
Amazon Linux 2023	6.1	6.1.79-99,167	6,179-99,167+	Nein	Ja	Ja
Amazon Linux 2	5,10	5.10.144-127,601	5.10.144-127,601+	Ja	Ja	Ja
			<5.10.144-127,601	Ja	Ja	Nein
	5.4	5,4.214-120,368	5,4.214-120,368+	Ja	Ja	Ja
			<5,4,214-120,368	Ja	Ja	Nein
	4,14	4,14.294-220,533	4,14.294-220,533+	Ja	Ja	Ja
			<4,14,294-220,533	Ja	Ja	Nein

Ubuntu-Clients

Betriebssystem	Betriebssystemversion	Minimale Kernelversion	Maximale Kernelversion	Version des Dateisystems		
				2.10	2,12	2,15
				2.10	2,12	2,15

Betriebssystem	Betriebssystemversion	Minimale Kernelversion	Maximale Kernelversion	Version des Dateisystems		
				2.10	2,12	2,15
Ubuntu	22	6.2.0-101 7.17~22,0 4	6.2.0. *	Nein	Ja	Ja
		5.15.0-10 15-aws	5.15.0-10 31-aws	Ja	Ja	Ja
	20	5.15.0-10 15-aws	5,15,0 +	Ja	Ja	Ja
		5.4.0-101 1-aws	5.13.0-10 31-aws	Ja	Ja	Nein

RHEL/CentOS/Rocky Linux-Clients

Betriebssystem	Betriebssystemversion	Architektur	Minimale Kernelversion	Maximale Kernelversion	Version des Dateisystems		
					2.10	2,12	2,15
RHEL/ Cent OS/ Rocky Linux	9.4	Arm + x86	5,14,0-42 7,13,1	5,14,0-42 7,16,1	Nein	Ja	Ja
			5,14,0-36 2,18,1	5,14,0-36 2,18,1	Nein	Ja	Ja
	9.3	Arm + x86	5,14,0-70 ,13,1	5,14,0-70 ,30,1	Nein	Ja	Ja
	9.0	Arm + x86			Nein	Ja	Ja

Betriebssystem	Betriebssystemversion	Architektur	Minimale Kernelversion	Maximale Kernelversion	Version des Dateisystems		
	8,9	Arm + x86	4,18,0-513*	4,18,0-513*	Ja	Ja	Ja
	8,8	Arm + x86	4,18,0-477*	4,18,0-477*	Ja	Ja	Ja
	8,7	Arm + x86	4,18,0-425*	4,18,0-425*	Ja	Ja	Ja
	8,6	Arm + x86	4,18,0-372*	4,18,0-372*	Ja	Ja	Ja
	8,5	Arm + x86	4,18,0-348*	4,18,0-348*	Ja	Ja	Ja
	8,4	Arm + x86	4,18,0-305*	4,18,0-305*	Ja	Ja	Ja
RHEL/ CentOS	8,3	Arm + x86	4,18,0-240*	4,18,0-240*	Ja	Ja	Nein
	8,2	Arm + x86	4,18,0-193*	4,18,0-193*	Ja	Ja	Nein
	7,9	86 x	3.10.0-1160*	3.10.0-1160*	Ja	Ja	Ja
	7,8	86 x	3.10.0-1127*	3.10.0-1127*	Ja	Ja	Nein
	7,7	86 x	3.10.0-1062*	3.10.0-1062*	Ja	Ja	Nein
CentOS	7,9	Arm	4,18,0-193*	4,18,0-193*	Ja	Ja	Ja

Betriebssystem	Betriebssystemversion	Architektur	Minimale Kernelversion	Maximale Kernelversion	Version des Dateisystems		
	7.8	Arm	4,18,0-14 7*	4,18,0-14 7*	Ja	Ja	Ja

Den Lustre-Client installieren

Um Ihr Amazon FSx for Lustre-Dateisystem von einer Linux-Instance aus zu mounten, installieren Sie zunächst den Open-Source-Lustre-Client. Wenden Sie dann, abhängig von Ihrer Betriebssystemversion, eines der folgenden Verfahren an. Informationen zur Kernel-Unterstützung finden Sie unter [Kompatibilität des Lustre-Dateisystems und des Client-Kernels](#).

Wenn auf Ihrer Recheninstanz nicht der in den Installationsanweisungen angegebene Linux-Kernel ausgeführt wird und Sie den Kernel nicht ändern können, können Sie Ihren eigenen Lustre-Client erstellen. Weitere Informationen finden Sie unter [Lustre kompilieren im Lustre-Wiki](#).

Amazon Linux

So installieren Sie den Lustre-Client auf Amazon Linux 2023

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Ermitteln Sie, welcher Kernel derzeit auf Ihrer Compute-Instance läuft, indem Sie den folgenden Befehl ausführen.

```
uname -r
```

3. Überprüfen Sie die Systemantwort und vergleichen Sie sie mit den folgenden Kernel-Mindestanforderungen für die Installation des Lustre-Clients auf Amazon Linux 2023:
 - 6.1 Kernel-Mindestanforderung — 6.1.79-99.167.amzn2023

Wenn Ihre EC2-Instance die Kernel-Mindestanforderungen erfüllt, fahren Sie mit dem Schritt fort und installieren Sie den Lustre-Client.

Wenn der Befehl ein Ergebnis zurückgibt, das unter den Kernel-Mindestanforderungen liegt, aktualisieren Sie den Kernel und starten Sie Ihre Amazon EC2 EC2-Instance neu, indem Sie den folgenden Befehl ausführen.

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

Bestätigen Sie mit dem `uname -r` Befehl, dass der Kernel aktualisiert wurde.

4. Laden Sie den Lustre-Client mit dem folgenden Befehl herunter und installieren Sie ihn.

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

So installieren Sie den Lustre-Client auf Amazon Linux 2

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Ermitteln Sie, welcher Kernel derzeit auf Ihrer Compute-Instance läuft, indem Sie den folgenden Befehl ausführen.

```
uname -r
```

3. Überprüfen Sie die Systemantwort und vergleichen Sie sie mit den folgenden Kernel-Mindestanforderungen für die Installation des Lustre-Clients auf Amazon Linux 2:
 - 5.10-Kernel-Mindestanforderung — 5.10.144-127.601.amzn2
 - 5.4 Kernel-Mindestanforderung — 5.4.214-120.368.amzn2
 - 4.14 Kernel-Mindestvoraussetzung — 4.14.294-220.533.amzn2

Wenn Ihre EC2-Instance die Kernel-Mindestanforderungen erfüllt, fahren Sie mit dem Schritt fort und installieren Sie den Lustre-Client.

Wenn der Befehl ein Ergebnis zurückgibt, das unter den Kernel-Mindestanforderungen liegt, aktualisieren Sie den Kernel und starten Sie Ihre Amazon EC2 EC2-Instance neu, indem Sie den folgenden Befehl ausführen.

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

Bestätigen Sie mit dem `uname -r` Befehl, dass der Kernel aktualisiert wurde.

4. Laden Sie den Lustre-Client mit dem folgenden Befehl herunter und installieren Sie ihn.

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

Wenn Sie den Kernel nicht auf die Kernel-Mindestvoraussetzungen aktualisieren können, können Sie den Legacy-2.10-Client mit dem folgenden Befehl installieren.

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

So installieren Sie den Lustre-Client auf Amazon Linux

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Ermitteln Sie, welcher Kernel derzeit auf Ihrer Compute-Instance läuft, indem Sie den folgenden Befehl ausführen. Der Lustre-Client benötigt einen Amazon Linux-Kernel 4.14, version 104 oder höher.

```
uname -r
```

3. Führen Sie eine der folgenden Aktionen aus:

- Wenn der Befehl `4.14.104-78.84.amzn1.x86_64` oder eine höhere Version von 4.14 zurückgegeben wird, laden Sie den Lustre-Client mit dem folgenden Befehl herunter und installieren Sie ihn.

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

- Wenn der Befehl ein niedrigeres Ergebnis als `zurückgibt4.14.104-78.84.amzn1.x86_64`, aktualisieren Sie den Kernel und starten Sie Ihre Amazon EC2 EC2-Instance neu, indem Sie den folgenden Befehl ausführen.

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

Bestätigen Sie mit dem `uname -r` Befehl, dass der Kernel aktualisiert wurde. Laden Sie dann den Lustre-Client herunter und installieren Sie ihn wie zuvor beschrieben.

CentOS, Rocky Linux und Red Hat

Um den Lustre-Client auf CentOS, Red Hat und Rocky Linux 9.0, 9.3 oder 9.4 zu installieren

Sie können Lustre-Client-Pakete, die mit Red Hat Enterprise Linux (RHEL), Rocky Linux und CentOS kompatibel sind, aus dem Amazon FSx Lustre Client Yum Package Repository installieren und aktualisieren. Diese Pakete sind signiert, um sicherzustellen, dass sie vor oder während des Downloads nicht manipuliert wurden. Die Repository-Installation schlägt fehl, wenn Sie den entsprechenden öffentlichen Schlüssel nicht auf Ihrem System installieren.

So fügen Sie das Yum-Paket-Repository des Amazon FSx Lustre-Clients hinzu

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Installieren Sie den öffentlichen Schlüssel Amazon FSx rpm mithilfe des folgenden Befehls.

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

3. Importieren Sie den Schlüssel mithilfe des folgenden Befehls.

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

4. Fügen Sie das Repository hinzu und aktualisieren Sie den Paketmanager mit dem folgenden Befehl.

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

So konfigurieren Sie das Yum-Repository des Amazon FSx Lustre-Clients

Das Yum-Paket-Repository des Amazon FSx Lustre-Clients ist standardmäßig so konfiguriert, dass der Lustre-Client installiert wird, der mit der Kernel-Version kompatibel ist, die ursprünglich mit der neuesten unterstützten CentOS-, Rocky Linux- und RHEL 9-Version ausgeliefert wurde. Um einen Lustre-Client zu installieren, der mit der von Ihnen verwendeten Kernelversion kompatibel ist, können Sie die Repository-Konfigurationsdatei bearbeiten.

In diesem Abschnitt wird beschrieben, wie Sie feststellen können, welchen Kernel Sie verwenden, ob Sie die Repository-Konfiguration bearbeiten müssen und wie Sie die Konfigurationsdatei bearbeiten.

1. Ermitteln Sie mithilfe des folgenden Befehls, welcher Kernel derzeit auf Ihrer Compute-Instance läuft.

```
uname -r
```

2. Führen Sie eine der folgenden Aktionen aus:
 - Wenn der Befehl zurückkehrt `5.14.0-427*`, müssen Sie die Repository-Konfiguration nicht ändern. Fahren Sie mit dem Verfahren So installieren Sie den Lustre-Client fort.
 - Wenn der Befehl zurückkehrt `5.14.0-362.18.1`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS-, Rocky Linux- und RHEL 9.3-Versionen verweist.
 - Wenn der Befehl zurückkehrt `5.14.0-70*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS-, Rocky Linux- und RHEL 9.0-Versionen verweist.
3. Bearbeiten Sie die Repository-Konfigurationsdatei mit dem folgenden Befehl so, dass sie auf eine bestimmte Version von RHEL verweist. `specific_RHEL_version` Ersetzen Sie es durch die RHEL-Version, die Sie verwenden müssen.

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

Um beispielsweise auf Version 9.3 zu verweisen, `specific_RHEL_version` ersetzen 9.3 Sie den Befehl durch, wie im folgenden Beispiel.

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

4. Verwenden Sie den folgenden Befehl, um den Yum-Cache zu löschen.

```
sudo yum clean all
```

Um den Lustre-Client zu installieren

- Installieren Sie die Pakete aus dem Repository mit dem folgenden Befehl.

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

Zusätzliche Informationen (CentOS, Rocky Linux und Red Hat 9.0 und neuer)

Mit den obigen Befehlen werden die beiden Pakete installiert, die für das Mounten und die Interaktion mit Ihrem Amazon FSx-Dateisystem erforderlich sind. Das Repository enthält zusätzliche Lustre-Pakete, wie z. B. ein Paket, das den Quellcode enthält, und Pakete, die Tests enthalten, und Sie können sie optional installieren. Verwenden Sie den folgenden Befehl, um alle verfügbaren Pakete im Repository aufzulisten.

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

Verwenden Sie den folgenden Befehl, um das Quell-RPM herunterzuladen, das einen Tarball mit dem Upstream-Quellcode und den Patches enthält, die wir installiert haben.

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

Wenn Sie `yum update` ausführen, wird eine neuere Version des Moduls installiert, sofern verfügbar, und die bestehende Version wird ersetzt. Um zu verhindern, dass die aktuell installierte Version beim Update entfernt wird, fügen Sie Ihrer `/etc/yum.conf` Datei eine Zeile wie die folgende hinzu.

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

Diese Liste enthält die in der `yum.conf` Manpage angegebenen Standardpakete, die nur für die Installation bestimmt sind, und das `kmod-lustre-client` Paket.

Um den Lustre-Client auf CentOS und Red Hat 8.2—8.9 oder auf Rocky Linux 8.4—8.9 zu installieren

Sie können Lustre-Client-Pakete, die mit Red Hat Enterprise Linux (RHEL), Rocky Linux und CentOS kompatibel sind, aus dem Amazon FSx Lustre Client Yum Package Repository installieren und aktualisieren. Diese Pakete sind signiert, um sicherzustellen, dass sie vor oder während des Downloads nicht manipuliert wurden. Die Repository-Installation schlägt fehl, wenn Sie den entsprechenden öffentlichen Schlüssel nicht auf Ihrem System installieren.

So fügen Sie das Yum-Paket-Repository des Amazon FSx Lustre-Clients hinzu

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Installieren Sie den öffentlichen Schlüssel Amazon FSx rpm mithilfe des folgenden Befehls.

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

3. Importieren Sie den Schlüssel mithilfe des folgenden Befehls.

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

4. Fügen Sie das Repository hinzu und aktualisieren Sie den Paketmanager mit dem folgenden Befehl.

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

So konfigurieren Sie das Yum-Repository des Amazon FSx Lustre-Clients

Das Yum-Paket-Repository des Amazon FSx Lustre-Clients ist standardmäßig so konfiguriert, dass der Lustre-Client installiert wird, der mit der Kernel-Version kompatibel ist, die ursprünglich mit der neuesten unterstützten CentOS-, Rocky Linux- und RHEL 8-Version ausgeliefert wurde. Um einen Lustre-Client zu installieren, der mit der von Ihnen verwendeten Kernelversion kompatibel ist, können Sie die Repository-Konfigurationsdatei bearbeiten.

In diesem Abschnitt wird beschrieben, wie Sie feststellen können, welchen Kernel Sie verwenden, ob Sie die Repository-Konfiguration bearbeiten müssen und wie Sie die Konfigurationsdatei bearbeiten.

1. Ermitteln Sie mithilfe des folgenden Befehls, welcher Kernel derzeit auf Ihrer Compute-Instance läuft.

```
uname -r
```

2. Führen Sie eine der folgenden Aktionen aus:

- Wenn der Befehl zurückkehrt `4.18.0-513*`, müssen Sie die Repository-Konfiguration nicht ändern. Fahren Sie mit dem Verfahren So installieren Sie den Lustre-Client fort.
- Wenn der Befehl zurückkehrt `4.18.0-477*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die Versionen CentOS, Rocky Linux und RHEL 8.8 verweist.

- Wenn der Befehl zurückkehrt `4.18.0-425*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS-, Rocky Linux- und RHEL 8.7-Version verweist.
 - Wenn der Befehl zurückkehrt `4.18.0-372*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS-, Rocky Linux- und RHEL 8.6-Version verweist.
 - Wenn der Befehl zurückkehrt `4.18.0-348*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS-, Rocky Linux- und RHEL 8.5-Version verweist.
 - Wenn der Befehl zurückkehrt `4.18.0-305*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS-, Rocky Linux- und RHEL 8.4-Version verweist.
 - Wenn der Befehl zurückkehrt `4.18.0-240*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS- und RHEL 8.3-Version verweist.
 - Wenn der Befehl zurückkehrt `4.18.0-193*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS- und RHEL 8.2-Version verweist.
3. Bearbeiten Sie die Repository-Konfigurationsdatei mit dem folgenden Befehl so, dass sie auf eine bestimmte Version von RHEL verweist.

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

Wenn Sie beispielsweise auf Version 8.8 verweisen möchten, *specific_RHEL_version* ersetzen Sie `8.8` den Befehl durch.

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

4. Verwenden Sie den folgenden Befehl, um den Yum-Cache zu löschen.

```
sudo yum clean all
```

Um den Lustre-Client zu installieren

- Installieren Sie die Pakete aus dem Repository mit dem folgenden Befehl.

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


Zusätzliche Informationen (CentOS, Rocky Linux und Red Hat 8.2 und neuer)

Mit den obigen Befehlen werden die beiden Pakete installiert, die für das Mounten und die Interaktion mit Ihrem Amazon FSx-Dateisystem erforderlich sind. Das Repository enthält zusätzliche Lustre-Pakete, wie z. B. ein Paket, das den Quellcode enthält, und Pakete, die Tests enthalten, und Sie können sie optional installieren. Verwenden Sie den folgenden Befehl, um alle verfügbaren Pakete im Repository aufzulisten.

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

Verwenden Sie den folgenden Befehl, um das Quell-RPM herunterzuladen, das einen Tarball mit dem Upstream-Quellcode und den Patches enthält, die wir installiert haben.

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

Wenn Sie `yum update` ausführen, wird eine neuere Version des Moduls installiert, sofern verfügbar, und die bestehende Version wird ersetzt. Um zu verhindern, dass die aktuell installierte Version beim Update entfernt wird, fügen Sie Ihrer `/etc/yum.conf` Datei eine Zeile wie die folgende hinzu.

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

Diese Liste enthält die in der `yum.conf` Manpage angegebenen Standardpakete, die nur für die Installation bestimmt sind, und das `kmod-lustre-client` Paket.

Um den Lustre-Client auf CentOS und Red Hat 7.7, 7.8 oder 7.9 (x86_64-Instanzen) zu installieren

Sie können Lustre-Client-Pakete, die mit Red Hat Enterprise Linux (RHEL) und CentOS kompatibel sind, aus dem Yum-Paket-Repository des Amazon FSx Lustre-Clients installieren und aktualisieren. Diese Pakete sind signiert, um sicherzustellen, dass sie vor oder während des Downloads nicht manipuliert wurden. Die Repository-Installation schlägt fehl, wenn Sie den entsprechenden öffentlichen Schlüssel nicht auf Ihrem System installieren.

So fügen Sie das Yum-Paket-Repository des Amazon FSx Lustre-Clients hinzu

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Installieren Sie den öffentlichen Schlüssel Amazon FSx rpm mit dem folgenden Befehl.

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

3. Importieren Sie den Schlüssel mit dem folgenden Befehl.

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

4. Fügen Sie das Repository hinzu und aktualisieren Sie den Paketmanager mit dem folgenden Befehl.

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

So konfigurieren Sie das Yum-Repository des Amazon FSx Lustre-Clients

Das Yum-Paket-Repository des Amazon FSx Lustre-Clients ist standardmäßig so konfiguriert, dass der Lustre-Client installiert wird, der mit der Kernel-Version kompatibel ist, die ursprünglich mit der neuesten unterstützten CentOS- und RHEL 7-Version ausgeliefert wurde. Um einen Lustre-Client zu installieren, der mit der von Ihnen verwendeten Kernel-Version kompatibel ist, können Sie die Repository-Konfigurationsdatei bearbeiten.

In diesem Abschnitt wird beschrieben, wie Sie feststellen können, welchen Kernel Sie verwenden, ob Sie die Repository-Konfiguration bearbeiten müssen und wie Sie die Konfigurationsdatei bearbeiten.

1. Ermitteln Sie mithilfe des folgenden Befehls, welcher Kernel derzeit auf Ihrer Compute-Instance läuft.

```
uname -r
```

2. Führen Sie eine der folgenden Aktionen aus:

- Wenn der Befehl zurückkehrt `3.10.0-1160*`, müssen Sie die Repository-Konfiguration nicht ändern. Fahren Sie mit dem Verfahren So installieren Sie den Lustre-Client fort.
- Wenn der Befehl zurückkehrt `3.10.0-1127*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS- und RHEL 7.8-Version verweist.
- Wenn der Befehl zurückkehrt `3.10.0-1062*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS- und RHEL 7.7-Versionen verweist.

3. Bearbeiten Sie die Repository-Konfigurationsdatei mit dem folgenden Befehl so, dass sie auf eine bestimmte Version von RHEL verweist.

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

Um auf Version 7.8 zu verweisen, *specific_RHEL_version* ersetzen Sie es 7.8 im Befehl durch.

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

Um auf Version 7.7 zu verweisen, *specific_RHEL_version* ersetzen Sie es 7.7 im Befehl durch.

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

4. Verwenden Sie den folgenden Befehl, um den Yum-Cache zu löschen.

```
sudo yum clean all
```

Um den Lustre-Client zu installieren

- Installieren Sie die Lustre-Client-Pakete mit dem folgenden Befehl aus dem Repository.

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

Zusätzliche Informationen (CentOS und Red Hat 7.7 und neuer)

Mit den obigen Befehlen werden die beiden Pakete installiert, die für das Mounten und die Interaktion mit Ihrem Amazon FSx-Dateisystem erforderlich sind. Das Repository enthält zusätzliche Lustre-Pakete, wie z. B. ein Paket, das den Quellcode enthält, und Pakete, die Tests enthalten, und Sie können sie optional installieren. Verwenden Sie den folgenden Befehl, um alle verfügbaren Pakete im Repository aufzulisten.

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

Verwenden Sie den folgenden Befehl, um das Quell-RPM herunterzuladen, das einen Tarball mit dem Upstream-Quellcode und den Patches enthält, die wir installiert haben.

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

Wenn Sie `yum update` ausführen, wird eine neuere Version des Moduls installiert, sofern verfügbar, und die bestehende Version wird ersetzt. Um zu verhindern, dass die aktuell installierte Version beim Update entfernt wird, fügen Sie Ihrer `/etc/yum.conf` Datei eine Zeile wie die folgende hinzu.

```
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
```

Diese Liste enthält die in der `yum.conf` Manpage angegebenen Standardpakete, die nur für die Installation bestimmt sind, und das `kmod-lustre-client` Paket.

So installieren Sie den Lustre-Client auf CentOS 7.8 oder 7.9 (AWS ARM-basierte Graviton-Instanzen)

Sie können Lustre-Client-Pakete aus dem Yum-Paket-Repository des Amazon FSx Lustre-Clients installieren und aktualisieren, die mit CentOS 7 für ARM-basierte Graviton-basierte EC2-Instances kompatibel sind. AWS Diese Pakete sind signiert, um sicherzustellen, dass sie vor oder während des Downloads nicht manipuliert wurden. Die Repository-Installation schlägt fehl, wenn Sie den entsprechenden öffentlichen Schlüssel nicht auf Ihrem System installieren.

So fügen Sie das Yum-Paket-Repository des Amazon FSx Lustre-Clients hinzu

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Installieren Sie den öffentlichen Schlüssel Amazon FSx rpm mit dem folgenden Befehl.

```
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. Importieren Sie den Schlüssel mit dem folgenden Befehl.

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

4. Fügen Sie das Repository hinzu und aktualisieren Sie den Paketmanager mit dem folgenden Befehl.

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

So konfigurieren Sie das Yum-Repository des Amazon FSx Lustre-Clients

Das Yum-Paket-Repository des Amazon FSx Lustre-Clients ist standardmäßig so konfiguriert, dass es den Lustre-Client installiert, der mit der Kernel-Version kompatibel ist, die ursprünglich mit der neuesten unterstützten CentOS 7-Version ausgeliefert wurde. Um einen Lustre-Client zu installieren, der mit der von Ihnen verwendeten Kernel-Version kompatibel ist, können Sie die Repository-Konfigurationsdatei bearbeiten.

In diesem Abschnitt wird beschrieben, wie Sie feststellen können, welchen Kernel Sie verwenden, ob Sie die Repository-Konfiguration bearbeiten müssen und wie Sie die Konfigurationsdatei bearbeiten.

1. Ermitteln Sie mithilfe des folgenden Befehls, welcher Kernel derzeit auf Ihrer Compute-Instance läuft.

```
uname -r
```

2. Führen Sie eine der folgenden Aktionen aus:
 - Wenn der Befehl zurückkehrt `4.18.0-193*`, müssen Sie die Repository-Konfiguration nicht ändern. Fahren Sie mit dem Verfahren So installieren Sie den Lustre-Client fort.
 - Wenn der Befehl zurückkehrt `4.18.0-147*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre-Client für die CentOS 7.8-Version verweist.
3. Bearbeiten Sie die Repository-Konfigurationsdatei mit dem folgenden Befehl so, dass sie auf die CentOS 7.8-Version verweist.

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

4. Verwenden Sie den folgenden Befehl, um den Yum-Cache zu löschen.

```
sudo yum clean all
```

Um den Lustre-Client zu installieren

- Installieren Sie die Pakete aus dem Repository mit dem folgenden Befehl.

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

Zusätzliche Informationen (CentOS 7.8 oder 7.9 für ARM-basierte AWS Graviton-betriebene EC2-Instances)

Mit den obigen Befehlen werden die beiden Pakete installiert, die für das Mounten und die Interaktion mit Ihrem Amazon FSx-Dateisystem erforderlich sind. Das Repository enthält zusätzliche Lustre-Pakete, wie z. B. ein Paket, das den Quellcode enthält, und Pakete, die Tests enthalten, und Sie können sie optional installieren. Verwenden Sie den folgenden Befehl, um alle verfügbaren Pakete im Repository aufzulisten.

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

Verwenden Sie den folgenden Befehl, um das Quell-RPM herunterzuladen, das einen Tarball mit dem Upstream-Quellcode und den Patches enthält, die wir installiert haben.

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

Wenn Sie `yum update` ausführen, wird eine neuere Version des Moduls installiert, sofern verfügbar, und die bestehende Version wird ersetzt. Um zu verhindern, dass die aktuell installierte Version beim Update entfernt wird, fügen Sie Ihrer `/etc/yum.conf` Datei eine Zeile wie die folgende hinzu.

```
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
```

Diese Liste enthält die in der `yum.conf` Manpage angegebenen Standardpakete, die nur für die Installation bestimmt sind, und das `kmod-lustre-client` Paket.

Ubuntu

Um den Lustre-Client auf Ubuntu 22.04 zu installieren

Sie können Lustre-Pakete aus dem Amazon FSx-Repository für Ubuntu 22.04 herunterladen. Um zu überprüfen, ob der Inhalt des Repositorys vor oder während des Herunterladens nicht manipuliert wurde, wird eine GNU Privacy Guard (GPG) -Signatur auf die Metadaten des Repositorys angewendet. Die Installation des Repositorys schlägt fehl, es sei denn, Sie haben den richtigen öffentlichen GPG-Schlüssel auf Ihrem System installiert.

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Gehen Sie wie folgt vor, um das Amazon FSx Ubuntu-Repository hinzuzufügen:
 - a. Wenn Sie noch kein Amazon FSx Ubuntu-Repository auf Ihrer Client-Instance registriert haben, laden Sie den erforderlichen öffentlichen Schlüssel herunter und installieren Sie ihn. Verwenden Sie den folgenden -Befehl.

```
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. Fügen Sie das Amazon FSx-Paket-Repository mit dem folgenden Befehl zu Ihrem lokalen Paketmanager hinzu.

```
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. Ermitteln Sie, welcher Kernel derzeit auf Ihrer Client-Instance läuft, und aktualisieren Sie ihn bei Bedarf. Der Lustre-Client auf Ubuntu 22.04 benötigt einen Kernel 5.15.0-1015-aws oder höher sowohl für x86-basierte EC2-Instances als auch für ARM-basierte EC2-Instances, die mit Graviton-Prozessoren betrieben werden. AWS
 - a. Führen Sie den folgenden Befehl aus, um festzustellen, welcher Kernel läuft.

```
uname -r
```

- b. Führen Sie den folgenden Befehl aus, um auf die neueste Ubuntu-Kernel- und Lustre-Version zu aktualisieren, und starten Sie dann den Computer neu.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
```

Wenn Ihre Kernelversion höher ist als sowohl 5.15.0-1015-aws für x86-basierte EC2-Instances als auch für Graviton-basierte EC2-Instances und Sie nicht auf die neueste Kernel-Version aktualisieren möchten, können Sie Lustre für den aktuellen Kernel mit dem folgenden Befehl installieren.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Die beiden Lustre-Pakete, die für das Mounten und die Interaktion mit Ihrem FSx for Lustre-Dateisystem erforderlich sind, sind installiert. Sie können optional zusätzliche verwandte Pakete installieren, z. B. ein Paket, das den Quellcode enthält, und Pakete mit Tests, die im Repository enthalten sind.

- c. Listet alle verfügbaren Pakete im Repository auf, indem Sie den folgenden Befehl verwenden.

```
sudo apt-cache search ^lustre
```

- d. (Optional) Wenn Sie möchten, dass Ihr System-Upgrade immer auch die Lustre-Client-Module aktualisiert, stellen Sie sicher, dass das `lustre-client-modules-aws` Paket mit dem folgenden Befehl installiert ist.

```
sudo apt install -y lustre-client-modules-aws
```

Note

Wenn Sie eine `Module Not Found` Fehlermeldung erhalten, finden Sie weitere Informationen unter [Informationen zur Behebung fehlender Modulfehler](#).

Um den Lustre-Client auf Ubuntu 20.04 zu installieren

Lustre 2.12-Clients werden auf Ubuntu 20.04 mit dem Kernel 5.15.0-1015-aws oder höher unterstützt. Lustre 2.10-Clients werden unter Ubuntu 20.04 mit Kernel 5.4.0-1011-aws oder höher auf x86-basierten EC2-Instances und Kernel 5.4.0-1015-aws oder höher auf ARM-basierten EC2-Instances unterstützt, die mit Graviton-Prozessoren betrieben werden. AWS

Sie können Lustre-Pakete aus dem Ubuntu 20.04 Amazon FSx-Repository abrufen. Um zu überprüfen, ob der Inhalt des Repositorys vor oder während des Herunterladens nicht manipuliert wurde, wird eine GNU Privacy Guard (GPG) -Signatur auf die Metadaten des Repositorys angewendet. Die Installation des Repositorys schlägt fehl, es sei denn, Sie haben den richtigen öffentlichen GPG-Schlüssel auf Ihrem System installiert.

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Gehen Sie wie folgt vor, um das Amazon FSx Ubuntu-Repository hinzuzufügen:
 - a. Wenn Sie noch kein Amazon FSx Ubuntu-Repository auf Ihrer Client-Instance registriert haben, laden Sie den erforderlichen öffentlichen Schlüssel herunter und installieren Sie ihn. Verwenden Sie den folgenden -Befehl.

```
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. Fügen Sie das Amazon FSx-Paket-Repository mit dem folgenden Befehl zu Ihrem lokalen Paketmanager hinzu.

```
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. Ermitteln Sie, welcher Kernel derzeit auf Ihrer Client-Instance läuft, und aktualisieren Sie ihn bei Bedarf.
 - a. Führen Sie den folgenden Befehl aus, um festzustellen, welcher Kernel läuft.

```
uname -r
```

- b. Führen Sie den folgenden Befehl aus, um auf die neueste Ubuntu-Kernel- und Lustre-Version zu aktualisieren, und starten Sie dann den Computer neu.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
```

Wenn Ihre Kernelversion höher als 5.4.0-1011-aws für x86-basierte EC2-Instances oder höher als 5.4.0-1015-aws für Graviton-basierte EC2-Instances ist und Sie nicht auf die

neueste Kernel-Version aktualisieren möchten, können Sie Lustre für den aktuellen Kernel mit dem folgenden Befehl installieren.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Die beiden Lustre-Pakete, die für das Mounten und die Interaktion mit Ihrem FSx for Lustre-Dateisystem erforderlich sind, sind installiert. Sie können optional zusätzliche verwandte Pakete installieren, z. B. ein Paket, das den Quellcode enthält, und Pakete mit Tests, die im Repository enthalten sind.

- c. Listet alle verfügbaren Pakete im Repository auf, indem Sie den folgenden Befehl verwenden.

```
sudo apt-cache search ^lustre
```

- d. (Optional) Wenn Sie möchten, dass Ihr System-Upgrade immer auch die Lustre-Client-Module aktualisiert, stellen Sie sicher, dass das `lustre-client-modules-aws` Paket mit dem folgenden Befehl installiert ist.

```
sudo apt install -y lustre-client-modules-aws
```

Note

Wenn Sie eine `Module Not Found` Fehlermeldung erhalten, finden Sie weitere Informationen unter [Informationen zur Behebung fehlender Modulfehler](#).

Um den Lustre-Client auf Ubuntu 18.04 zu installieren

Note

Die letzte unterstützte Ubuntu 18-Kernelversion ist `5.4.0.1103.aws`

Sie können Lustre-Pakete aus dem Ubuntu 18.04 Amazon FSx-Repository abrufen. Um zu überprüfen, ob der Inhalt des Repositories vor oder während des Herunterladens nicht manipuliert wurde, wird eine GNU Privacy Guard (GPG) -Signatur auf die Metadaten des Repositories

angewendet. Die Installation des Repositorys schlägt fehl, es sei denn, Sie haben den richtigen öffentlichen GPG-Schlüssel auf Ihrem System installiert.

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Gehen Sie wie folgt vor, um das Amazon FSx Ubuntu-Repository hinzuzufügen:
 - a. Wenn Sie noch kein Amazon FSx Ubuntu-Repository auf Ihrer Client-Instance registriert haben, laden Sie den erforderlichen öffentlichen Schlüssel herunter und installieren Sie ihn. Verwenden Sie den folgenden -Befehl.

```
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. Fügen Sie das Amazon FSx-Paket-Repository mit dem folgenden Befehl zu Ihrem lokalen Paketmanager hinzu.

```
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. Ermitteln Sie, welcher Kernel derzeit auf Ihrer Client-Instance läuft, und aktualisieren Sie ihn bei Bedarf. Der Lustre-Client auf Ubuntu 18.04 benötigt Kernel 4.15.0-1054-aws oder höher für x86-basierte EC2-Instances und Kernel 5.3.0-1023-aws oder höher für ARM-basierte EC2-Instances, die mit Graviton-Prozessoren betrieben werden. AWS
 - a. Führen Sie den folgenden Befehl aus, um festzustellen, welcher Kernel läuft.

```
uname -r
```

- b. Führen Sie den folgenden Befehl aus, um auf die neueste Ubuntu-Kernel- und Lustre-Version zu aktualisieren, und starten Sie dann den Computer neu.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
```

Wenn Ihre Kernelversion höher als 4.15.0-1054-aws für x86-basierte EC2-Instances oder höher als 5.3.0-1023-aws für Graviton-basierte EC2-Instances ist und Sie nicht auf die neueste Kernel-Version aktualisieren möchten, können Sie Lustre für den aktuellen Kernel mit dem folgenden Befehl installieren.

```
sudo apt install -y lustre-client-modules-$(uname -r)
```

Die beiden Lustre-Pakete, die für das Mounten und die Interaktion mit Ihrem FSx for Lustre-Dateisystem erforderlich sind, sind installiert. Sie können optional zusätzliche zugehörige Pakete installieren, z. B. ein Paket, das den Quellcode enthält, und Pakete mit Tests, die im Repository enthalten sind.

- c. Listet alle verfügbaren Pakete im Repository auf, indem Sie den folgenden Befehl verwenden.

```
sudo apt-cache search ^lustre
```

- d. (Optional) Wenn Sie möchten, dass Ihr System-Upgrade immer auch die Lustre-Client-Module aktualisiert, stellen Sie sicher, dass das `lustre-client-modules-aws` Paket mit dem folgenden Befehl installiert ist.

```
sudo apt install -y lustre-client-modules-aws
```

Note

Wenn Sie eine `Module Not Found` Fehlermeldung erhalten, finden Sie weitere Informationen unter [Informationen zur Behebung fehlender Modulfehler](#).

Informationen zur Behebung fehlender Modulfehler

Wenn bei der Installation auf einer beliebigen Version von Ubuntu ein `Module Not Found` Fehler auftritt, gehen Sie wie folgt vor:

Führen Sie ein Downgrade Ihres Kernels auf die neueste unterstützte Version durch. Listet alle verfügbaren Versionen des `lustre-client-modules` Pakets auf und installiert den entsprechenden Kernel. Verwenden Sie dazu den folgenden Befehl.

```
sudo apt-cache search lustre-client-modules
```

Wenn die neueste Version, die im Repository enthalten ist, beispielsweise lautet `lustre-client-modules-5.4.0-1011-aws`, gehen Sie wie folgt vor:

1. Installieren Sie den Kernel, für den dieses Paket gebaut wurde, mit den folgenden Befehlen.

```
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. Starten Sie Ihre Instance mit dem folgenden Befehl neu.

```
sudo reboot
```

3. Installieren Sie den Lustre-Client mit dem folgenden Befehl.

```
sudo apt-get install -y lustre-client-modules-$(uname -r)
```

SUSE Linux

So installieren Sie den Lustre-Client auf SUSE Linux 12 SP3, SP4 oder SP5

So installieren Sie den Lustre-Client auf SUSE Linux 12 SP3

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Installieren Sie den öffentlichen Schlüssel Amazon FSx rpm mithilfe des folgenden Befehls.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-  
public-key.asc
```

3. Importieren Sie den Schlüssel mithilfe des folgenden Befehls.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Fügen Sie das Repository für den Lustre-Client mit dem folgenden Befehl hinzu.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-  
lustre-client.repo
```

5. Laden Sie den Lustre-Client mit den folgenden Befehlen herunter und installieren Sie ihn.

```
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
```

Um den Lustre-Client auf SUSE Linux 12 SP4 zu installieren

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Installieren Sie den öffentlichen Schlüssel Amazon FSx rpm mithilfe des folgenden Befehls.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-
public-key.asc
```

3. Importieren Sie den Schlüssel mithilfe des folgenden Befehls.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Fügen Sie das Repository für den Lustre-Client mit dem folgenden Befehl hinzu.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-
lustre-client.repo
```

5. Führen Sie eine der folgenden Aktionen aus:
 - Wenn Sie SP4 direkt installiert haben, laden Sie den Lustre-Client mit den folgenden Befehlen herunter und installieren Sie ihn.

```
sudo zypper ar --pgpcheck-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
```

- Wenn Sie von SP3 auf SP4 migriert und zuvor das Amazon FSx-Repository für SP3 hinzugefügt haben, laden Sie den Lustre-Client mit den folgenden Befehlen herunter und installieren Sie ihn.

```
sudo zypper ar --pgpcheck-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
```

Um den Lustre-Client auf SUSE Linux 12 SP5 zu installieren

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Installieren Sie den öffentlichen Schlüssel Amazon FSx rpm mithilfe des folgenden Befehls.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Importieren Sie den Schlüssel mithilfe des folgenden Befehls.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Fügen Sie das Repository für den Lustre-Client mit dem folgenden Befehl hinzu.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Führen Sie eine der folgenden Aktionen aus:

- Wenn Sie SP5 direkt installiert haben, laden Sie den Lustre-Client mit den folgenden Befehlen herunter und installieren Sie ihn.

```
sudo zypper ar --pgpcheck-strict fsx-lustre-client.repo
sudo zypper refresh
sudo zypper in lustre-client
```

- Wenn Sie von SP4 auf SP5 migriert und zuvor das Amazon FSx-Repository für SP4 hinzugefügt haben, laden Sie den Lustre-Client mit den folgenden Befehlen herunter und installieren Sie ihn.

```
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

Möglicherweise müssen Sie Ihre Compute-Instance neu starten, damit der Client die Installation abschließen kann.

Mounten von einer Amazon Elastic Compute Cloud-Instance

Sie können Ihr Dateisystem von einer Amazon EC2 EC2-Instance aus mounten.

So mounten Sie Ihr Dateisystem von Amazon EC2

1. Stellen Sie eine Verbindung zu Ihrer Amazon-EC2-Instance her.
2. Erstellen Sie mit dem folgenden Befehl ein Verzeichnis auf Ihrem FSx for Lustre-Dateisystem für den Einhängpunkt.

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

3. Hängen Sie das Amazon FSx for Lustre-Dateisystem in das Verzeichnis ein, das Sie erstellt haben. Verwenden Sie den folgenden Befehl und ersetzen Sie die folgenden Elemente:
 - *file_system_dns_name* Ersetzen Sie es durch den tatsächlichen DNS-Namen des Dateisystems.
 - *mountname* Ersetzen Sie durch den Mount-Namen des Dateisystems. Dieser Mount-Name wird in der Antwort auf den CreateFileSystem API-Vorgang zurückgegeben. Er wird auch in der Antwort auf den describe-file-systems AWS CLI Befehl und in der [DescribeFileSystem-API-Operation](#) zurückgegeben.

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

Dieser Befehl mountet Ihr Dateisystem mit zwei Optionen `-o relatime` und `flock`:

- `relatime`— Die `atime` Option verwaltet zwar Daten `atime` (Inode-Zugriffszeiten) für jeden Dateizugriff, aber die `relatime` Option verwaltet auch `atime` Daten, jedoch nicht für jeden Dateizugriff. Wenn die `relatime` Option aktiviert ist, `atime` werden Daten nur dann auf die Festplatte geschrieben, wenn die Datei seit der `atime` letzten Aktualisierung (`mtime`) geändert wurde oder wenn der letzte Zugriff auf die Datei vor mehr als einer bestimmten

Zeit (standardmäßig 6 Stunden) stattgefunden hat. Wenn Sie entweder die `atime` Option `relatime` oder verwenden, werden die [Dateifreigabeprozesse](#) optimiert.

Note

Wenn Ihr Workload eine genaue Genauigkeit der Zugriffszeit erfordert, können Sie das Mounten mit der Option `atime mount` durchführen. Dies kann sich jedoch negativ auf die Leistung der Arbeitslast auswirken, da der Netzwerkverkehr erhöht wird, der zur Einhaltung genauer Werte für die Zugriffszeit erforderlich ist.

Wenn Ihr Workload keine Zugriffszeit für Metadaten erfordert, kann die Verwendung der `noatime` Mount-Option zur Deaktivierung von Aktualisierungen der Zugriffszeit zu einer Leistungssteigerung führen. Beachten Sie, dass `atime` zielgerichtete Prozesse wie die Freigabe von Dateien oder die Freigabe von Datenvalidität bei ihrer Veröffentlichung ungenau sein können.

- `flock`— Aktiviert das Sperren von Dateien für Ihr Dateisystem. Wenn Sie nicht möchten, dass das Sperren von Dateien aktiviert wird, verwenden Sie den `mount` Befehl ohne `flock`.
4. Vergewissern Sie sich, dass der Befehl `mount` erfolgreich war, indem Sie den Inhalt des Verzeichnisses `/mnt/fsx` auflisten, in das Sie das Dateisystem gemountet haben. Verwenden Sie dazu den folgenden Befehl.

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

Sie können auch den `df` folgenden Befehl verwenden.

```
$ 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
```

Die Ergebnisse zeigen das Amazon FSx-Dateisystem, das auf `/fsx` gemountet ist.

Montage über Amazon Elastic Container Service

Sie können auf Ihr FSx for Lustre-Dateisystem von einem Amazon Elastic Container Service (Amazon ECS) Docker-Container Container Container Container Container Container Container auf einer Amazon EC2 EC2-Instance aus zugreifen. Sie können dies tun, indem Sie eine der folgenden Optionen verwenden:

1. Indem Sie Ihr FSx for Lustre-Dateisystem von der Amazon EC2 EC2-Instance aus mounten, die Ihre Amazon ECS-Aufgaben hostet, und diesen Mount-Punkt in Ihre Container exportieren.
2. Indem Sie das Dateisystem direkt in Ihrem Task-Container mounten.

Weitere Informationen zu Amazon ECS finden Sie unter [Was ist Amazon Elastic Container Service?](#) im Amazon Elastic Container Service Developer Guide.

Wir empfehlen die Verwendung von Option 1 ([Mounten von einer Amazon EC2 EC2-Instance aus, die Amazon ECS-Aufgaben hostet](#)), da sie eine bessere Ressourcennutzung ermöglicht, insbesondere wenn Sie viele Container (mehr als fünf) auf derselben EC2-Instance starten oder wenn Ihre Aufgaben nur von kurzer Dauer sind (weniger als 5 Minuten).

Verwenden Sie Option 2 ([Mounten aus einem Docker-Container](#)), wenn Sie die EC2-Instance nicht konfigurieren können oder wenn Ihre Anwendung die Flexibilität des Containers erfordert.

Note

Die Installation von FSx for Lustre auf einem AWS Fargate-Starttyp wird nicht unterstützt.

In den folgenden Abschnitten werden die Verfahren für jede der Optionen zum Mounten Ihres FSx for Lustre-Dateisystems aus einem Amazon ECS-Container beschrieben.

Themen

- [Mounten von einer Amazon EC2 EC2-Instance aus, die Amazon ECS-Aufgaben hostet](#)
- [Mounten aus einem Docker-Container](#)

Mounten von einer Amazon EC2 EC2-Instance aus, die Amazon ECS-Aufgaben hostet

Dieses Verfahren zeigt, wie Sie eine Amazon ECS on EC2-Instance konfigurieren können, um Ihr FSx for Lustre-Dateisystem lokal zu mounten. Das Verfahren verwendet `volumes mountPoints` Container-Eigenschaften, um die Ressource gemeinsam zu nutzen und dieses Dateisystem für lokal ausgeführte Aufgaben zugänglich zu machen. Weitere Informationen finden Sie unter [Launching an Amazon ECS Container Instance](#) im Amazon Elastic Container Service Developer Guide.

Dieses Verfahren gilt für ein Amazon ECS-optimiertes Amazon Linux 2-AMI. Wenn Sie eine andere Linux-Distribution verwenden, finden Sie weitere Informationen unter [Den Lustre-Client installieren](#).

So mounten Sie Ihr Dateisystem von Amazon ECS auf einer EC2-Instance

1. Wenn Sie Amazon ECS-Instances entweder manuell oder mithilfe einer Auto Scaling Scaling-Gruppe starten, fügen Sie die Zeilen im folgenden Codebeispiel am Ende des Benutzerdatenfeldes hinzu. Ersetzen Sie die folgenden Elemente im Beispiel:
 - `file_system_dns_name` Ersetzen Sie es durch den tatsächlichen DNS-Namen des Dateisystems.
 - `mountname` Ersetzen Sie durch den Mount-Namen des Dateisystems.
 - `mountpoint` Ersetzen Sie ihn durch den Einhängpunkt des Dateisystems, den Sie erstellen müssen.

```
#!/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. Wenn Sie Ihre Amazon ECS-Aufgaben erstellen, fügen Sie der JSON-Definition Folgendes `volumes` und `mountPoints` Container-Eigenschaften hinzu. `mountpoint` Ersetzen Sie es durch den Einhängpunkt des Dateisystems (z. B. `/mnt/fsx`).

```
{
  "volumes": [
    {
      "host": {
        "sourcePath": "mountpoint"
      },
      "name": "Lustre"
    }
  ],
  "mountPoints": [
    {
      "containerPath": "mountpoint",
      "sourceVolume": "Lustre"
    }
  ],
}
```

Mounten aus einem Docker-Container

Das folgende Verfahren zeigt, wie Sie einen Amazon ECS-Taskcontainer konfigurieren können, um das `lustre-client` Paket zu installieren und Ihr FSx for Lustre-Dateisystem darin zu mounten. Das Verfahren verwendet ein Amazon Linux (`amazonlinux`) Docker-Image, aber ein ähnlicher Ansatz kann auch für andere Distributionen funktionieren.

Um Ihr Dateisystem von einem Docker-Container aus zu mounten

1. Installieren Sie das `lustre-client` Paket auf Ihrem Docker-Container und mounten Sie Ihr FSx for Lustre-Dateisystem mit der Eigenschaft. `command` Ersetzen Sie die folgenden Elemente im Beispiel:
 - *file_system_dns_name* Ersetzen Sie es durch den tatsächlichen DNS-Namen des Dateisystems.
 - *mountname* Ersetzen Sie durch den Mount-Namen des Dateisystems.
 - Ersetzen Sie *mountpoint* durch den Mountingpunkt des Dateisystems.

```
"command": [
  "/bin/sh -c \"amazon-linux-extras install -y lustre; mount -t
  lustre file_system_dns_name@tcp:/mountname mountpoint -o relatime,flock;\""
```

```
],
```

2. Fügen Sie Ihrem Container die SYS_ADMIN Möglichkeit hinzu, ihn mithilfe der Eigenschaft zum Mounten Ihres FSx for Lustre-Dateisystems zu autorisieren. `linuxParameters`

```
"linuxParameters": {  
  "capabilities": {  
    "add": [  
      "SYS_ADMIN"  
    ]  
  }  
}
```

Mounten von Amazon FSx-Dateisystemen vor Ort oder über eine Peering-Amazon VPC

Sie können auf zwei Arten auf Ihr Amazon FSx-Dateisystem zugreifen. Eine davon stammt von Amazon EC2 EC2-Instances, die sich in einer Amazon-VPC befinden, die per Peering mit der VPC des Dateisystems verbunden ist. Die andere stammt von lokalen Clients, die über unser VPN mit AWS Direct Connect der VPC Ihres Dateisystems verbunden sind.

Sie verbinden die VPC des Kunden und die VPC Ihres Amazon FSx-Dateisystems entweder über eine VPC-Peering-Verbindung oder ein VPC-Transit-Gateway. Wenn Sie eine VPC-Peering-Verbindung oder ein Transit-Gateway verwenden, um VPCs zu verbinden, können Amazon EC2 EC2-Instances, die sich in einer VPC befinden, auf Amazon FSx-Dateisysteme in einer anderen VPC zugreifen, auch wenn die VPCs zu unterschiedlichen Konten gehören.

Bevor Sie das folgende Verfahren verwenden können, müssen Sie entweder eine VPC-Peering-Verbindung oder ein VPC-Transit-Gateway einrichten.

Ein Transit-Gateway ist ein Netzwerk-Transit-Hub, mit dem Sie Ihre VPCs und On-Premises-Netzwerke miteinander verbinden können. Weitere Informationen zur Verwendung von VPC-Transit Gateways finden Sie unter [Erste Schritte mit Transit Gateways](#) im Amazon VPC-Gateways-Handbuch.

Eine VPC-Peering-Verbindung ist eine Netzwerkverbindung zwischen zwei VPCs. Mit diesem Verbindungstyp können Sie Datenverkehr dazwischen über private IPv4 (Internet Protocol Version 4) oder IPv6-Adressen (Internet Protocol Version 6) weiterleiten. Sie können VPC-Peering verwenden,

um VPCs innerhalb derselben AWS Region oder zwischen Regionen zu verbinden. AWS Weitere Informationen zu VPC-Peering finden Sie unter [Was ist VPC-Peering?](#) im Amazon VPC Peering Guide.

Sie können Ihr Dateisystem von außerhalb seiner VPC mithilfe der IP-Adresse seiner primären Netzwerkschnittstelle mounten. Die primäre Netzwerkschnittstelle ist die erste Netzwerkschnittstelle, die zurückgegeben wird, wenn Sie den `aws fsx describe-file-systems` AWS CLI Befehl ausführen. Sie können diese IP-Adresse auch von der Amazon Web Services Management Console abrufen.

Die folgende Tabelle zeigt die IP-Adressanforderungen für den Zugriff auf Amazon FSx-Dateisysteme über einen Client, der sich außerhalb der VPC des Dateisystems befindet.

Für Kunden in...	Zugriff auf Dateisysteme, die vor dem 17. Dezember 2020 erstellt wurden	Zugriff auf Dateisysteme, die am oder nach dem 17. Dezember 2020 erstellt wurden
Gepeerte VPCs mit VPC Peering oder AWS Transit Gateway	Clients mit IP-Adressen in einem privaten IP-Adressbereich nach RFC 1918 :	✓
Peering-Netzwerke, die oder verwenden AWS Direct Connect AWS VPN	<ul style="list-style-type: none"> • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16 	✓

Wenn Sie auf Ihr Amazon FSx-Dateisystem zugreifen müssen, das vor dem 17. Dezember 2020 mit einem nicht privaten IP-Adressbereich erstellt wurde, können Sie ein neues Dateisystem erstellen, indem Sie eine Sicherungskopie des Dateisystems wiederherstellen. Weitere Informationen finden Sie unter [Arbeiten mit Backups](#).

Um die IP-Adresse der primären Netzwerkschnittstelle für ein Dateisystem abzurufen

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Navigationsbereich Dateisysteme aus.
3. Wählen Sie im Dashboard Ihr Dateisystem aus.
4. Wählen Sie auf der Seite mit den Dateisystemdetails die Option Netzwerk und Sicherheit aus.

5. Wählen Sie unter Netzwerkschnittstelle die ID für Ihre primäre elastic network interface aus. Dadurch gelangen Sie zur Amazon EC2 EC2-Konsole.
6. Suchen Sie auf der Registerkarte Details nach der primären privaten IPv4-IP. Dies ist die IP-Adresse für Ihre primäre Netzwerkschnittstelle.

Note

Sie können die DNS-Namensauflösung (Domain Name System) nicht verwenden, wenn Sie ein Amazon FSx-Dateisystem von außerhalb der VPC mounten, mit der es verknüpft ist.

Automatisches Mounten Ihres Amazon FSx-Dateisystems

Sie können die `/etc/fstab` Datei in Ihrer Amazon EC2 EC2-Instance aktualisieren, nachdem Sie sich zum ersten Mal mit der Instance verbunden haben, sodass sie bei jedem Neustart Ihr Amazon FSx-Dateisystem mountet.

Automatisches Mounten von FSx for Lustre mit `/etc/fstab`

Um Ihr Amazon FSx-Dateisystemverzeichnis beim Neustart der Amazon EC2 EC2-Instance automatisch zu mounten, können Sie die Datei verwenden. `fstab` Die `fstab`-Datei enthält Informationen zu Dateisystemen. Der Befehl `mount -a`, der beim Start der Instance ausgeführt wird, mountet die in der Datei aufgelisteten Dateisysteme. `fstab`

Note

Bevor Sie die `/etc/fstab` Datei Ihrer EC2-Instance aktualisieren können, stellen Sie sicher, dass Sie Ihr Amazon FSx-Dateisystem bereits erstellt haben. Weitere Informationen finden Sie [Erstellen Sie Ihr FSx for Lustre-Dateisystem](#) in der Übung Erste Schritte.

So aktualisieren Sie die `/etc/fstab`-Datei in Ihrer EC2-Instance:

1. Stellen Sie eine Verbindung mit der EC2-Instance her und öffnen Sie die Datei `/etc/fstab` in einem Editor.
2. Fügen Sie der Datei `/etc/fstab` die folgende Zeile hinzu.

Hängen Sie das Amazon FSx for Lustre-Dateisystem in das Verzeichnis ein, das Sie erstellt haben. Verwenden Sie den folgenden Befehl und ersetzen Sie Folgendes:

- `/fsx` Ersetzen Sie durch das Verzeichnis, in das Sie Ihr Amazon FSx-Dateisystem mounten möchten.
- `file_system_dns_name` Ersetzen Sie es durch den tatsächlichen DNS-Namen des Dateisystems.
- `mountname` Ersetzen Sie durch den Mount-Namen des Dateisystems. Dieser Mount-Name wird in der Antwort auf den `CreateFileSystem` API-Vorgang zurückgegeben. Er wird auch in der Antwort auf den `describe-file-systems` AWS CLI Befehl und in der [DescribeFileSystems](#) API-Operation zurückgegeben.

```
file_system_dns_name@tcp://mountname /fsx lustre defaults,relatime,flock,_netdev,x-systemd.automount,x-systemd.requires=network.service 0 0
```

Warning

Verwenden Sie beim automatischen Mounting Ihres Dateisystems die Option `_netdev`, um es als Netzwerkdateisystem zu identifizieren. Wenn `_netdev` fehlt, reagiert die EC2-Instance möglicherweise nicht mehr. Der Grund dafür ist, dass zuerst das Netzwerk auf der Datenverarbeitungs-Instance gestartet worden sein muss. Die Netzwerkdateisysteme müssen danach initialisiert werden. Weitere Informationen finden Sie unter [Automatisches Mounting schlägt fehl und die Instance reagiert nicht](#).

3. Speichern Sie die Änderungen an der Datei.


Ihre EC2-Instance ist jetzt so konfiguriert, dass sie das Amazon FSx-Dateisystem bei jedem Neustart mountet.

Note

In einigen Fällen muss Ihre Amazon EC2 EC2-Instance möglicherweise unabhängig vom Status Ihres bereitgestellten Amazon FSx-Dateisystems gestartet werden. In diesen Fällen fügen Sie die `nofail` Option zum Eintrag Ihres Dateisystems in Ihrer `/etc/fstab` Datei hinzu.

Die Felder in der Codezeile, die Sie der `/etc/fstab` Datei hinzugefügt haben, bewirken Folgendes.

Feld	Beschreibung
<code>file_system_dns_name @tcp:/</code>	Der DNS-Name für Ihr Amazon FSx-Dateisystem, der das Dateisystem identifiziert. Sie können diesen Namen von der Konsole oder programmgesteuert aus dem AWS CLI oder einem SDK abrufen. AWS
<code>mountname</code>	Der Mount-Name für das Dateisystem. Sie können diesen Namen von der Konsole oder programmgesteuert AWS CLI mithilfe des <code>describe-file-systems</code> Befehls oder der AWS API oder des SDK mithilfe des DescribeFileSystems Vorgangs abrufen.
<code>/fsx</code>	Der Bereitstellungspunkt für das Amazon FSx-Dateisystem auf Ihrer EC2-Instance.
<code>lustre</code>	Der Typ des Dateisystems, Amazon FSx.
<code>mount options</code>	<p>Einhängeoptionen für das Dateisystem, dargestellt als kommagetrennte Liste der folgenden Optionen:</p> <ul style="list-style-type: none"> <code>defaults</code>— Dieser Wert weist das Betriebssystem an, die Standard-Einhängeoptionen zu verwenden. Sie können die Standard-Einhängeoptionen auflisten, nachdem das Dateisystem gemountet wurde, indem Sie sich die Ausgabe des <code>mount</code> Befehls ansehen. <code>relatime</code>— Diese Option verwaltet Daten <code>atime</code> (Inode-Zugriffszeiten), jedoch nicht für jeden Dateizugriff. Wenn diese Option aktiviert ist, <code>atime</code> werden Daten nur dann auf die Festplatte geschrieben, wenn die Datei seit der letzten Aktualisierung der <code>atime</code> Daten geändert wurde (<code>mtime</code>) oder wenn vor mehr als einer bestimmten Zeit (standardmäßig ein Tag) zuletzt auf die Datei zugegriffen wurde. Wenn Sie Aktualisierungen der Inode-Zugriffszeit deaktivieren möchten, verwenden Sie stattdessen die <code>noatime</code> Mount-Option. <code>flock</code>— hängt Ihr Dateisystem mit aktivierter Dateisperre ein. Wenn Sie nicht möchten, dass die Dateisperre aktiviert ist, verwenden Sie stattdessen die <code>noflock</code> Mount-Option.

Feld	Beschreibung
	<ul style="list-style-type: none"> • <code>_netdev</code>— Der Wert teilt dem Betriebssystem mit, dass sich das Dateisystem auf einem Gerät befindet, das Netzwerkzugriff benötigt. Diese Option verhindert, dass die Instance das Dateisystem mountet, bis das Netzwerk auf dem Client aktiviert wurde.
<pre>x-systemd .automount,x- systemd.requires=network.service</pre>	<p>Diese Optionen stellen sicher, dass der Auto Mounter nicht läuft, bis die Netzwerkverbindung online ist.</p> <div data-bbox="505 562 1507 877" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p> Note</p> <p>Verwenden Sie für Amazon Linux 2023 und Ubuntu 22.04 die <code>x-systemd.requires=systemd-networkd-wait-online.service</code> Option anstelle der <code>x-systemd.requires=network.service</code> Option.</p> </div>
<pre>0</pre>	<p>Ein Wert, der angibt, ob das Dateisystem von dump gesichert werden soll. Für Amazon FSx sollte dieser Wert sein. <code>0</code></p>
<pre>0</pre>	<p>Ein Wert, der die Reihenfolge angibt, in der Dateisysteme beim Booten <code>fsck</code> überprüft werden. Für Amazon FSx-Dateisysteme sollte dieser Wert angeben, dass <code>0</code> sie beim Start nicht ausgeführt werden <code>fsck</code> sollen.</p>

Mounten bestimmter Dateisätze

Mithilfe der Lustre-Dateisatzfunktion können Sie nur eine Teilmenge des Dateisystem-Namespaces mounten, die als Dateisatz bezeichnet wird. Um einen Dateisatz des Dateisystems einzuhängen, geben Sie auf dem Client den Unterverzeichnispfad nach dem Dateisystemnamen an. Ein Dateisatz-Mount (auch Unterverzeichnis-Mount genannt) schränkt die Sichtbarkeit des Dateisystem-Namespaces auf einem bestimmten Client ein.

Beispiel — Hängen Sie einen Lustre-Dateisatz ein

1. Angenommen, Sie haben ein FSx for Lustre-Dateisystem mit den folgenden Verzeichnissen:

```
team1/dataset1/  
team2/dataset2/
```

2. Sie mounten nur den team1/dataset1 Dateisatz, sodass nur dieser Teil des Dateisystems lokal auf dem Client sichtbar ist. Verwenden Sie den folgenden Befehl und ersetzen Sie die folgenden Elemente:
 - *file_system_dns_name* Ersetzen Sie es durch den tatsächlichen DNS-Namen des Dateisystems.
 - *mountname* Ersetzen Sie durch den Mount-Namen des Dateisystems. Dieser Mount-Name wird in der Antwort auf den CreateFileSystem API-Vorgang zurückgegeben. Er wird auch in der Antwort auf den describe-file-systems AWS CLI Befehl und in der [DescribeFileSystem-API-Operation](#) zurückgegeben.

```
mount -t lustre file_system_dns_name@tcp:/mountname/team1/dataset1 /fsx
```

Beachten Sie bei der Verwendung der Lustre-Dateisatzfunktion Folgendes:

- Es gibt keine Einschränkungen, die einen Client daran hindern, das Dateisystem mit einem anderen oder gar keinem Dateisatz erneut zu mounten.
- Bei der Verwendung eines Dateisatzes funktionieren einige Lustre-Administrationsbefehle, die Zugriff auf das `.lustre/` Verzeichnis erfordern, möglicherweise nicht, wie z. B. der Befehl `lfs fid2path`
- Wenn Sie planen, mehrere Unterverzeichnisse aus demselben Dateisystem auf demselben Host zu mounten, sollten Sie sich bewusst sein, dass dies mehr Ressourcen beansprucht als ein einzelner Einhängpunkt und es daher effizienter sein könnte, das Dateisystem-Stammverzeichnis stattdessen nur einmal zu mounten.

[Weitere Informationen zur Lustre-Dateisatzfunktion finden Sie im Lustre-Betriebshandbuch auf der Lustre-Dokumentationswebsite.](#)

Aufheben des Mountings von Dateisystemen

Bevor Sie ein Dateisystem löschen, empfehlen wir, dass Sie sein Mounting auf allen Amazon-EC2-Instances aufheben, mit denen es verbunden ist. Sie können das Mounting eines Dateisystems

auf der Amazon-EC2-Instance aufheben, indem Sie den Befehl `umount` auf der Instance selbst ausführen. Sie können ein Amazon FSx-Dateisystem nicht über das AWS CLI, das oder über eines der AWS Management Console SDKs unmounten AWS . Um ein Amazon FSx-Dateisystem auszuhängen, das mit einer Amazon EC2 EC2-Instance unter Linux verbunden ist, verwenden Sie den `umount` Befehl wie folgt:

```
umount /mnt/fsx
```

Wir empfehlen, dass Sie keine anderen `umount`-Optionen angeben. Vermeiden Sie die Einstellung anderer `umount`-Optionen, die sich von den Standardwerten unterscheiden.

Sie können überprüfen, ob Ihr Amazon FSx-Dateisystem unmountet wurde, indem Sie den `df` Befehl ausführen. Mit diesem Befehl werden die Datenträgnutzungsstatistiken für die Dateisysteme angezeigt, die derzeit auf der Linux-basierten Amazon-EC2-Instance gemountet werden. Wenn das Amazon FSx-Dateisystem, das Sie unmounten möchten, nicht in der `df` Befehlsausgabe aufgeführt ist, bedeutet dies, dass das Dateisystem unmountet ist.

Example — Identifizieren Sie den Mount-Status eines Amazon FSx-Dateisystems und hängen Sie es aus

```
$ 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% /
```

Arbeiten mit Amazon EC2-Spot-Instances

FSx for Lustre kann mit EC2-Spot-Instances verwendet werden, um Ihre Amazon EC2 EC2-Kosten deutlich zu senken. Eine Spot-Instance ist eine ungenutzte EC2-Instance, die für weniger als den On-Demand-Preis erhältlich ist. Amazon EC2 kann Ihre Spot-Instance unterbrechen, wenn der Spot-

Preis Ihren Höchstpreis überschreitet, wenn die Nachfrage nach Spot-Instances steigt oder wenn das Angebot an Spot-Instances sinkt.

Wenn Amazon EC2 eine Spot-Instance unterbricht, wird eine Benachrichtigung über die Unterbrechung der Spot-Instance bereitgestellt. Dadurch erhält die Instance zwei Minuten, bevor sie von Amazon EC2 unterbrochen wird, eine Warnmeldung. Weitere Informationen finden Sie unter [Spot-Instances](#) im Amazon EC2 EC2-Benutzerhandbuch.

Um sicherzustellen, dass Amazon FSx-Dateisysteme nicht von EC2-Spot-Instance-Unterbrechungen betroffen sind, empfehlen wir, die Bereitstellung von Amazon FSx-Dateisystemen aufzuheben, bevor EC2-Spot-Instances beendet oder in den Ruhezustand versetzt werden. Weitere Informationen finden Sie unter [Aufheben des Mountings von Dateisystemen](#).

Umgang mit Amazon EC2-Spot-Instance-Unterbrechungen

FSx for Lustre ist ein verteiltes Dateisystem, bei dem Server- und Client-Instanzen zusammenarbeiten, um ein performantes und zuverlässiges Dateisystem bereitzustellen. Sie sorgen für einen verteilten und kohärenten Zustand sowohl auf Client- als auch auf Serverinstanzen. FSx for Lustre-Server delegieren temporäre Zugriffsberechtigungen an Clients, während sie aktiv I/O durchführen und Dateisystemdaten zwischenspeichern. Es wird erwartet, dass Clients innerhalb kurzer Zeit antworten, wenn Server sie auffordern, ihre temporären Zugriffsberechtigungen zu widerrufen. Um das Dateisystem vor Clients zu schützen, die sich schlecht benehmen, können Server Lustre-Clients, die nach einigen Minuten nicht antworten, vom Server entfernen. Um zu vermeiden, dass Sie mehrere Minuten warten müssen, bis ein Client, der nicht reagiert, auf die Serveranfrage antwortet, ist es wichtig, die Lustre-Clients sauber auszuhängen, insbesondere bevor Sie EC2-Spot-Instances beenden.

EC2 Spot sendet Kündigungsmittelungen 2 Minuten im Voraus, bevor eine Instance heruntergefahren wird. Wir empfehlen, dass Sie den Prozess der sauberen Deinstallation der Lustre-Clients automatisieren, bevor Sie EC2-Spot-Instances beenden.

Example — Skript zum sauberen Aushängen terminierter EC2-Spot-Instances

Dieses Beispielskript macht die Bereitstellung terminierter EC2-Spot-Instances sauber rückgängig, indem es wie folgt vorgeht:

- Sucht nach Kündigungsmittelungen von Spot.
- Wenn es eine Kündigungsmittelung erhält:
 - Beenden Sie Anwendungen, die auf das Dateisystem zugreifen.

- Hängt das Dateisystem aus, bevor die Instanz beendet wird.

Sie können das Skript nach Bedarf anpassen, insbesondere um Ihre Anwendung ordnungsgemäß herunterzufahren. Weitere Informationen zu bewährten Methoden für den Umgang mit Spot-Instance-Unterbrechungen finden Sie unter [Bewährte Methoden für den Umgang mit EC2-Spot-Instance-Unterbrechungen](#).

```
#!/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

# Start a graceful shutdown of the host
shutdown now

done
```

Verwaltung von Dateisystemen

FSx for Lustre bietet eine Reihe von Funktionen, die die Ausführung Ihrer administrativen Aufgaben vereinfachen. Dazu gehören die Möglichkeit, point-in-time Backups zu erstellen, Speicherkontingente für das Dateisystem zu verwalten, Ihre Speicher- und Durchsatzkapazität zu verwalten, die Datenkomprimierung zu verwalten und Wartungsfenster für die routinemäßige Durchführung von Software-Patches des Systems festzulegen.

Sie können Ihre FSx for Lustre-Dateisysteme mithilfe der Amazon FSx Management Console AWS Command Line Interface (AWS CLI), der Amazon FSx-API oder SDKs verwalten. AWS

Themen

- [Arbeiten mit Backups](#)
- [Speicherkontingente](#)
- [Verwaltung der Speicherkapazität](#)
- [Verwaltung der Metadaten-Performance](#)
- [Verwaltung der Durchsatzkapazität](#)
- [Lustre-Datenkomprimierung](#)
- [Lustre-Wurzelkürbis](#)
- [Status des Dateisystems FSx for Lustre](#)
- [Kennzeichnen Sie Ihre Amazon FSx-Ressourcen](#)
- [Wartungsfenster von Amazon FSx for Lustre](#)
- [Löschen eines Dateisystems](#)

Arbeiten mit Backups

Mit Amazon FSx for Lustre können Sie automatische tägliche Backups und vom Benutzer initiierte Backups von persistenten Dateisystemen erstellen, die nicht mit einem dauerhaften Amazon S3 S3-Daten-Repository verknüpft sind. Amazon FSx-Backups sind file-system-consistent äußerst robust und inkrementell. Um eine hohe Haltbarkeit zu gewährleisten, speichert Amazon FSx for Lustre Backups im Amazon Simple Storage Service (Amazon S3) mit einer Haltbarkeit von 99,999999999% (11 9).

FSx for Lustre-Dateisystem-Backups sind blockbasierte, inkrementelle Backups, unabhängig davon, ob sie mit der automatischen täglichen Sicherung oder der vom Benutzer initiierten Backup-Funktion

generiert werden. Das bedeutet, dass Amazon FSx, wenn Sie ein Backup erstellen, die Daten auf Ihrem Dateisystem mit Ihrem vorherigen Backup auf Blockebene vergleicht. Dann speichert Amazon FSx eine Kopie aller Änderungen auf Blockebene im neuen Backup. Daten auf Blockebene, die seit der vorherigen Sicherung unverändert geblieben sind, werden nicht in der neuen Sicherung gespeichert. Die Dauer des Sicherungsvorgangs hängt davon ab, wie viele Daten sich seit der letzten Sicherung geändert haben, und ist unabhängig von der Speicherkapazität des Dateisystems. Die folgende Liste zeigt die Backup-Zeiten unter verschiedenen Umständen:

- Die erste Sicherung eines brandneuen Dateisystems mit sehr wenigen Daten dauert Minuten.
- Die erste Sicherung eines brandneuen Dateisystems, die nach dem Laden von TB an Daten erstellt wurde, dauert Stunden.
- Ein zweites Backup des Dateisystems mit TB an Daten mit minimalen Änderungen an den Daten auf Blockebene (relativ wenige Erstellungen/Änderungen) dauert Sekunden.
- Eine dritte Sicherung desselben Dateisystems, nachdem eine große Datenmenge hinzugefügt und geändert wurde, dauert Stunden.

Wenn Sie eine Sicherung löschen, werden nur die Daten entfernt, die für diese Sicherung eindeutig sind. Jedes FSx for Lustre-Backup enthält alle Informationen, die benötigt werden, um aus dem Backup ein neues Dateisystem zu erstellen, wodurch effektiv ein point-in-time Snapshot des Dateisystems wiederhergestellt wird.

Das Erstellen regelmäßiger Backups für Ihr Dateisystem ist eine bewährte Methode, die die Replikation ergänzt, die Amazon FSx for Lustre für Ihr Dateisystem durchführt. Amazon FSx-Backups helfen Ihnen dabei, Ihre Anforderungen an die Aufbewahrung von Backups und die Einhaltung von Vorschriften zu erfüllen. Die Arbeit mit Amazon FSx for Lustre-Backups ist einfach, egal ob es um das Erstellen von Backups, das Kopieren eines Backups, das Wiederherstellen eines Dateisystems aus einem Backup oder das Löschen eines Backups geht.

Backups werden auf Scratch-Dateisystemen nicht unterstützt, da diese Dateisysteme für die temporäre Speicherung und kurzfristige Verarbeitung von Daten konzipiert sind. Backups werden auf Dateisystemen, die mit einem Amazon S3 S3-Bucket verknüpft sind, nicht unterstützt, da der S3-Bucket als primäres Daten-Repository dient und das Lustre-Dateisystem nicht unbedingt den gesamten Datensatz zu einem bestimmten Zeitpunkt enthält.

Themen

- [Backup-Unterstützung in FSx for Lustre](#)
- [Arbeiten mit automatischen täglichen Backups](#)

- [Arbeiten mit vom Benutzer initiierten Backups](#)
- [Verwendung AWS Backup mit Amazon FSx](#)
- [Kopieren eines Backups](#)
- [Backups werden innerhalb derselben Datei kopiert AWS-Konto](#)
- [Backups wiederherstellen](#)
- [Löschen eines Backups](#)

Backup-Unterstützung in FSx for Lustre

Backups werden nur auf persistenten Dateisystemen von FSx for Lustre unterstützt, die nicht mit einem Amazon S3 S3-Datenrepository verknüpft sind.

Amazon FSx unterstützt keine Backups auf Scratch-Dateisystemen, da Scratch-Dateisysteme für die temporäre Speicherung und kurzfristige Verarbeitung von Daten konzipiert sind. Amazon FSx unterstützt keine Backups auf Dateisystemen, die mit einem Amazon S3 S3-Bucket verknüpft sind, da der S3-Bucket als primäres Daten-Repository dient und das Dateisystem nicht unbedingt den gesamten Datensatz zu einem bestimmten Zeitpunkt enthält. Weitere Informationen finden Sie unter [Bereitstellungsoptionen für das Dateisystem](#) und [Verwenden von Datenrepositorys](#).

Arbeiten mit automatischen täglichen Backups

Amazon FSx for Lustre kann täglich ein automatisches Backup Ihres Dateisystems erstellen. Diese automatischen täglichen Backups erfolgen während des täglichen Backup-Fensters, das bei der Erstellung des Dateisystems festgelegt wurde. Irgendwann während des täglichen Backup-Fensters wird die Speicher-I/O möglicherweise kurzzeitig unterbrochen, während der Backup-Vorgang initialisiert wird (normalerweise für weniger als ein paar Sekunden). Wir empfehlen Ihnen, bei der Auswahl Ihres täglichen Backup-Fensters eine passende Tageszeit zu wählen. Diese Zeit liegt idealerweise außerhalb der normalen Betriebszeiten der Anwendungen, die das Dateisystem verwenden.

Automatische tägliche Backups werden für einen bestimmten Zeitraum aufbewahrt, der als Aufbewahrungszeitraum bezeichnet wird. Sie können die Aufbewahrungsfrist auf 0 bis 90 Tage festlegen. Wenn Sie den Aufbewahrungszeitraum auf 0 (Null) Tage festlegen, werden automatische tägliche Backups deaktiviert. Die Standardaufbewahrungsdauer für automatische tägliche Backups beträgt 0 Tage. Automatische tägliche Backups werden gelöscht, wenn das Dateisystem gelöscht wird.

Note

Wenn Sie die Aufbewahrungsfrist auf 0 Tage festlegen, wird Ihr Dateisystem niemals automatisch gesichert. Es wird dringend empfohlen, automatische tägliche Backups für Dateisysteme zu verwenden, mit denen ein gewisses Maß an kritischer Funktionalität verknüpft ist.

Sie können das AWS CLI oder eines der AWS SDKs verwenden, um das Backup-Fenster und den Aufbewahrungszeitraum für Backups für Ihre Dateisysteme zu ändern. Verwenden Sie die [UpdateFileSystem](#)API-Operation oder den [update-file-system](#)CLI-Befehl.

Arbeiten mit vom Benutzer initiierten Backups

Mit Amazon FSx for Lustre können Sie jederzeit manuell Backups Ihrer Dateisysteme erstellen. Sie können dies mit der Amazon FSx for Lustre-Konsole, der API oder der AWS Command Line Interface (CLI) tun. Ihre vom Benutzer initiierten Backups von Amazon FSx-Dateisystemen laufen nie ab und sie sind so lange verfügbar, wie Sie sie behalten möchten. Benutzerinitiierte Backups werden auch nach dem Löschen des Dateisystems, das gesichert wurde, beibehalten. Sie können vom Benutzer initiierte Backups nur mithilfe der Amazon FSx for Lustre-Konsole, API oder CLI löschen. Sie werden niemals automatisch von Amazon FSx gelöscht. Weitere Informationen finden Sie unter [Löschen eines Backups](#).

Benutzerinitiierte Backups erstellen

Das folgende Verfahren führt Sie durch die Erstellung eines benutzerinitiierten Backups in der Amazon FSx-Konsole für ein vorhandenes Dateisystem.

Um ein vom Benutzer initiiertes Dateisystem-Backup zu erstellen

1. [Öffnen Sie die Amazon FSx for Lustre-Konsole unter https://console.aws.amazon.com/fsx/](https://console.aws.amazon.com/fsx/).
2. Wählen Sie im Konsolen-Dashboard den Namen des Dateisystems aus, das Sie sichern möchten.
3. Wählen Sie unter Aktionen die Option Backup erstellen aus.
4. Geben Sie im sich öffnenden Dialogfeld „Backup erstellen“ einen Namen für Ihr Backup ein. Backup-Namen können maximal 256 Unicode-Zeichen enthalten, einschließlich Buchstaben, Leerzeichen, Zahlen und Sonderzeichen. + - = _:/

5. Wählen Sie Create backup (Backup erstellen).

Sie haben jetzt Ihr Dateisystem-Backup erstellt. Sie finden eine Tabelle mit all Ihren Backups in der Amazon FSx for Lustre-Konsole, indem Sie in der linken Navigationsleiste Backups wählen. Sie können nach dem Namen suchen, den Sie Ihrem Backup gegeben haben, und die Tabelle so filtern, dass nur passende Ergebnisse angezeigt werden.

Wenn Sie ein vom Benutzer initiiertes Backup wie in diesem Verfahren beschrieben erstellen, hat es den Typ und den Status Wird erstellt **USER_INITIATED**, während Amazon FSx das Backup erstellt. Während das Backup auf Amazon S3 übertragen wird, ändert sich der Status in Übertragen, bis es vollständig verfügbar ist.

Verwendung AWS Backup mit Amazon FSx

AWS Backup ist eine einfache und kostengünstige Möglichkeit, Ihre Daten zu schützen, indem Sie Ihre Amazon FSx-Dateisysteme sichern. AWS Backup ist ein einheitlicher Backup-Service, der das Erstellen, Kopieren, Wiederherstellen und Löschen von Backups vereinfacht und gleichzeitig eine verbesserte Berichterstattung und Prüfung bietet. AWS Backup erleichtert die Entwicklung einer zentralen Backup-Strategie zur Einhaltung gesetzlicher, regulatorischer und professioneller Vorschriften. AWS Backup erleichtert außerdem den Schutz Ihrer AWS Speichervolumen, Datenbanken und Dateisysteme, indem es einen zentralen Ort bereitstellt, an dem Sie Folgendes tun können:

- Konfigurieren und prüfen Sie die AWS Ressourcen, die Sie sichern möchten.
- Automatisieren geplanter Sicherungen
- Festlegen von Aufbewahrungsrichtlinien
- Kopieren Sie Backups zwischen AWS Regionen und AWS Konten.
- Überwachen der letzten Sicherungs- und Wiederherstellungsaktivitäten

AWS Backup verwendet die integrierte Backup-Funktionalität von Amazon FSx. Von der AWS Backup Konsole aus erstellte Backups haben dieselbe Konsistenz und Leistung des Dateisystems und dieselben Wiederherstellungsoptionen wie Backups, die über die Amazon FSx-Konsole erstellt wurden. Wenn Sie AWS Backup diese Backups verwalten, erhalten Sie zusätzliche Funktionen, wie z. B. unbegrenzte Aufbewahrungsoptionen und die Möglichkeit, geplante Backups so oft wie jede Stunde zu erstellen. Darüber hinaus werden Ihre unveränderlichen Backups auch nach dem Löschen

des Quelldateisystems AWS Backup beibehalten. Dies schützt vor versehentlichem oder böswilligem Löschen.

Von erstellte Backups AWS Backup gelten als vom Benutzer initiierte Backups und werden auf das vom Benutzer initiierte Backup-Kontingent für Amazon FSx angerechnet. Sie können Backups, die von erstellt wurden, AWS Backup in der Amazon FSx-Konsole, CLI und API sehen und wiederherstellen. Backups, die von erstellt wurden AWS Backup , haben einen Backup-Typ `AWS_BACKUP`. Sie können jedoch die von AWS Backup der Amazon FSx-Konsole, CLI oder API erstellten Backups nicht löschen. Weitere Informationen AWS Backup zur Sicherung Ihrer Amazon FSx-Dateisysteme finden Sie unter [Arbeiten mit Amazon FSx-Dateisystemen](#) im AWS Backup Entwicklerhandbuch.

Kopieren eines Backups

Sie können Amazon FSx verwenden, um Backups innerhalb desselben AWS Kontos manuell in eine andere AWS Region (regionsübergreifende Kopien) oder innerhalb derselben AWS Region (regionsinterne Kopien) zu kopieren. Sie können regionsübergreifende Kopien nur innerhalb derselben Partition erstellen. AWS Sie können benutzerinitiierte Backup-Kopien mithilfe der Amazon FSx-Konsole oder API AWS CLI erstellen. Wenn Sie eine vom Benutzer initiierte Sicherungskopie erstellen, hat sie den folgenden Typ. `USER_INITIATED`

Sie können es auch verwenden AWS Backup , um Backups zwischen AWS Regionen und AWS Konten zu kopieren. AWS Backup ist ein vollständig verwalteter Backup-Management-Service, der eine zentrale Schnittstelle für richtlinienbasierte Backup-Pläne bietet. Dank der kontenübergreifenden Verwaltung können Sie Backup-Richtlinien automatisch verwenden, um Backup-Pläne für alle Konten innerhalb Ihres Unternehmens anzuwenden.

Regionsübergreifende Backup-Kopien sind besonders wertvoll für die regionsübergreifende Notfallwiederherstellung. Sie erstellen Backups und kopieren sie in eine andere AWS Region, sodass Sie im Falle eines Notfalls in der primären AWS Region die Daten aus dem Backup wiederherstellen und die Verfügbarkeit in der anderen AWS Region schnell wiederherstellen können. Sie können auch Sicherungskopien verwenden, um Ihren Dateidatensatz in eine andere AWS Region oder innerhalb derselben AWS Region zu klonen. Sie erstellen Sicherungskopien innerhalb desselben AWS Kontos (regionsübergreifend oder regionsübergreifend), indem Sie die Amazon FSx-Konsole oder die Amazon FSx for AWS CLI Lustre-API verwenden. Sie können sie auch verwenden, um Sicherungskopien [AWS Backup](#) zu erstellen, entweder auf Abruf oder auf Grundlage von Richtlinien.

Kontoübergreifende Sicherungskopien sind nützlich, wenn es darum geht, Ihre gesetzlichen Anforderungen zu erfüllen und Backups auf ein isoliertes Konto zu kopieren. Sie bieten auch eine

zusätzliche Datenschutzebene, um das versehentliche oder böswillige Löschen von Backups, den Verlust von Anmeldeinformationen oder die Kompromittierung von AWS KMS Schlüsseln zu verhindern. Kontoübergreifende Backups unterstützen Fan-In (Kopieren von Backups von mehreren Primärkonten auf ein isoliertes Backup-Kopie-Konto) und Fan-Out (Kopieren von Backups von einem primären Konto auf mehrere isolierte Backup-Kopie-Konten).

Mithilfe von `with support` können Sie kontoübergreifende Sicherungskopien erstellen. AWS Backup AWS Organizations Kontogrenzen für kontoübergreifende Kopien werden durch AWS Organizations Richtlinien definiert. Weitere Informationen zur Erstellung von AWS Backup kontoübergreifenden Backup-Kopien finden Sie AWS-Konten im AWS Backup Developer Guide unter [Backup-Kopien erstellen](#).

Einschränkungen bei Backup-Kopien

Im Folgenden sind einige Einschränkungen beim Kopieren von Backups aufgeführt:

- Regionsübergreifende Sicherungskopien werden nur zwischen zwei beliebigen Handelsregionen AWS-Regionen, zwischen den Regionen China (Peking) und China (Ningxia) sowie zwischen den Regionen AWS GovCloud (USA Ost) und AWS GovCloud (USA West) unterstützt, nicht jedoch zwischen diesen Gruppen von Regionen.
- Regionsübergreifende Backup-Kopien werden in Opt-in-Regionen nicht unterstützt.
- Sie können innerhalb jeder Region regionsinterne Sicherungskopien erstellen. AWS
- Das Quell-Backup muss den Status von haben, AVAILABLE bevor Sie es kopieren können.
- Sie können ein Quell-Backup nicht löschen, wenn es kopiert wird. Zwischen dem Zeitpunkt, zu dem das Ziel-Backup verfügbar wird, und dem Zeitpunkt, zu dem Sie das Quell-Backup löschen dürfen, kann es zu einer kurzen Verzögerung kommen. Sie sollten diese Verzögerung berücksichtigen, wenn Sie erneut versuchen, ein Quell-Backup zu löschen.
- Pro Konto können bis zu fünf Backup-Kopie-Anfragen in eine einzelne AWS Zielregion ausgeführt werden.

Berechtigungen für regionsübergreifende Sicherungskopien

Sie verwenden eine IAM-Richtlinienanweisung, um Berechtigungen zur Durchführung eines Sicherungskopievorgangs zu erteilen. Um mit der AWS Quellregion zu kommunizieren und eine regionsübergreifende Sicherungskopie anzufordern, muss der Anforderer (IAM-Rolle oder IAM-Benutzer) Zugriff auf das Quell-Backup und die Quellregion haben. AWS

Sie verwenden die Richtlinie, um der CopyBackup Aktion für den Sicherungskopievorgang Berechtigungen zu erteilen. Sie geben die Aktion im Action Feld der Richtlinie an, und Sie geben den Ressourcenwert im Resource Feld der Richtlinie an, wie im folgenden Beispiel.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "fsx:CopyBackup",
      "Resource": "arn:aws:fsx:*:111122223333:backup/*"
    }
  ]
}
```

Weitere Informationen zu IAM-Richtlinien finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.

Vollständige und inkrementelle Kopien

Wenn Sie ein Backup in ein anderes AWS-Region Backup als das Quell-Backup kopieren, ist die erste Kopie eine vollständige Sicherungskopie. Nach der ersten Sicherungskopie werden alle nachfolgenden Sicherungskopien in dieselbe Zielregion innerhalb desselben AWS Kontos inkrementell ausgeführt, sofern Sie nicht alle zuvor kopierten Backups in dieser Region gelöscht haben und denselben Schlüssel verwendet haben. AWS KMS Wenn beide Bedingungen nicht erfüllt sind, führt der Kopiervorgang zu einer vollständigen (nicht inkrementellen) Sicherungskopie.

Backups werden innerhalb derselben Datei kopiert AWS-Konto

Sie können Backups von FSx for Lustre-Dateisystemen mithilfe der AWS Management Console CLI und der API kopieren, wie in den folgenden Verfahren beschrieben.

Um ein Backup innerhalb desselben Kontos (regionsübergreifend oder regionsübergreifend) mithilfe der Konsole zu kopieren

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Navigationsbereich Sicherungen aus.
3. Wählen Sie in der Tabelle Backups das Backup aus, das Sie kopieren möchten, und wählen Sie dann Backup kopieren aus.

4. Gehen Sie im Abschnitt Settings (Einstellungen) wie folgt vor:
 - Wählen Sie in der Liste Zielregion eine AWS Zielregion aus, in die das Backup kopiert werden soll. Das Ziel kann sich in einer anderen AWS Region (regionsübergreifende Kopie) oder innerhalb derselben AWS Region (regionsinterne Kopie) befinden.
 - (Optional) Wählen Sie „Tags kopieren“, um Tags aus dem Quell-Backup in das Ziel-Backup zu kopieren. Wenn Sie in Schritt 6 „Tags kopieren“ auswählen und auch Tags hinzufügen, werden alle Tags zusammengeführt.
5. Wählen Sie unter Verschlüsselung den AWS KMS Verschlüsselungsschlüssel aus, um das kopierte Backup zu verschlüsseln.
6. Geben Sie unter Tags — optional einen Schlüssel und einen Wert ein, um Tags für Ihr kopiertes Backup hinzuzufügen. Wenn Sie hier Tags hinzufügen und in Schritt 4 auch Tags kopieren ausgewählt haben, werden alle Tags zusammengeführt.
7. Klicken Sie auf Copy backup (Backup kopieren).

Ihr Backup wird innerhalb desselben in AWS-Konto das ausgewählte kopiert AWS-Region.

Um ein Backup innerhalb desselben Kontos (regionsübergreifend oder regionsübergreifend) mit der CLI zu kopieren

- Verwenden Sie den `copy-backup` CLI-Befehl oder die [CopyBackup](#) API-Operation, um ein Backup innerhalb desselben AWS Kontos zu kopieren, entweder innerhalb einer AWS Region oder innerhalb einer AWS Region.

Der folgende Befehl kopiert ein Backup mit der ID `backup-0abc123456789cba7` aus der `us-east-1` Region.

```
aws fsx copy-backup \  
  --source-backup-id backup-0abc123456789cba7 \  
  --source-region us-east-1
```

Die Antwort enthält die Beschreibung des kopierten Backups.

Sie können Ihre Backups auf der Amazon FSx-Konsole oder programmgesteuert mit dem `describe-backups` CLI-Befehl oder der [DescribeBackups](#) API-Operation anzeigen.

Backups wiederherstellen

Sie können ein verfügbares Backup verwenden, um ein neues Dateisystem zu erstellen und so einen point-in-time Snapshot eines anderen Dateisystems wiederherzustellen. Sie können ein Backup mithilfe der Konsole oder eines der AWS SDKs wiederherstellen. AWS CLI Das Wiederherstellen eines Backups in einem neuen Dateisystem dauert genauso lange wie das Erstellen eines neuen Dateisystems. Die aus dem Backup wiederhergestellten Daten werden verzögert in das Dateisystem geladen. Während dieser Zeit kommt es zu einer etwas höheren Latenz.

Das folgende Verfahren führt Sie durch die Wiederherstellung eines Backups mithilfe der Konsole, um ein neues Dateisystem zu erstellen.

Note

Sie können Ihr Backup nur auf einem Dateisystem wiederherstellen, das denselben Lustre-Versionstyp, denselben Bereitstellungstyp, denselben Durchsatz pro Speichereinheit, dieselbe Speicherkapazität, denselben Datenkomprimierungstyp und dieselbe AWS Region aufweist wie das Original. Sie können die Speicherkapazität Ihres wiederhergestellten Dateisystems erhöhen, sobald es verfügbar ist. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#).

So stellen Sie ein Dateisystem aus einer Sicherung wieder her

1. [Öffnen Sie die Amazon FSx for Lustre-Konsole unter https://console.aws.amazon.com/fsx/](https://console.aws.amazon.com/fsx/).
2. Wählen Sie im Konsolen-Dashboard in der linken Navigationsleiste Backups aus.
3. Wählen Sie in der Tabelle Backups das Backup aus, das Sie wiederherstellen möchten, und wählen Sie dann Backup wiederherstellen aus.

Dadurch wird der Assistent zum Erstellen von Dateisystemen geöffnet. Dieser Assistent ist mit dem Standardassistenten für die Erstellung von Dateisystemen identisch, mit Ausnahme der Dateisystemkonfiguration (z. B. Bereitstellungstyp, Durchsatz pro Speichereinheit). Sie können jedoch die zugehörigen VPC- und Backup-Einstellungen ändern.

4. Führen Sie den Assistenten genauso aus, wie Sie es beim Erstellen eines neuen Dateisystems tun.
5. Wählen Sie Review and create.

6. Überprüfen Sie die Einstellungen, die Sie für Ihr Amazon FSx for Lustre-Dateisystem ausgewählt haben, und wählen Sie dann Dateisystem erstellen.

Sie haben die Daten aus einem Backup wiederhergestellt und ein neues Dateisystem wird gerade erstellt. Wenn sich der Status auf ändertAVAILABLE, können Sie das Dateisystem wie gewohnt verwenden.

Löschen eines Backups

Das Löschen eines Backups ist eine permanente, nicht wiederherstellbare Aktion. Alle Daten in einem gelöschten Backup werden ebenfalls gelöscht. Löschen Sie kein Backup, es sei denn, Sie sind sich sicher, dass Sie dieses Backup in future nicht mehr benötigen werden. Sie können keine Backups löschen, die AWS Backup in der Amazon FSx-Konsole, CLI oder API erstellt wurden.

So löschen Sie ein Backup

1. [Öffnen Sie die Amazon FSx for Lustre-Konsole unter https://console.aws.amazon.com/fsx/](https://console.aws.amazon.com/fsx/).
2. Wählen Sie im Konsolen-Dashboard in der linken Navigationsleiste Backups aus.
3. Wählen Sie in der Tabelle Backups das Backup aus, das Sie löschen möchten, und wählen Sie dann Backup löschen aus.
4. Vergewissern Sie sich im sich öffnenden Dialogfeld „Backups löschen“, dass die ID des Backups das Backup identifiziert, das Sie löschen möchten.
5. Vergewissern Sie sich, dass das Kontrollkästchen für das Backup, das Sie löschen möchten, aktiviert ist.
6. Wählen Sie Backups löschen.

Ihr Backup und alle enthaltenen Daten sind jetzt dauerhaft und unwiederbringlich gelöscht.

Speicherkontingente

Sie können Speicherkontingente für Benutzer, Gruppen und Projekte auf FSx for Lustre-Dateisystemen erstellen. Mit Speicherkontingenten können Sie den Speicherplatz und die Anzahl der Dateien, die ein Benutzer, eine Gruppe oder ein Projekt verbrauchen kann, begrenzen. Speicherkontingente verfolgen automatisch die Nutzung auf Benutzer-, Gruppen- und Projektebene, sodass Sie den Verbrauch überwachen können, unabhängig davon, ob Sie Speicherlimits festlegen oder nicht.

Amazon FSx setzt Kontingente durch und verhindert, dass Benutzer, die diese überschritten haben, auf den Speicherplatz schreiben. Wenn Benutzer ihre Kontingente überschreiten, müssen sie genügend Dateien löschen, um die Kontingentgrenzen zu unterschreiten, sodass sie wieder in das Dateisystem schreiben können.

Themen

- [Durchsetzung von Kontingenten](#)
- [Arten von Kontingenten](#)
- [Kontingentgrenzen und Übergangsfristen](#)
- [Kontingente festlegen und anzeigen](#)
- [Kontingente und mit Amazon S3 verknüpfte Buckets](#)
- [Kontingente und Wiederherstellung von Backups](#)

Durchsetzung von Kontingenten

Die Durchsetzung von Benutzer-, Gruppen- und Projektkontingenten wird automatisch auf allen FSx for Lustre-Dateisystemen aktiviert. Sie können die Durchsetzung von Kontingenten nicht deaktivieren.

Arten von Kontingenten

Systemadministratoren mit AWS Root-Benutzeranmeldedaten können die folgenden Arten von Kontingenten erstellen:

- Ein Benutzerkontingent gilt für einen einzelnen Benutzer. Ein Benutzerkontingent für einen bestimmten Benutzer kann sich von den Kontingenten anderer Benutzer unterscheiden.
- Ein Gruppenkontingent gilt für alle Benutzer, die Mitglieder einer bestimmten Gruppe sind.
- Ein Projektkontingent gilt für alle Dateien oder Verzeichnisse, die einem Projekt zugeordnet sind. Ein Projekt kann mehrere Verzeichnisse oder einzelne Dateien enthalten, die sich in verschiedenen Verzeichnissen innerhalb eines Dateisystems befinden.

Note

Projektkontingente werden nur in Lustre-Version 2.15 auf FSx for Lustre-Dateisystemen unterstützt.

- Ein Blockkontingent begrenzt den Speicherplatz, den ein Benutzer, eine Gruppe oder ein Projekt belegen kann. Sie konfigurieren die Speichergröße in Kilobyte.
- Ein Inode-Kontingent begrenzt die Anzahl der Dateien oder Verzeichnisse, die ein Benutzer, eine Gruppe oder ein Projekt erstellen kann. Sie konfigurieren die maximale Anzahl von Inodes als Ganzzahl.

Note

Standardkontingente werden nicht unterstützt.

Wenn Sie Kontingente für einen bestimmten Benutzer und eine Gruppe festlegen und der Benutzer Mitglied dieser Gruppe ist, gilt die Datennutzung des Benutzers für beide Kontingente. Es ist auch durch beide Kontingente begrenzt. Wenn eine der Kontingentgrenzen erreicht wird, wird der Benutzer daran gehindert, in das Dateisystem zu schreiben.

Note

Für den Root-Benutzer festgelegte Kontingente werden nicht durchgesetzt. In ähnlicher Weise umgeht das Schreiben von Daten als Root-Benutzer mithilfe des `sudo` Befehls die Durchsetzung des Kontingents.

Kontingentgrenzen und Übergangsfristen

Amazon FSx setzt Benutzer-, Gruppen- und Projektkontingente als festes Limit oder als Soft-Limit mit einer konfigurierbaren Kulanzzeit durch.

Das harte Limit ist das absolute Limit. Wenn Benutzer ihr festes Limit überschreiten, schlägt eine Block- oder Inode-Zuweisung fehl und es wird eine Meldung angezeigt, dass das Festplattenkontingent überschritten wurde. Benutzer, die ihr festes Kontingentlimit erreicht haben, müssen genügend Dateien oder Verzeichnisse löschen, um das Kontingentlimit zu unterschreiten, bevor sie wieder in das Dateisystem schreiben können. Wenn ein Kulanzzeitraum festgelegt ist, können Benutzer das Soft-Limit innerhalb des Kulanzzeitraums überschreiten, wenn das Hard-Limit unterschritten wird.

Für Soft-Limits konfigurieren Sie eine Kulanzzeit in Sekunden. Das Soft-Limit muss kleiner als das Hard-Limit sein.

Sie können unterschiedliche Übergangsfristen für Inode- und Blockkontingente festlegen. Sie können auch unterschiedliche Kulanzzeiträume für ein Benutzerkontingent, ein Gruppenkontingent und ein Projektkontingent festlegen. Wenn Benutzer-, Gruppen- und Projektkontingente unterschiedliche Kulanzzeiträume haben, wird das weiche Limit nach Ablauf der Kulanzzeit eines dieser Kontingente in ein festes Limit umgewandelt.

Wenn Benutzer ein Soft-Limit überschreiten, ermöglicht Amazon FSx ihnen, ihr Kontingent weiter zu überschreiten, bis die Kulanzfrist abgelaufen ist oder bis das Hard-Limit erreicht ist. Nach Ablauf der Karenzzeit wird das weiche Limit in ein hartes Limit umgewandelt, und Benutzer werden für weitere Schreibvorgänge gesperrt, bis ihre Speichernutzung wieder unter die definierten Blockkontingent- oder Inode-Kontingentgrenzen fällt. Benutzer erhalten keine Benachrichtigung oder Warnung, wenn die Kulanzfrist beginnt.

Kontingente festlegen und anzeigen

Sie legen Speicherkontingente mithilfe von `lfs` Lustre-Dateisystembefehlen in Ihrem Linux-Terminal fest. Der `lfs setquota` Befehl legt Kontingentgrenzen fest und der `lfs quota` Befehl zeigt Kontingentinformationen an.

Weitere Informationen zu Lustre-Kontingentbefehlen finden Sie im Lustre-Betriebshandbuch auf der [Lustre-Dokumentationswebsite](#).

Festlegung von Benutzer-, Gruppen- und Projektkontingenten

Die Syntax des `setquota` Befehls zum Festlegen von Benutzer-, Gruppen- oder Projektkontingenten lautet wie folgt.

```
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
```

Wobei gilt:

- `-u` oder `--user` gibt einen Benutzer an, für den ein Kontingent festgelegt werden soll.
- `-g` oder `--group` gibt eine Gruppe an, für die ein Kontingent festgelegt werden soll.
- `-p` oder `--project` gibt ein Projekt an, für das ein Kontingent festgelegt werden soll.

- -blegt ein Blockkontingent mit einem weichen Limit fest. -Blegt ein Blockkontingent mit einem festen Limit fest. Sowohl *block_softlimit* als auch *block_hardlimit* werden in Kilobyte ausgedrückt, und der Mindestwert ist 1024 KB.
- -ilegt ein Inode-Kontingent mit einem Soft-Limit fest. -Ilegt ein Inode-Kontingent mit einem festen Limit fest. Sowohl *inode_softlimit* als auch *inode_hardlimit* werden in der Anzahl von Inodes ausgedrückt, und der Mindestwert ist 1024 Inodes.
- *mount_point* ist das Verzeichnis, in dem das Dateisystem eingehängt wurde.

Beispiel für ein Benutzerkontingent: Mit dem folgenden Befehl wird ein Softblock-Limit von 5.000 KB, ein Hardblock-Limit von 8.000 KB, ein Soft-Inode-Limit von 2.000 KB und ein Hard-Inode-Limit von 3.000 KB für das Dateisystem festgelegt, `user1` auf das gemountet ist. `/mnt/fsx`

```
sudo lfs setquota -u user1 -b 5000 -B 8000 -i 2000 -I 3000 /mnt/fsx
```

Beispiel für ein Gruppenkontingent: Mit dem folgenden Befehl wird ein Hardblock-Limit von 100.000 KB für die Gruppe festgelegt, die auf dem Dateisystem benannt ist, `group1` auf das gemountet wurde. `/mnt/fsx`

```
sudo lfs setquota -g group1 -B 100000 /mnt/fsx
```

Beispiel für ein Projektkontingent: Stellen Sie zunächst sicher, dass Sie den `project` Befehl verwendet haben, um die gewünschten Dateien und Verzeichnisse dem Projekt zuzuordnen. Mit dem folgenden Befehl werden beispielsweise alle Dateien und Unterverzeichnisse des `/mnt/fsxfs/dir1` Verzeichnisses dem Projekt zugeordnet, dessen Projekt-ID lautet `100`.

```
sudo lfs project -p 100 -r -s /mnt/fsxfs/dir1
```

Verwenden Sie dann den `setquota` Befehl, um das Projektkontingent festzulegen. Mit dem folgenden Befehl wird ein Softblock-Limit von 307.200 KB, ein Hardblock-Limit von 309.200 KB, ein Soft-Inode-Limit von 10.000 KB und ein Hard-Inode-Limit von 11.000 KB für das Projekt `250` auf dem Dateisystem festgelegt, auf das gemountet ist. `/mnt/fsx`

```
sudo lfs setquota -p 250 -b 307200 -B 309200 -i 10000 -I 11000 /mnt/fsx
```

Kulanzfristen festlegen

Die Standard-Nachfrist beträgt eine Woche. Sie können den Standard-Kulanzzeitraum für Benutzer, Gruppen oder Projekte mithilfe der folgenden Syntax anpassen.

```
lfs setquota -t {-u|-g|-p}
               [-b block_grace]
               [-i inode_grace]
               /mount_point
```

Wobei gilt:

- -t gibt an, dass ein Kulanzzeitraum festgelegt wird.
- -u legt eine Übergangsfrist für alle Benutzer fest.
- -g legt eine Übergangsfrist für alle Gruppen fest.
- -p legt eine Übergangsfrist für alle Projekte fest.
- -b legt eine Übergangsfrist für Blockkontingente fest. -i legt eine Übergangsfrist für Inode-Kontingente fest. Sowohl *block_grace* als auch *inode_grace* werden in ganzzahligen Sekunden oder im folgenden Format ausgedrückt. XXwXXdXXhXXmXXs
- *mount_point* ist das Verzeichnis, in dem das Dateisystem eingehängt wurde.

Mit dem folgenden Befehl werden Übergangsfristen von 1.000 Sekunden für Benutzerblockkontingente und von 1 Woche und 4 Tagen für Benutzer-Inode-Kontingente festgelegt.

```
sudo lfs setquota -t -u -b 1000 -i 1w4d /mnt/fsx
```

Kontingente anzeigen

Der quota Befehl zeigt Informationen zu Benutzerkontingenten, Gruppenkontingenten, Projektkontingenten und Kulanzfristen an.

Befehl „Quota anzeigen“	Kontingentinformatio- nen werden angezeigt
<code>lfs quota /<i>mount_point</i></code>	Allgemeine Kontingentinformatio- nen (Festplattennutzung und Grenzwerte) für den Benutzer,

Befehl „Quota anzeigen“	Kontingentinformationen werden angezeigt
	der den Befehl ausführt, und für die primäre Gruppe des Benutzers.
<pre>lfs quota -u <i>username</i> /<i>mount_point</i></pre>	Allgemeine Kontingentinformat ionen für einen bestimmten Benutzer. Benutzer mit AWS Root-Benutzeranmeldedaten können diesen Befehl für jeden Benutzer ausführen, Benutzer ohne Root-Rechte können diesen Befehl jedoch nicht ausführen, um Kontingen tinformationen über andere Benutzer abzurufen.
<pre>lfs quota -u <i>username</i> -v /<i>mount_point</i></pre>	Allgemeine Kontingentinformat ionen für einen bestimmte n Benutzer und detaillierte Kontingentstatistiken für jedes Object Storage-Ziel (OST) und Metadatenziel (MDT). Benutzer mit AWS Root-Benutzeranmeldedaten können diesen Befehl für jeden Benutzer ausführen, Benutzer ohne Root-Rechte können diesen Befehl jedoch nicht ausführen, um Kontingen tinformationen über andere Benutzer abzurufen.

Befehl „Quota anzeigen“	Kontingentinformationen werden angezeigt
<code>lfs quota -g <i>groupname</i> /<i>mount_point</i></code>	Allgemeine Kontingentinformationen für eine bestimmte Gruppe.
<code>lfs quota -p <i>projectid</i> /<i>mount_point</i></code>	Allgemeine Quoteninformationen für ein bestimmtes Projekt.
<code>lfs quota -t -u /<i>mount_point</i></code>	Übergangszeiten für Benutzerkontingente beim Blockieren und Inoden.
<code>lfs quota -t -g /<i>mount_point</i></code>	Block- und Inode-Übergangszeiten für Gruppenkontingente.
<code>lfs quota -t -p /<i>mount_point</i></code>	Block- und Inode-Übergangszeiten für Projektkontingente.

Kontingente und mit Amazon S3 verknüpfte Buckets

Sie können Ihr FSx for Lustre-Dateisystem mit einem Amazon S3 S3-Daten-Repository verknüpfen. Weitere Informationen finden Sie unter [Ihr Dateisystem mit einem S3-Bucket verknüpfen](#).

Sie können optional einen bestimmten Ordner oder ein Präfix innerhalb eines verknüpften S3-Buckets als Importpfad zu Ihrem Dateisystem wählen. Wenn ein Ordner in Amazon S3 angegeben und von S3 in Ihr Dateisystem importiert wird, werden nur die Daten aus diesem Ordner auf das Kontingent angerechnet. Die Daten des gesamten Buckets werden nicht auf die Kontingentgrenzen angerechnet.

Dateimetadaten in einem verknüpften S3-Bucket werden in einen Ordner importiert, dessen Struktur dem importierten Ordner aus Amazon S3 entspricht. Diese Dateien werden auf die Inode-Kontingente der Benutzer und Gruppen angerechnet, denen die Dateien gehören.

Wenn ein Benutzer eine Datei `hsm_restore` verzögert oder verzögert lädt, wird die volle Größe der Datei auf das Blockkontingent angerechnet, das dem Eigentümer der Datei zugewiesen ist. Wenn Benutzer A beispielsweise eine Datei verzögert lädt, deren Eigentümer Benutzer B ist, werden der Speicherplatz und die Inode-Nutzung auf das Kontingent von Benutzer B angerechnet. Wenn ein Benutzer die Amazon FSx-API verwendet, um eine Datei freizugeben, werden die Daten ebenfalls von den Blockquoten des Benutzers oder der Gruppe befreit, der die Datei gehört.

Da HSM-Wiederherstellungen und verzögertes Laden mit Root-Zugriff ausgeführt werden, umgehen sie die Quotendurchsetzung. Sobald Daten importiert wurden, werden sie auf der Grundlage der in S3 festgelegten Eigentumsrechte dem Benutzer oder der Gruppe angerechnet, was dazu führen kann, dass Benutzer oder Gruppen ihre Blocklimits überschreiten. In diesem Fall müssen sie Dateien freigeben, um wieder in das Dateisystem schreiben zu können.

In ähnlicher Weise erstellen Dateisysteme mit aktiviertem automatischem Import automatisch neue Inodes für Objekte, die zu S3 hinzugefügt wurden. Diese neuen Inodes werden mit Root-Zugriff erstellt und umgehen die Einhaltung von Kontingenten, während sie erstellt werden. Diese neuen Inodes werden auf die Benutzer und Gruppen angerechnet, je nachdem, wem das Objekt in S3 gehört. Wenn diese Benutzer und Gruppen aufgrund der automatischen Importaktivität ihre Inode-Kontingente überschreiten, müssen sie Dateien löschen, um zusätzliche Kapazität freizugeben und ihre Kontingentgrenzen zu unterschreiten.

Kontingente und Wiederherstellung von Backups

Wenn Sie ein Backup wiederherstellen, werden die Kontingenteinstellungen des ursprünglichen Dateisystems im wiederhergestellten Dateisystem implementiert. Wenn beispielsweise Kontingente in Dateisystem A festgelegt sind und Dateisystem B aus einer Sicherung von Dateisystem A erstellt wird, werden die Kontingente von Dateisystem A in Dateisystem B durchgesetzt.

Verwaltung der Speicherkapazität

Sie können die auf Ihrem FSx for Lustre-Dateisystem konfigurierte Speicherkapazität erhöhen, wenn Sie zusätzlichen Speicherplatz und Durchsatz benötigen. Da der Durchsatz eines FSx for Lustre-Dateisystems linear mit der Speicherkapazität skaliert, erzielen Sie auch eine vergleichbare Steigerung der Durchsatzkapazität. Um die Speicherkapazität zu erhöhen, können Sie die Amazon FSx-Konsole, die AWS Command Line Interface (AWS CLI) oder die Amazon FSx-API verwenden.

Wenn Sie eine Aktualisierung der Speicherkapazität Ihres Dateisystems anfordern, fügt Amazon FSx automatisch neue Netzwerk-Dateiserver hinzu und skaliert Ihren Metadatenserver. Während

der Skalierung der Speicherkapazität ist das Dateisystem möglicherweise für einige Minuten nicht verfügbar. Dateioperationen, die von Clients ausgeführt werden, während das Dateisystem nicht verfügbar ist, werden auf transparente Weise wiederholt und sind schließlich erfolgreich, nachdem die Speicherskalierung abgeschlossen ist. Während der Zeit, in der das Dateisystem nicht verfügbar ist, wird der Dateisystemstatus auf gesetzt. UPDATING Sobald die Speicherskalierung abgeschlossen ist, wird der Dateisystemstatus auf gesetztAVAILABLE.

Amazon FSx führt dann einen Speicheroptimierungsprozess durch, der die Daten auf transparente Weise auf die vorhandenen und neu hinzugefügten Dateiserver verteilt. Das Rebalancing wird im Hintergrund durchgeführt, ohne dass die Verfügbarkeit des Dateisystems beeinträchtigt wird. Beim Rebalancing kann es zu einer verminderten Leistung des Dateisystems kommen, da Ressourcen für die Datenverschiebung verbraucht werden. Bei den meisten Dateisystemen dauert die Speicheroptimierung einige Stunden bis zu einigen Tagen. Während der Optimierungsphase können Sie auf Ihr Dateisystem zugreifen und es verwenden.

Sie können den Fortschritt der Speicheroptimierung jederzeit mithilfe der Amazon FSx-Konsole, CLI und API verfolgen. Weitere Informationen finden Sie unter [Überwachung: Die Speicherkapazität steigt](#).

Themen

- [Überlegungen zur Erhöhung der Speicherkapazität](#)
- [Wann sollte die Speicherkapazität erhöht werden](#)
- [Wie werden gleichzeitige Speicherskalierungs- und Backup-Anfragen behandelt](#)
- [Wie erhöht man die Speicherkapazität](#)
- [Überwachung: Die Speicherkapazität steigt](#)

Überlegungen zur Erhöhung der Speicherkapazität

Hier sind einige wichtige Punkte, die Sie bei der Erhöhung der Speicherkapazität berücksichtigen sollten:

- Nur erhöhen — Sie können nur die Speicherkapazität für ein Dateisystem erhöhen; Sie können die Speicherkapazität nicht verringern.
- Inkremente erhöhen — Wenn Sie die Speicherkapazität erhöhen, verwenden Sie die im Dialogfeld Speicherkapazität erhöhen aufgeführten Stufen.

- **Zeit zwischen Erhöhungen** — Sie können die Speicherkapazität in einem Dateisystem erst 6 Stunden nach der Anforderung der letzten Erhöhung weiter erhöhen oder bis der Speicheroptimierungsprozess abgeschlossen ist, je nachdem, welcher Zeitraum länger ist.
- **Durchsatzkapazität** — Sie erhöhen automatisch die Durchsatzkapazität, wenn Sie die Speicherkapazität erhöhen. Bei persistenten HDD-Dateisystemen mit SSD-Cache wird die Lese-Cache-Speicherkapazität ebenfalls erhöht, um einen SSD-Cache aufrechtzuerhalten, der auf 20 Prozent der Festplattenspeicherkapazität ausgelegt ist. Amazon FSx berechnet die neuen Werte für die Speicher- und Durchsatzkapazitätseinheiten und listet sie im Dialogfeld Speicherkapazität erhöhen auf.

Note

Sie können die Durchsatzkapazität eines persistenten SSD-basierten Dateisystems unabhängig ändern, ohne die Speicherkapazität des Dateisystems aktualisieren zu müssen. Weitere Informationen finden Sie unter [Verwaltung der Durchsatzkapazität](#).

- **Bereitstellungstyp** — Sie können die Speicherkapazität aller Bereitstellungstypen mit Ausnahme von Scratch-1-Dateisystemen erhöhen. Wenn Sie ein Scratch-1-Dateisystem haben, können Sie ein neues mit einer größeren Speicherkapazität erstellen.

Wann sollte die Speicherkapazität erhöht werden

Erhöhen Sie die Speicherkapazität Ihres Dateisystems, wenn die freie Speicherkapazität knapp wird. Verwenden Sie die `FreeStorageCapacity` CloudWatch Metrik, um die Menge an freiem Speicherplatz zu überwachen, der im Dateisystem verfügbar ist. Sie können einen CloudWatch Amazon-Alarm für diese Metrik erstellen und sich benachrichtigen lassen, wenn sie einen bestimmten Schwellenwert unterschreitet. Weitere Informationen finden Sie unter [Überwachung mit Amazon CloudWatch](#).

Sie können CloudWatch Metriken verwenden, um die laufende Durchsatznutzung Ihres Dateisystems zu überwachen. Wenn Sie feststellen, dass Ihr Dateisystem eine höhere Durchsatzkapazität benötigt, können Sie anhand der Metrikinformationen entscheiden, um wie viel die Speicherkapazität erhöht werden soll. Informationen darüber, wie Sie den aktuellen Durchsatz Ihres Dateisystems ermitteln können, finden Sie unter [So verwenden Sie Amazon FSx for Lustre-Metriken](#). Informationen darüber, wie sich die Speicherkapazität auf die Durchsatzkapazität auswirkt, finden Sie unter [Leistung von Amazon FSx for Lustre](#).

Sie können die Speicherkapazität und den Gesamtdurchsatz Ihres Dateisystems auch im Bereich Zusammenfassung auf der Seite mit den Dateisystemdetails einsehen.

Wie werden gleichzeitige Speicherskalierungs- und Backup-Anfragen behandelt

Sie können ein Backup anfordern, kurz bevor ein Speicherskalierungs-Workflow beginnt oder während dieser ausgeführt wird. Die Reihenfolge, in der Amazon FSx die beiden Anfragen verarbeitet, ist wie folgt:

- Wenn ein Speicherskalierungs-Workflow läuft (Speicherskalierungsstatus ist `IN_PROGRESS` und Dateisystemstatus ist `UPDATING`) und Sie ein Backup anfordern, wird die Backup-Anfrage in die Warteschlange gestellt. Die Backup-Aufgabe wird gestartet, wenn sich die Speicherskalierung in der Speicheroptimierungsphase befindet (der Speicherskalierungsstatus ist `UPDATED_OPTIMIZING` und der Dateisystemstatus ist `AVAILABLE`).
- Wenn das Backup gerade läuft (Backup-Status ist `CREATING`) und Sie eine Speicherskalierung anfordern, wird die Speicherskalierungsanforderung in die Warteschlange gestellt. Der Speicherskalierungs-Workflow wird gestartet, wenn Amazon FSx das Backup auf Amazon S3 überträgt (Backup-Status ist `TRANSFERRING`).

Wenn eine Speicherskalierungsanforderung aussteht und auch eine Dateisystem-Backup-Anfrage aussteht, hat die Backup-Aufgabe eine höhere Priorität. Die Speicherskalierungsaufgabe wird erst gestartet, wenn die Sicherungsaufgabe abgeschlossen ist.

Wie erhöht man die Speicherkapazität

Sie können die Speicherkapazität eines Dateisystems mithilfe der Amazon FSx-Konsole AWS CLI, der oder der Amazon FSx-API erhöhen.

Um die Speicherkapazität für ein Dateisystem (Konsole) zu erhöhen

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Lustre-Dateisystem aus, für das Sie die Speicherkapazität erhöhen möchten.
3. Wählen Sie unter Aktionen die Option Speicherkapazität aktualisieren aus. Oder wählen Sie im Übersichtsbereich neben der Speicherkapazität des Dateisystems die Option Aktualisieren aus, um das Dialogfeld „Speicherkapazität erhöhen“ anzuzeigen.

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. Geben Sie für Gewünschte Speicherkapazität eine neue Speicherkapazität in GiB an, die größer ist als die aktuelle Speicherkapazität des Dateisystems:
 - Für ein persistentes SSD- oder Scratch-2-Dateisystem muss dieser Wert ein Vielfaches von 2400 GiB sein.
 - Für ein persistentes HDD-Dateisystem muss dieser Wert ein Vielfaches von 6000 GiB für 12 MB/s/TiB-Dateisysteme und ein Vielfaches von 1800 GiB für 40 MB/s/TiB-Dateisysteme sein.

 Note

Sie können die Speicherkapazität von Scratch-1-Dateisystemen nicht erhöhen.

5. Wählen Sie Update, um die Aktualisierung der Speicherkapazität zu starten.
6. Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme auf der Registerkarte Updates überwachen.

Um die Speicherkapazität für ein Dateisystem (CLI) zu erhöhen

1. Verwenden Sie den Befehl, um die Speicherkapazität für ein FSx for Lustre-Dateisystem zu erhöhen. AWS CLI [update-file-system](#) Legen Sie die folgenden Parameter fest:

Geben Sie `--file-system-id` die ID des Dateisystems ein, das Sie aktualisieren.

Auf `--storage-capacity` einen ganzzahligen Wert gesetzt, der den Betrag der Erhöhung der Speicherkapazität in GiB angibt. Für ein persistentes SSD- oder Scratch-2-Dateisystem muss dieser Wert ein Vielfaches von 2400 sein. Für ein persistentes HDD-Dateisystem muss dieser Wert ein Vielfaches von 6000 für Dateisysteme mit 12 MB/s/TiB und ein Vielfaches von 1800 für Dateisysteme mit 40 MB/s/TiB sein. Der neue Zielwert muss größer als die aktuelle Speicherkapazität des Dateisystems sein.

Dieser Befehl gibt einen Zielwert für die Speicherkapazität von 9600 GiB für ein persistentes SSD- oder Scratch-2-Dateisystem an.

```
$ aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --storage-capacity 9600
```

2. Sie können den Fortschritt des Updates mithilfe des AWS CLI Befehls [describe-file-systems](#) überwachen. Suchen Sie `administrative-actions` in der Ausgabe nach dem.

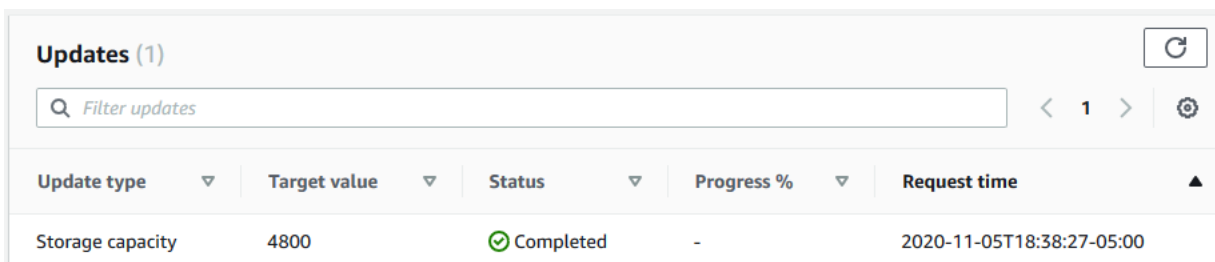
Weitere Informationen finden Sie unter [AdministrativeAction](#).

Überwachung: Die Speicherkapazität steigt

Sie können den Fortschritt einer Erhöhung der Speicherkapazität mithilfe der Amazon FSx-Konsole, der API oder der AWS CLI überwachen.

Überwachung von Zunahmen in der Konsole

Auf der Registerkarte Updates auf der Seite mit den Dateisystemdetails können Sie die 10 neuesten Updates für jeden Updatetyp einsehen.



Update type	Target value	Status	Progress %	Request time
Storage capacity	4800	Completed	-	2020-11-05T18:38:27-05:00

Sie können die folgenden Informationen einsehen:

Art der Aktualisierung

Unterstützte Typen sind Speicherkapazität und Speicheroptimierung.

Zielwert

Der gewünschte Wert, auf den die Speicherkapazität des Dateisystems aktualisiert werden soll.

Status

Der aktuelle Status der Speicherkapazität wird aktualisiert. Die möglichen Werte lauten wie folgt:

- **Ausstehend** — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.
- **In Bearbeitung** — Amazon FSx verarbeitet die Aktualisierungsanfrage.
- **Aktualisiert; Optimierung** — Amazon FSx hat die Speicherkapazität des Dateisystems erhöht. Bei der Speicheroptimierung werden nun die Daten auf den Dateiservern neu verteilt.
- **Abgeschlossen** — Die Erhöhung der Speicherkapazität wurde erfolgreich abgeschlossen.
- **Fehlgeschlagen** — Die Erhöhung der Speicherkapazität ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Informationen darüber zu erhalten, warum das Speicherupdate fehlgeschlagen ist.

Fortschritt%

Zeigt den Fortschritt des Speicheroptimierungsprozesses in Prozent als abgeschlossen an.

Uhrzeit der Anfrage

Der Zeitpunkt, zu dem Amazon FSx die Anfrage zur Aktualisierungsaktion erhalten hat.

Die Überwachung nimmt mit der API AWS CLI und zu

Mithilfe des [describe-file-systems](#) AWS CLI Befehls und der [DescribeFileSystems](#) API-Aktion können Sie Anfragen zur Erhöhung der Speicherkapazität des Dateisystems anzeigen und überwachen. Das `AdministrativeActions` Array listet die 10 letzten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die Speicherkapazität eines Dateisystems erhöhen, `AdministrativeActions` werden zwei generiert: eine Aktion `FILE_SYSTEM_UPDATE` und eine `STORAGE_OPTIMIZATION` Aktion.

Das folgende Beispiel zeigt einen Auszug der Antwort auf einen `describe-file-systems` CLI-Befehl. Das Dateisystem hat eine Speicherkapazität von 4800 GB, und eine Verwaltungsmaßnahme zur Erhöhung der Speicherkapazität auf 9600 GB steht noch aus.


```
{
  "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 verarbeitet die `FILE_SYSTEM_UPDATE` Aktion zuerst und fügt dem Dateisystem neue Dateiserver hinzu. Wenn der neue Speicher für das Dateisystem verfügbar ist, ändert sich der `FILE_SYSTEM_UPDATE` Status auf `UPDATED_OPTIMIZING`. Die Speicherkapazität zeigt den neuen größeren Wert an und Amazon FSx beginnt mit der Verarbeitung der `STORAGE_OPTIMIZATION` administrativen Aktion. Dies wird im folgenden Auszug aus der Antwort auf einen `describe-file-systems` CLI-Befehl gezeigt.

Die `ProgressPercent` Eigenschaft zeigt den Fortschritt des Speicheroptimierungsprozesses an. Nachdem der Speicheroptimierungsprozess erfolgreich abgeschlossen wurde, ändert sich der Status der `FILE_SYSTEM_UPDATE` Aktion in `COMPLETED`, und die `STORAGE_OPTIMIZATION` Aktion wird nicht mehr angezeigt.

```
{
  "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,
  }
]

```

Wenn die Erhöhung der Speicherkapazität fehlschlägt, ändert sich der Status der FILE_SYSTEM_UPDATE Aktion in FAILED. Die FailureDetails Eigenschaft enthält Informationen über den Fehler, wie im folgenden Beispiel dargestellt.

```

{
  "FileSystems": [
    {
      "OwnerId": "111122223333",
      .
      .
      .
      "StorageCapacity": 4800,
      "AdministrativeActions": [
        {
          "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
          "FailureDetails": {
            "Message": "string"
          },
          "RequestTime": 1581694764.757,
          "Status": "FAILED",
          "TargetFileSystemValues":
            "StorageCapacity": 9600
        }
      ]
    }
  ]
}

```

```
] }  
]
```

Verwaltung der Metadaten-Performance

Sie können die Metadatenkonfiguration Ihres FSx for Lustre-Dateisystems aktualisieren, ohne Ihre Endbenutzer oder Anwendungen zu stören, indem Sie die Amazon FSx-Konsole, die Amazon FSx-API oder () verwenden. AWS Command Line Interface AWS CLI Das Aktualisierungsverfahren erhöht die Anzahl der bereitgestellten Metadaten-IOPS für Ihr Dateisystem.

Note

Sie können die Metadaten-Performance nur auf FSx for Lustre-Dateisystemen erhöhen, die mit dem Bereitstellungstyp Persistent_2 und einer angegebenen Metadatenkonfiguration erstellt wurden.

Die erhöhte Metadaten-Performance Ihres Dateisystems ist innerhalb weniger Minuten einsatzbereit. Sie können die Leistung der Metadaten jederzeit aktualisieren, sofern die Anfragen zur Steigerung der Metadatenleistung mindestens 6 Stunden auseinander liegen. Während der Skalierung der Metadatenleistung ist das Dateisystem möglicherweise für einige Minuten nicht verfügbar. Dateioperationen, die von Clients ausgeführt werden, während das Dateisystem nicht verfügbar ist, werden auf transparente Weise wiederholt und sind schließlich erfolgreich, wenn die Skalierung der Metadaten-Leistung abgeschlossen ist. Die Leistungssteigerung der neuen Metadaten wird Ihnen in Rechnung gestellt, sobald sie Ihnen zur Verfügung steht.

Sie können den Fortschritt einer Leistungssteigerung bei Metadaten jederzeit mithilfe der Amazon FSx-Konsole, CLI und API verfolgen. Weitere Informationen finden Sie unter [Überwachung von Aktualisierungen der Metadaten-Konfiguration](#).

Themen

- [Leistungskonfiguration für Lustre-Metadaten](#)
- [Überlegungen zur Steigerung der Metadaten-Performance](#)
- [Wann sollte die Leistung von Metadaten erhöht werden](#)
- [Wie kann die Leistung von Metadaten gesteigert werden](#)
- [Ändern des Metadaten-Konfigurationsmodus](#)

- [Überwachung von Aktualisierungen der Metadaten-Konfiguration](#)

Leistungskonfiguration für Lustre-Metadaten

Die Anzahl der bereitgestellten Metadaten-IOPS bestimmt die maximale Rate an Metadatenoperationen, die vom Dateisystem unterstützt werden können.

Wenn Sie das Dateisystem erstellen, wählen Sie einen von zwei Metadaten-Konfigurationsmodi: Automatisch oder Benutzerbereitgestellt:

- Im automatischen Modus stellt Amazon FSx automatisch die Anzahl der Metadaten-IOPS in Ihrem Dateisystem bereit und skaliert sie auf der Grundlage der Speicherkapazität Ihres Dateisystems.
- Im vom Benutzer bereitgestellten Modus geben Sie die Anzahl der Metadaten-IOPS an, die für Ihr Dateisystem bereitgestellt werden sollen.

Sie können jederzeit vom automatischen Modus in den vom Benutzer bereitgestellten Modus wechseln. Sie können auch vom Modus „Benutzerbereitgestellt“ in den Modus „Automatisch“ wechseln, wenn die Anzahl der in Ihrem Dateisystem bereitgestellten Metadaten-IOPS mit der Standardanzahl der im automatischen Modus bereitgestellten Metadaten-IOPS übereinstimmt.

Gültige IOPS-Werte für Metadaten sind 1500, 3000, 6000, 12000 und Vielfache von 12000 bis zu einem Maximum von 192000. Jeder IOPS-Wert für 12000 Metadaten erfordert eine IP-Adresse innerhalb des Subnetzes, in dem sich Ihr Dateisystem befindet.

Die Standardanzahl der im automatischen Modus bereitgestellten Metadaten-IOPS hängt von der Kapazität Ihres Dateisystems ab. [In dieser Tabelle](#) finden Sie Informationen zur Standardanzahl von Metadaten-IOPS, die basierend auf der Speicherkapazität des Dateisystems bereitgestellt werden.

Wenn die Metadaten-Performance Ihres Workloads die Anzahl der im automatischen Modus bereitgestellten Metadaten-IOPS übersteigt, können Sie den vom Benutzer bereitgestellten Modus verwenden, um den Metadaten-IOPS-Wert für Ihr Dateisystem zu erhöhen.

Sie können den aktuellen Wert der Metadaten-serverkonfiguration des Dateisystems wie folgt anzeigen:

- Mithilfe der Konsole — Im Bereich Zusammenfassung der Seite mit den Dateisystemdetails werden im Feld Metadaten-IOPS der aktuelle Wert der bereitgestellten Metadaten-IOPS und der aktuelle Metadaten-Konfigurationsmodus (entweder Automatisch oder Benutzerbereitgestellt) des Dateisystems angezeigt.

- Verwenden der CLI oder API — Verwenden Sie den CLI-Befehl [describe-file-systems](#) oder den [DescribeFileSystems-API-Vorgang](#) und suchen Sie nach der Eigenschaft `MetadataConfiguration`

Überlegungen zur Steigerung der Metadaten-Performance

Im Folgenden sind einige wichtige Überlegungen zur Steigerung der Leistung Ihrer Metadaten aufgeführt:

- Nur Steigerung der Metadaten-Performance — Sie können nur die Anzahl der Metadaten-IOPS für ein Dateisystem erhöhen; Sie können die Anzahl der Metadaten-IOPS nicht verringern.
- Die Angabe von Metadaten-IOPS im Automatikmodus wird nicht unterstützt — Sie können die Anzahl der Metadaten-IOPS in einem Dateisystem, das sich im automatischen Modus befindet, nicht angeben. Sie müssen in den vom Benutzer bereitgestellten Modus wechseln und dann die Anfrage stellen. Weitere Informationen finden Sie unter [Ändern des Metadaten-Konfigurationsmodus](#).
- Zeit zwischen Erhöhungen — Sie können die Leistung von Metadaten in einem Dateisystem erst 6 Stunden, nachdem die letzte Erhöhung angefordert wurde, weiter erhöhen.
- Gleichzeitige Erhöhung der Metadatenleistung und Erhöhung des SSD-Speichers — Sie können die Metadatenleistung und die Speicherkapazität des Dateisystems nicht gleichzeitig skalieren.

Wann sollte die Leistung von Metadaten erhöht werden

Erhöhen Sie die Anzahl der Metadaten-IOPS, wenn Sie Workloads ausführen müssen, die eine höhere Metadaten-Performance erfordern als die, die standardmäßig in Ihrem Dateisystem bereitgestellt wird. Sie können die Leistung Ihrer Metadaten AWS Management Console anhand des `Metadata IOPS Utilization` Diagramms überwachen, das den Prozentsatz der Leistung des bereitgestellten Metadaten-servers angibt, den Sie in Ihrem Dateisystem verbrauchen.

Sie können die Leistung Ihrer Metadaten auch anhand CloudWatch detaillierterer Messwerte überwachen. CloudWatch Zu den Metriken gehören `DiskReadOperations` und `DiskWriteOperations`, die das Volumen der Metadaten-Serveroperationen angeben, für die Festplatten-E/A erforderlich ist, sowie detaillierte Metriken für Metadatenvorgänge, einschließlich Datei- und Verzeichniserstellung, Statistiken, Lese- und Löschvorgänge. Weitere Informationen finden Sie unter [Metriken für Metadaten des Dateisystems](#).

Wie kann die Leistung von Metadaten gesteigert werden

Sie können die Metadaten-Performance eines Dateisystems erhöhen, indem Sie die Amazon FSx-Konsole AWS CLI, die oder die Amazon FSx-API verwenden.

Um die Leistung von Metadaten für ein Dateisystem (Konsole) zu erhöhen

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im linken Navigationsbereich die Option Dateisysteme aus. Wählen Sie in der Liste Dateisysteme das FSx for Lustre-Dateisystem aus, für das Sie die Metadaten-Performance erhöhen möchten.
3. Wählen Sie für Aktionen die Option Metadaten IOPS aktualisieren aus. Oder wählen Sie im Übersichtsbereich neben dem Feld Metadaten-IOPS des Dateisystems die Option Aktualisieren aus.

Das Dialogfeld „Metadaten-IOPS aktualisieren“ wird angezeigt.

4. Wählen Sie Vom Benutzer bereitgestellt aus.
5. Wählen Sie für Desired Metadata IOPS den neuen Metadaten-IOPS-Wert aus. Gültige Werte sind 1500, 3000, 6000, 12000, und Vielfache von 12000 bis zu einem Maximum von 192000. Der eingegebene Wert muss größer oder gleich dem aktuellen IOPS-Wert für Metadaten sein.
6. Wählen Sie Aktualisieren.

Um die Metadatenleistung für ein Dateisystem (CLI) zu erhöhen

Um die Metadaten-Performance für ein FSx for Lustre-Dateisystem zu erhöhen, verwenden Sie den AWS CLI Befehl [update-file-system](#) (UpdateFileSystem entspricht der API-Aktion). Legen Sie die folgenden Parameter fest:

- Geben Sie `--file-system-id` die ID des Dateisystems ein, das Sie aktualisieren.
- Verwenden Sie die `--lustre-configuration MetadataConfiguration` Eigenschaft, um die Leistung Ihrer Metadaten zu erhöhen. Diese Eigenschaft hat zwei Parameter `Mode` und `Iops`.
 1. Wenn sich Ihr Dateisystem im Modus `USER_PROVISIONED` befindet, `Mode` ist die Verwendung optional (falls verwendet, auf `gesetztMode`). `USER_PROVISIONED`

Wenn sich Ihr Dateisystem im `AUTOMATIC`-Modus befindet, legen Sie den Wert `Mode` auf `USER_PROVISIONED` fest (wodurch der Dateisystemmodus auf `USER_PROVISIONED` umgeschaltet wird und zusätzlich der IOPS-Wert für Metadaten erhöht wird).

2. Legen Iops Sie einen Wert von 1500, 3000, 6000, 12000, oder ein Vielfaches von 12000 bis zu einem Maximum von fest. 192000. Der eingegebene Wert muss größer oder gleich dem aktuellen IOPS-Wert für Metadaten sein.

Im folgenden Beispiel werden die bereitgestellten Metadaten-IOPS auf 96000 aktualisiert.

```
aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --lustre-configuration 'MetadataConfiguration={Mode=USER_PROVISIONED,Iops=96000}'
```

Ändern des Metadaten-Konfigurationsmodus

Sie können den Metadaten-Konfigurationsmodus eines vorhandenen Dateisystems mithilfe der AWS Konsole und der CLI ändern, wie in den folgenden Verfahren beschrieben.

Wenn Sie vom automatischen Modus in den vom Benutzer bereitgestellten Modus wechseln, müssen Sie einen Metadaten-IOPS-Wert angeben, der größer oder gleich dem aktuellen IOPS-Wert für Metadaten des Dateisystems ist.

Wenn Sie vom Modus Benutzerbereitgestellt in den automatischen Modus wechseln möchten und der aktuelle Metadaten-IOPS-Wert höher als der automatisierte Standard ist, lehnt Amazon FSx die Anfrage ab, da das Herunterskalieren von Metadaten-IOPS nicht unterstützt wird. Um den Moduswechsel zu entsperren, müssen Sie die Speicherkapazität so erhöhen, dass sie Ihren aktuellen Metadaten-IOPS im automatischen Modus entspricht, um den Moduswechsel wieder zu aktivieren.

Sie können den Metadaten-Konfigurationsmodus eines Dateisystems ändern, indem Sie die Amazon FSx-Konsole, AWS CLI, die oder die Amazon FSx-API verwenden.

Um den Metadaten-Konfigurationsmodus für ein Dateisystem (Konsole) zu ändern

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im linken Navigationsbereich die Option Dateisysteme aus. Wählen Sie in der Liste Dateisysteme das FSx for Lustre-Dateisystem aus, für das Sie den Metadaten-Konfigurationsmodus ändern möchten.
3. Wählen Sie für Aktionen die Option Metadata IOPS aktualisieren aus. Oder wählen Sie im Übersichtsbereich neben dem Feld Metadaten-IOPS des Dateisystems die Option Aktualisieren aus.

Das Dialogfeld „Metadaten-IOPS aktualisieren“ wird angezeigt.

4. Führen Sie eine der folgenden Aufgaben aus.
 - Um vom vom Benutzer bereitgestellten Modus in den automatischen Modus zu wechseln, wählen Sie Automatisch.
 - Um vom automatischen Modus in den vom Benutzer bereitgestellten Modus zu wechseln, wählen Sie Benutzerbereitgestellt. Geben Sie dann für Desired Metadata IOPS einen Metadaten-IOPS-Wert an, der größer oder gleich dem aktuellen IOPS-Wert für Metadaten im Dateisystem ist.
5. Wählen Sie Aktualisieren.

So ändern Sie den Metadaten-Konfigurationsmodus für ein Dateisystem (CLI)

Um den Metadaten-Konfigurationsmodus für ein FSx for Lustre-Dateisystem zu ändern, verwenden Sie den AWS CLI Befehl [update-file-system](#) (UpdateFileSystem entspricht der API-Aktion). Legen Sie die folgenden Parameter fest:

- Geben Sie `--file-system-id` die ID des Dateisystems ein, das Sie aktualisieren.
- Verwenden Sie die `--lustre-configuration` `MetadataConfiguration` Eigenschaft, um den Metadaten-Konfigurationsmodus zu ändern. Diese Eigenschaft hat zwei Parameter `Mode` und `Iops`.
- Um vom Modus `AUTOMATIC` in den Modus `USER_PROVISIONED` zu wechseln, legen Sie `Mode` einen Metadaten-IOPS-Wert fest, der größer oder gleich dem aktuellen IOPS-Wert für Metadaten im Dateisystem ist. `USER_PROVISIONED` Iops Beispielsweise:

```
aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --lustre-configuration  
  'MetadataConfiguration={Mode=USER_PROVISIONED,Iops=96000}'
```

- Um vom Modus `USER_PROVISIONED` in den Modus `AUTOMATIC` zu wechseln, stellen Sie den Parameter auf ein und verwenden Sie `Mode` ihn nicht. `AUTOMATIC` Iops Beispielsweise:

```
aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --lustre-configuration 'MetadataConfiguration={Mode=AUTOMATIC}'
```


Überwachung von Aktualisierungen der Metadaten-Konfiguration

Sie können den Fortschritt der Aktualisierungen der Metadaten-Konfiguration mithilfe der Amazon FSx-Konsole, der API oder der AWS CLI überwachen.

Überwachung der Aktualisierungen der Metadaten-Konfiguration (Konsole)

Sie können Aktualisierungen der Metadatenkonfiguration auf der Registerkarte Updates auf der Seite mit den Dateisystemdetails überwachen.

Für Aktualisierungen der Metadaten-Konfiguration können Sie die folgenden Informationen einsehen:

Art des Updates

Unterstützte Typen sind Metadaten-IOPS und Metadaten-Konfigurationsmodus.

Zielwert

Der aktualisierte Wert für den Metadaten-IOPS- oder Metadaten-Konfigurationsmodus des Dateisystems.

Status

Der aktuelle Status des Updates. Die möglichen Werte lauten wie folgt:

- Ausstehend — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.
- In Bearbeitung — Amazon FSx verarbeitet die Aktualisierungsanfrage.
- Abgeschlossen — Das Update wurde erfolgreich abgeschlossen.
- Fehlgeschlagen — Die Aktualisierungsanforderung ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Details darüber zu sehen, warum die Anfrage fehlgeschlagen ist.

Uhrzeit der Anfrage

Der Zeitpunkt, zu dem Amazon FSx die Anfrage zur Aktualisierungsaktion erhalten hat.

Überwachung von Metadaten-Konfigurationsupdates (CLI)

[Sie können Anfragen zur Aktualisierung der Metadatenkonfiguration mithilfe des AWS CLI Befehls `describe-file-systems` und der `Systems-API-Operation` anzeigen und überwachen.](#)

[DescribeFile](#) Das `AdministrativeActions` Array listet die 10 neuesten Aktualisierungsaktionen

für jeden administrativen Aktionstyp auf. Wenn Sie die Metadaten-Performance oder den Metadaten-Konfigurationsmodus eines Dateisystems aktualisieren, `FILE_SYSTEM_UPDATE` AdministrativeActions wird ein generiert.

Das folgende Beispiel zeigt einen Auszug der Antwort auf einen `describe-file-systems` CLI-Befehl. Im Dateisystem steht eine Verwaltungsaktion zur Erhöhung der Metadaten-IOPS auf 96000 und des Metadaten-Konfigurationsmodus auf `USER_PROVISIONED` aus.

```
"AdministrativeActions": [  
  {  
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",  
    "RequestTime": 1678840205.853,  
    "Status": "PENDING",  
    "TargetFileSystemValues": {  
      "LustreConfiguration": {  
        "MetadataConfiguration": {  
          "Iops": 96000,  
          "Mode": USER_PROVISIONED  
        }  
      }  
    }  
  }  
]
```

Amazon FSx verarbeitet die `FILE_SYSTEM_UPDATE` Aktion und ändert die Metadaten-IOPS und den Metadaten-Konfigurationsmodus des Dateisystems. Wenn die neuen Metadatenressourcen für das Dateisystem verfügbar sind, ändert sich der `FILE_SYSTEM_UPDATE` Status in `COMPLETED`

Wenn die Anforderung zur Aktualisierung der Metadatenkonfiguration fehlschlägt, ändert sich der Status der `FILE_SYSTEM_UPDATE` Aktion auf `FAILED`, wie im folgenden Beispiel gezeigt. Die `FailureDetails` Eigenschaft stellt Informationen über den Fehler bereit.

```
"AdministrativeActions": [  
  {  
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",  
    "RequestTime": 1678840205.853,  
    "Status": "FAILED",  
    "TargetFileSystemValues": {  
      "LustreConfiguration": {  
        "MetadataConfiguration": {  
          "Iops": 96000,  
          "Mode": USER_PROVISIONED  
        }  
      }  
    }  
  }  
]
```

```
        "Mode": USER_PROVISIONED
      }
    },
    "FailureDetails": {
      "Message": "failure-message"
    }
  }
]
```

Verwaltung der Durchsatzkapazität

Jedes FSx for Lustre-Dateisystem hat eine Durchsatzkapazität, die bei der Erstellung des Dateisystems konfiguriert wird. Der Durchsatz eines Dateisystems FSx for Lustre wird in Megabyte pro Sekunde gemessen. pro Tebibyte (MB/s/TiB). Die Durchsatzkapazität ist ein Faktor, der die Geschwindigkeit bestimmt, mit der der Dateiserver, der das Dateisystem hostet, Dateidaten bereitstellen kann. Höhere Durchsatzkapazitäten bedeuten auch höhere I/O-Operationen pro Sekunde (IOPS) und mehr Speicher für das Zwischenspeichern von Daten auf dem Dateiserver. Weitere Informationen finden Sie unter [Leistung von Amazon FSx for Lustre](#).

Sie können die Durchsatzstufe eines persistenten SSD-basierten Dateisystems ändern, indem Sie den Wert des Dateisystemdurchsatzes pro Speichereinheit erhöhen oder verringern. Gültige Werte hängen wie folgt vom Bereitstellungstyp des Dateisystems ab:

- Für SSD-basierte Bereitstellungstypen Persistent_1 sind die gültigen Werte 50, 100 und 200 MB/s/TiB gültig.
- Für Persistent_2 SSD-basierte Bereitstellungstypen sind gültige Werte 125, 250, 500 und 1000 MB/s/TiB.

Sie können den aktuellen Wert des Durchsatzes des Dateisystems pro Speichereinheit wie folgt anzeigen:

- Mithilfe der Konsole — Im Bereich Zusammenfassung der Seite mit den Dateisystemdetails wird im Feld Durchsatz pro Speichereinheit der aktuelle Wert angezeigt.
- Verwenden der CLI oder API — Verwenden Sie den [describe-file-systems](#) CLI-Befehl oder die [DescribeFileSystems](#) API-Operation und suchen Sie nach der `PerUnitStorageThroughput` Eigenschaft.

Wenn Sie die Durchsatzkapazität Ihres Dateisystems ändern, schaltet Amazon FSx im Hintergrund die Dateiserver des Dateisystems aus. Ihr Dateisystem wird während der Skalierung der Durchsatzkapazität für einige Minuten nicht verfügbar sein. Die neue Menge an Durchsatzkapazität wird Ihnen in Rechnung gestellt, sobald sie für Ihr Dateisystem verfügbar ist.

Themen

- [Überlegungen zur Aktualisierung der Durchsatzkapazität](#)
- [Wann muss die Durchsatzkapazität geändert werden](#)
- [Wie ändert man die Durchsatzkapazität](#)
- [Überwachung von Änderungen der Durchsatzkapazität](#)

Überlegungen zur Aktualisierung der Durchsatzkapazität

Hier sind einige wichtige Punkte, die Sie bei der Aktualisierung der Durchsatzkapazität berücksichtigen sollten:

- Erhöhen oder verringern — Sie können die Durchsatzkapazität für ein Dateisystem erhöhen oder verringern.
- Inkremente aktualisieren — Wenn Sie die Durchsatzkapazität ändern, verwenden Sie die Inkremente, die im Dialogfeld Durchsatzstufe aktualisieren aufgeführt sind.
- Zeit zwischen Erhöhungen — Weitere Änderungen der Durchsatzkapazität in einem Dateisystem können Sie erst 6 Stunden nach der letzten Anforderung oder bis zum Abschluss der Durchsatzoptimierung vornehmen, je nachdem, welcher Zeitraum länger ist.
- Bereitstellungstyp — Sie können die Durchsatzkapazität nur persistenter SSD-basierter Bereitstellungstypen aktualisieren.

Wann muss die Durchsatzkapazität geändert werden

Amazon FSx ist in Amazon integriert CloudWatch, sodass Sie die laufende Durchsatznutzung Ihres Dateisystems überwachen können. Die Leistung (Durchsatz und IOPS), die Sie über Ihr Dateisystem erzielen können, hängt neben der Durchsatzkapazität, der Speicherkapazität und dem Speichertyp Ihres Dateisystems von den Merkmalen Ihres spezifischen Workloads ab. Informationen darüber, wie Sie den aktuellen Durchsatz Ihres Dateisystems ermitteln können, finden Sie unter [So verwenden Sie Amazon FSx for Lustre-Metriken](#). Informationen zu CloudWatch Metriken finden Sie unter [Überwachung mit Amazon CloudWatch](#).

Wie ändert man die Durchsatzkapazität

Sie können die Durchsatzkapazität eines Dateisystems mithilfe der Amazon FSx-Konsole, der AWS Command Line Interface (AWS CLI) oder der Amazon FSx-API ändern.

Um die Durchsatzkapazität eines Dateisystems zu ändern (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das FSx for Lustre-Dateisystem aus, für das Sie die Durchsatzkapazität ändern möchten.
3. Wählen Sie für Aktionen die Option Durchsatzstufe aktualisieren aus. Oder wählen Sie im Bereich „Zusammenfassung“ neben „Durchsatz pro Speichereinheit“ des Dateisystems die Option „Aktualisieren“ aus.

Das Fenster Durchsatzstufe aktualisieren wird angezeigt.

4. Wählen Sie den neuen Wert für Gewünschter Durchsatz pro Speichereinheit aus der Liste aus.

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. Wählen Sie Update, um die Aktualisierung der Durchsatzkapazität zu starten.

Note

Ihr Dateisystem kann während des Updates für einen sehr kurzen Zeitraum nicht verfügbar sein.

So ändern Sie die Durchsatzkapazität (CLI) eines Dateisystems

- Verwenden Sie den [update-file-system](#) CLI-Befehl (oder die entsprechende [UpdateFileSystem](#) API-Operation), um die Durchsatzkapazität eines Dateisystems zu ändern. Legen Sie die folgenden Parameter fest:
 - Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.
 - Auf `--lustre-configuration PerUnitStorageThroughput` einen Wert von `50 100` oder `200` MB/s/TiB für `Persistent_1` SSD-Dateisysteme oder auf einen Wert von `125`, oder MB/s/TiB für `Persistent_2` SSD-Dateisysteme setzen. `250 500 1000`

Dieser Befehl gibt an, dass die Durchsatzkapazität für das Dateisystem auf 1000 MB/s/TiB festgelegt wird.

```
aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --lustre-configuration PerUnitStorageThroughput=1000
```

Überwachung von Änderungen der Durchsatzkapazität

Sie können den Fortschritt einer Änderung der Durchsatzkapazität mithilfe der Amazon FSx-Konsole, der API und der AWS CLI überwachen.

Überwachung von Änderungen der Durchsatzkapazität (Konsole)

Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.

- Auf der Registerkarte Updates auf der Seite mit den Dateisystemdetails können Sie die 10 neuesten Aktualisierungsaktionen für jeden Aktualisierungstyp einsehen.

Updates (1) ↻				
<input type="text" value="Filter updates"/> < 1 > ⚙				
Update type	Target value	Status	Progress %	Request time
Per unit storage throughput	500	✔ Completed	-	2023-11-07T15:32:41-05:00

Informationen zu Aktionen zur Aktualisierung der Durchsatzkapazität finden Sie in den folgenden Informationen.

Art der Aktualisierung

Der unterstützte Typ ist Speicherdurchsatz pro Einheit.

Zielwert

Der gewünschte Wert, auf den der Durchsatz des Dateisystems pro Speichereinheit geändert werden soll.

Status

Der aktuelle Status des Updates. Für Aktualisierungen der Durchsatzkapazität sind die folgenden Werte möglich:

- **Ausstehend** — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.
- **In Bearbeitung** — Amazon FSx verarbeitet die Aktualisierungsanfrage.
- **Aktualisiert; Optimierung** — Amazon FSx hat die Netzwerk-I/O-, CPU- und Speicherressourcen des Dateisystems aktualisiert. Die neue Festplatten-I/O-Leistungsstufe ist für Schreibvorgänge verfügbar. Bei Ihren Lesevorgängen liegt die Festplatten-I/O-Leistung zwischen der vorherigen Stufe und der neuen Stufe, bis sich Ihr Dateisystem nicht mehr in diesem Zustand befindet.
- **Abgeschlossen** — Die Aktualisierung der Durchsatzkapazität wurde erfolgreich abgeschlossen.
- **Fehlgeschlagen** — Die Aktualisierung der Durchsatzkapazität ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Einzelheiten darüber zu erhalten, warum die Durchsatzaktualisierung fehlgeschlagen ist.

Uhrzeit der Anfrage

Der Zeitpunkt, zu dem Amazon FSx die Aktualisierungsanfrage erhalten hat.

Überwachung von Dateisystem-Updates (CLI)

- Sie können Anfragen zur Änderung der Kapazität des Dateisystemdurchsatzes mithilfe des [describe-file-systems](#) CLI-Befehls und der [DescribeFileSystems](#) API-Aktion anzeigen und überwachen. Das `AdministrativeActions` Array listet die 10 neuesten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die Durchsatzkapazität eines Dateisystems ändern, wird eine `FILE_SYSTEM_UPDATE` Verwaltungsaktion generiert.

Das folgende Beispiel zeigt den Antwortausschnitt eines `describe-file-systems` CLI-Befehls. Das Dateisystem hat einen Zieldurchsatz pro Speichereinheit von 500 MB/s/TiB.

```
.  
. .  
.  
"AdministrativeActions": [  
  {  
    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",  
    "RequestTime": 1581694764.757,  
    "Status": "PENDING",  
    "TargetFileSystemValues": {  
      "LustreConfiguration": {  
        "PerUnitStorageThroughput": 500  
      }  
    }  
  }  
]
```

Wenn Amazon FSx die Aktion erfolgreich verarbeitet, ändert sich der Status in `COMPLETED`. Die neue Durchsatzkapazität ist dann für das Dateisystem verfügbar und wird in der `PerUnitStorageThroughput` Eigenschaft angezeigt.

Wenn die Änderung der Durchsatzkapazität fehlschlägt, ändert sich der Status in `FAILED`, und die `FailureDetails` Eigenschaft enthält Informationen über den Fehler.

Lustre-Datenkomprimierung

Sie können die Lustre-Datenkomprimierungsfunktion verwenden, um Kosteneinsparungen bei Ihren leistungsstarken Amazon FSx for Lustre-Dateisystemen und Backup-Speichern zu erzielen. Wenn

die Datenkomprimierung aktiviert ist, komprimiert Amazon FSx for Lustre neu geschriebene Dateien automatisch, bevor sie auf die Festplatte geschrieben werden, und dekomprimiert sie automatisch, wenn sie gelesen werden.

Die Datenkomprimierung verwendet den LZ4-Algorithmus, der für ein hohes Maß an Komprimierung optimiert ist, ohne die Leistung des Dateisystems zu beeinträchtigen. LZ4 ist ein von der Lustre-Community vertrauenswürdiger und leistungsorientierter Algorithmus, der ein Gleichgewicht zwischen Komprimierungsgeschwindigkeit und komprimierter Dateigröße bietet. Die Aktivierung der Datenkomprimierung hat in der Regel keine messbaren Auswirkungen auf die Latenz.

Die Datenkomprimierung reduziert die Datenmenge, die zwischen Amazon FSx for Lustre-Dateiservern und Speicher übertragen wird. Wenn Sie noch keine komprimierten Dateiformate verwenden, werden Sie bei Verwendung der Datenkomprimierung einen Anstieg der Gesamtdurchsatzkapazität des Dateisystems feststellen. Erhöhungen der Durchsatzkapazität im Zusammenhang mit der Datenkomprimierung werden begrenzt, wenn Sie Ihre Front-End-Netzwerkschnittstellenkarten voll ausgelastet haben.

Wenn es sich bei Ihrem Dateisystem beispielsweise um einen PERSISTENT-50-SSD-Bereitstellungstyp handelt, hat Ihr Netzwerkdurchsatz einen Basiswert von 250 MB/s pro TiB Speicher. Ihr Festplattendurchsatz hat einen Basiswert von 50 MB/s pro TiB. Durch Datenkomprimierung könnte Ihr Festplattendurchsatz von 50 MB/s pro TiB auf maximal 250 MB/s pro TiB steigen, was die grundlegende Netzwerkdurchsatzgrenze darstellt. Weitere Informationen zu den Netzwerk- und Festplattendurchsatzgrenzen finden Sie in den Leistungstabellen für Dateisysteme unter [Aggregierte Dateisystemleistung](#). Weitere Informationen zur Datenkomprimierungsleistung finden Sie im Beitrag [Weniger ausgeben und gleichzeitig die Leistung mit Amazon FSx for Lustre-Datenkomprimierung steigern](#) im AWS Storage Blog.

Themen

- [Verwaltung der Datenkomprimierung](#)
- [Komprimieren zuvor geschriebener Dateien](#)
- [Dateigrößen anzeigen](#)
- [Metriken verwenden CloudWatch](#)

Verwaltung der Datenkomprimierung

Sie können die Datenkomprimierung ein- oder ausschalten, wenn Sie ein neues Amazon FSx for Lustre-Dateisystem erstellen. Die Datenkomprimierung ist standardmäßig deaktiviert, wenn Sie ein Amazon FSx for Lustre-Dateisystem über die Konsole oder API AWS CLI erstellen.

Um die Datenkomprimierung beim Erstellen eines Dateisystems (Konsole) zu aktivieren

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, das [Erstellen Sie Ihr FSx for Lustre-Dateisystem](#) im Abschnitt Erste Schritte beschrieben ist.
3. Wählen Sie im Abschnitt Dateisystemdetails für Datenkomprimierungstyp die Option LZ4 aus.
4. Führen Sie den Assistenten genauso aus, wie Sie es beim Erstellen eines neuen Dateisystems tun.
5. Wählen Sie Review and create.
6. Überprüfen Sie die Einstellungen, die Sie für Ihr Amazon FSx for Lustre-Dateisystem ausgewählt haben, und wählen Sie dann Dateisystem erstellen.

Wenn das Dateisystem verfügbar ist, ist die Datenkomprimierung aktiviert.

So aktivieren Sie die Datenkomprimierung beim Erstellen eines Dateisystems (CLI)

- Um ein FSx for Lustre-Dateisystem mit aktivierter Datenkomprimierung zu erstellen, verwenden Sie den Amazon FSx CLI-Befehl [create-file-system](#) mit dem `DataCompressionType` Parameter, wie unten gezeigt. Die entsprechende API-Operation ist [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
```

Nach erfolgreicher Erstellung des Dateisystems gibt Amazon FSx die Dateisystembeschreibung als JSON zurück, wie im folgenden Beispiel gezeigt.

```
{
  "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
      }
    }
  ]
}
```

Sie können auch die Datenkomprimierungskonfiguration Ihrer vorhandenen Dateisysteme ändern. Wenn Sie die Datenkomprimierung für ein vorhandenes Dateisystem aktivieren, werden nur neu

geschriebene Dateien komprimiert und vorhandene Dateien werden nicht komprimiert. Weitere Informationen finden Sie unter [Komprimieren zuvor geschriebener Dateien](#).

Um die Datenkomprimierung auf einem vorhandenen Dateisystem (Konsole) zu aktualisieren

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Lustre-Dateisystem aus, für das Sie die Datenkomprimierung verwalten möchten.
3. Wählen Sie für Aktionen die Option Datenkomprimierungstyp aktualisieren aus.
4. Wählen Sie im Dialogfeld Datenkomprimierungstyp aktualisieren die Option LZ4 aus, um die Datenkomprimierung zu aktivieren, oder wählen Sie KEINE, um sie zu deaktivieren.
5. Wählen Sie Aktualisieren.
6. Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme auf der Registerkarte Updates überwachen.

So aktualisieren Sie die Datenkomprimierung auf einem vorhandenen Dateisystem (CLI)

Verwenden Sie den Befehl, um die Datenkomprimierungskonfiguration für ein vorhandenes FSx for Lustre-Dateisystem zu aktualisieren. AWS CLI [update-file-system](#) Legen Sie die folgenden Parameter fest:

- Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.
- Legt fest `--lustre-configuration DataCompressionType`, NONE ob die Datenkomprimierung ausgeschaltet oder LZ4 die Datenkomprimierung mit dem LZ4-Algorithmus aktiviert werden soll.

Dieser Befehl gibt an, dass die Datenkomprimierung mit dem LZ4-Algorithmus aktiviert ist.

```
$ aws fsx update-file-system \  
  --file-system-id fs-0123456789abcdef0 \  
  --lustre-configuration DataCompressionType=LZ4
```

Konfiguration der Datenkomprimierung beim Erstellen eines Dateisystems aus einer Sicherungskopie

Sie können ein verfügbares Backup verwenden, um ein neues Amazon FSx for Lustre-Dateisystem zu erstellen. Wenn Sie aus einem Backup ein neues Dateisystem erstellen, müssen Sie das

nicht angeben. Die `DataCompressionType` Einstellung wird anhand der Backup-Einstellung angewendet. `DataCompressionType` Wenn Sie `DataCompressionType` bei der Erstellung aus einer Sicherungskopie die angeben, muss der Wert mit der `DataCompressionType` Einstellung der Sicherung übereinstimmen.

Um die Einstellungen eines Backups anzuzeigen, wählen Sie es auf der Registerkarte Backups der Amazon FSx-Konsole aus. Details des Backups werden auf der Übersichtsseite für das Backup aufgeführt. Sie können den [describe-backups](#) AWS CLI Befehl auch ausführen (die entsprechende API-Aktion ist [DescribeBackups](#)).

Komprimieren zuvor geschriebener Dateien

Dateien sind unkomprimiert, wenn sie erstellt wurden, als die Datenkomprimierung auf dem Amazon FSx for Lustre-Dateisystem ausgeschaltet war. Wenn Sie die Datenkomprimierung aktivieren, werden Ihre vorhandenen unkomprimierten Daten nicht automatisch komprimiert.

Sie können den `lfs_migrate` Befehl verwenden, der als Teil der Lustre-Client-Installation installiert ist, um vorhandene Dateien zu komprimieren. Ein Beispiel finden Sie unter [FSXL-Komprimierung](#), verfügbar unter [GitHub](#)

Dateigrößen anzeigen

Sie können die folgenden Befehle verwenden, um die unkomprimierten und komprimierten Größen Ihrer Dateien und Verzeichnisse anzuzeigen.

- `du` zeigt komprimierte Größen an.
- `du --apparent-size` zeigt unkomprimierte Größen an.
- `ls -l` zeigt unkomprimierte Größen an.

Die folgenden Beispiele zeigen die Ausgabe der einzelnen Befehle mit derselben Datei.

```
$ 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
```

Die `-h` Option ist für diese Befehle nützlich, da sie Größen in einem für Menschen lesbaren Format ausgibt.

Metriken verwenden CloudWatch

Sie können Amazon CloudWatch Logs-Metriken verwenden, um Ihre Dateisystemnutzung einzusehen. Die `LogicalDiskUsage` Metrik zeigt die gesamte logische Festplattennutzung (ohne Komprimierung), und die `PhysicalDiskUsage` Metrik zeigt die gesamte physische Festplattennutzung (mit Komprimierung). Diese beiden Messwerte sind nur verfügbar, wenn in Ihrem Dateisystem die Datenkomprimierung aktiviert ist oder sie zuvor aktiviert war.

Sie können das Komprimierungsverhältnis Ihres Dateisystems ermitteln, indem Sie den Wert `Sum` der `LogicalDiskUsage` Statistik durch den Wert `Sum` der `PhysicalDiskUsage` Statistik dividieren. Hinweise zur Verwendung metrischer Mathematik zur Berechnung dieses Verhältnisses finden Sie unter [Metrische Mathematik: Datenkomprimierungsverhältnis](#)

Weitere Informationen zur Überwachung der Leistung Ihres Dateisystems finden Sie unter [Überwachung von Amazon FSx for Lustre](#).

Lustre-Wurzelkürbis

Root Squash ist eine Verwaltungsfunktion, die zusätzlich zur aktuellen netzwerkbasierten Zugriffskontrolle und den POSIX-Dateiberechtigungen eine zusätzliche Ebene der Dateizugriffskontrolle hinzufügt. Mithilfe der Root-Squash-Funktion können Sie den Zugriff auf Root-Ebene von Clients einschränken, die versuchen, als Root auf Ihr FSx for Lustre-Dateisystem zuzugreifen.

Root-Benutzerberechtigungen sind erforderlich, um administrative Aktionen durchzuführen, wie z. B. die Verwaltung von Berechtigungen auf FSx for Lustre-Dateisystemen. Der Root-Zugriff bietet den Benutzern jedoch uneingeschränkten Zugriff, sodass sie Berechtigungsprüfungen umgehen können, um auf Dateisystemobjekte zuzugreifen, sie zu ändern oder zu löschen. Mithilfe der Root-Squash-Funktion können Sie den unbefugten Zugriff auf oder das Löschen von Daten verhindern, indem Sie eine Benutzer-ID (UID) und Gruppen-ID (GID) für Ihr Dateisystem angeben, die keine Root-Rechte haben. Root-Benutzer, die auf das Dateisystem zugreifen, werden automatisch in den angegebenen Benutzer/die angegebene Gruppe mit eingeschränkten Rechten umgewandelt, die vom Speicheradministrator festgelegt werden.

Mit der Root-Squash-Funktion können Sie optional auch eine Liste von Clients bereitstellen, die von der Root-Squash-Einstellung nicht betroffen sind. Diese Clients können als Root-Benutzer mit uneingeschränkten Rechten auf das Dateisystem zugreifen.

Themen

- [Wie funktioniert Root Squash](#)
- [Root Squash verwalten](#)

Wie funktioniert Root Squash

Die Root-Squash-Funktion funktioniert, indem sie die Benutzer-ID (UID) und Gruppen-ID (GID) des Root-Benutzers einer vom Lustre-Systemadministrator angegebenen UID und GID neu zuordnet. Mit der Root-Squash-Funktion können Sie optional auch eine Gruppe von Clients angeben, für die eine erneute Zuordnung von UID/GID nicht gilt.

Wenn Sie ein neues FSx for Lustre-Dateisystem erstellen, ist Root-Squash standardmäßig deaktiviert. Sie aktivieren Root-Squash, indem Sie eine UID- und GID-Root-Squash-Einstellung für Ihr FSx for Lustre-Dateisystem konfigurieren. Die UID- und GID-Werte sind ganze Zahlen, die zwischen 0 und 4294967294 liegen können: 0 4294967294

- Ein Wert ungleich Null für UID und GID aktiviert Root-Squash. Die UID- und GID-Werte können unterschiedlich sein, aber jeder Wert muss ungleich Null sein.
- Ein Wert von 0 (Null) für UID und GID gibt Root an und deaktiviert daher Root-Squash.

Während der Erstellung des Dateisystems können Sie die Amazon FSx-Konsole verwenden, um die Root-Squash-UID- und GID-Werte in der Root Squash-Eigenschaft anzugeben, wie unter [Um Root Squash beim Erstellen eines Dateisystems \(Konsole\) zu aktivieren](#) gezeigt. Sie können den RootSquash Parameter auch mit der API AWS CLI oder verwenden, um die UID- und GID-Werte bereitzustellen, wie unter [So aktivieren Sie Root Squash beim Erstellen eines Dateisystems \(CLI\)](#) gezeigt.

Optional können Sie auch eine Liste mit NIDs von Clients angeben, für die Root-Squash nicht gilt. Eine Client-NID ist eine Lustre-Netzwerkennung, die zur eindeutigen Identifizierung eines Clients verwendet wird. Sie können die NID entweder als einzelne Adresse oder als Adressbereich angeben:

- Eine einzelne Adresse wird im Standard-Lustre-NID-Format beschrieben, indem die IP-Adresse des Clients gefolgt von der Lustre-Netzwerk-ID angegeben wird (z. B.). 10.0.1.6@tcp

- Ein Adressbereich wird beschrieben, indem der Bereich durch einen Bindestrich getrennt wird (z. B.). `10.0.[2-10].[1-255]@tcp`
- Wenn Sie keine Client-NIDs angeben, gibt es keine Ausnahmen für Root-Squash.

Wenn Sie Ihr Dateisystem erstellen oder aktualisieren, können Sie die Eigenschaft Exceptions to Root Squash in der Amazon FSx-Konsole verwenden, um die Liste der Client-NIDs bereitzustellen. Verwenden Sie in der API AWS CLI oder den Parameter. `NoSquashNids` Weitere Informationen finden Sie in den Verfahren unter [Root Squash verwalten](#).

Note

Root Squash wird für Backups und Wiederherstellungen nicht unterstützt. Um Backups und Wiederherstellungen verwenden zu können, müssen Sie Root Squash deaktivieren, indem Sie den `RootSquashNoSquashNids` Parameter auf `0:0` und den Parameter auf `[]` mit der AWS CLI oder API setzen oder indem Sie im Dialogfeld Root Squash-Einstellungen aktualisieren in der Amazon FSx-Konsole Deaktivieren wählen.

Root Squash verwalten

Bei der Erstellung des Dateisystems ist Root-Squash standardmäßig deaktiviert. Sie können Root Squash aktivieren, wenn Sie ein neues Amazon FSx for Lustre-Dateisystem über die Amazon FSx-Konsole oder API erstellen. AWS CLI

Um Root Squash beim Erstellen eines Dateisystems (Konsole) zu aktivieren

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, das [Erstellen Sie Ihr FSx for Lustre-Dateisystem](#) im Abschnitt Erste Schritte beschrieben ist.
3. Öffnen Sie den Abschnitt Root Squash — optional.

4. Geben Sie für Root Squash die Benutzer- und Gruppen-IDs an, mit denen der Root-Benutzer auf das Dateisystem zugreifen kann. Sie können eine beliebige ganze Zahl im Bereich von 1 — 4294967294 angeben:
 1. Geben Sie unter Benutzer-ID die Benutzer-ID an, die der Root-Benutzer verwenden soll.
 2. Geben Sie unter Gruppen-ID die Gruppen-ID an, die der Root-Benutzer verwenden soll.
5. (Optional) Gehen Sie für Ausnahmen von Root Squash wie folgt vor:
 1. Wählen Sie „Kundenadresse hinzufügen“.
 2. Geben Sie im Feld Clientadressen die IP-Adresse eines Clients an, für den Root Squash nicht gilt. Informationen zum IP-Adressformat finden Sie unter [Wie funktioniert Root Squash](#).
 3. Wiederholen Sie den Vorgang nach Bedarf, um weitere Client-IP-Adressen hinzuzufügen.
6. Führen Sie den Assistenten wie beim Erstellen eines neuen Dateisystems aus.
7. Wählen Sie Review and create.
8. Überprüfen Sie die Einstellungen, die Sie für Ihr Amazon FSx for Lustre-Dateisystem ausgewählt haben, und wählen Sie dann Dateisystem erstellen.

Wenn das Dateisystem verfügbar ist, ist Root-Squash aktiviert.

So aktivieren Sie Root Squash beim Erstellen eines Dateisystems (CLI)

- Um ein FSx for Lustre-Dateisystem mit aktiviertem Root-Squash zu erstellen, verwenden Sie den Amazon FSx CLI-Befehl [create-file-system](#) mit dem Parameter `RootSquashConfiguration`. Die entsprechende API-Operation ist [CreateFileSystem](#).

Stellen Sie für den `RootSquashConfiguration` Parameter die folgenden Optionen ein:

- **RootSquash**— Die durch Doppelpunkte getrennten UID:GID-Werte, die die Benutzer-ID und Gruppen-ID angeben, die der Root-Benutzer verwenden soll. Sie können für jede ID eine ganze Zahl im Bereich von 0 — 4294967294 (0 ist Stamm) angeben (z. B.). 65534:65534
- **NoSquashNids**— Geben Sie die Lustre-Netzwerkennungen (NIDs) von Clients an, für die Root Squash nicht gilt. Informationen zum Client-NID-Format finden Sie unter. [Wie funktioniert Root Squash](#)

Das folgende Beispiel erstellt ein FSx for Lustre-Dateisystem mit aktiviertem Root-Squash:

```
$ 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
```

Nach erfolgreicher Erstellung des Dateisystems gibt Amazon FSx die Dateisystembeschreibung als JSON zurück, wie im folgenden Beispiel gezeigt.

```
{  
  
  "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"
        }
    }
}
]
}

```

Sie können auch die Root-Squash-Einstellungen Ihres vorhandenen Dateisystems mithilfe der Amazon FSx-Konsole oder API AWS CLI aktualisieren. Sie können beispielsweise die Root-Squash-UID- und GID-Werte ändern, Client-NIDs hinzufügen oder entfernen oder Root-Squash deaktivieren.

Um die Root-Squash-Einstellungen auf einem vorhandenen Dateisystem (Konsole) zu aktualisieren

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Lustre-Dateisystem aus, für das Sie Root-Squash verwalten möchten.
3. Wählen Sie unter Aktionen die Option Root Squash aktualisieren aus. Oder wählen Sie im Übersichtsfenster neben dem Root-Squash-Feld des Dateisystems die Option „Aktualisieren“, um das Dialogfeld „Root-Squash-Einstellungen aktualisieren“ zu öffnen.

Update Root Squash Settings ✕

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 Group ID

Exceptions to Root Squash
Specify the NID range of the clients to which root squash does not apply.

Client addresses

4. Aktualisieren Sie für Root Squash die Benutzer- und Gruppen-IDs, mit denen der Root-Benutzer auf das Dateisystem zugreifen kann. Sie können eine beliebige ganze Zahl im Bereich von 0 — 4294967294 angeben. Um Root Squash zu deaktivieren, geben Sie 0 (Null) für beide IDs an.
 1. Geben Sie unter Benutzer-ID die Benutzer-ID an, die der Root-Benutzer verwenden soll.
 2. Geben Sie unter Gruppen-ID die Gruppen-ID an, die der Root-Benutzer verwenden soll.
5. Gehen Sie für Ausnahmen von Root Squash wie folgt vor:
 1. Wählen Sie Kundenadresse hinzufügen.
 2. Geben Sie im Feld Client-Adressen die IP-Adresse eines Clients an, für den Root Squash nicht gilt.
 3. Wiederholen Sie den Vorgang nach Bedarf, um weitere Client-IP-Adressen hinzuzufügen.
6. Wählen Sie Aktualisieren.

Note

Wenn Root Squash aktiviert ist und Sie es deaktivieren möchten, wählen Sie Deaktivieren, anstatt die Schritte 4-6 auszuführen.

Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme auf der Registerkarte Updates überwachen.

So aktualisieren Sie die Root-Squash-Einstellungen auf einem vorhandenen Dateisystem (CLI)

Verwenden Sie den Befehl, um die Root-Squash-Einstellungen für ein vorhandenes FSx for Lustre-Dateisystem zu aktualisieren. AWS CLI [update-file-system](#) Die entsprechende API-Operation ist [UpdateFileSystem](#)

Legen Sie die folgenden Parameter fest:

- Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.
- Stellen Sie die `--lustre-configuration` `RootSquashConfiguration` Optionen wie folgt ein:
 - `RootSquash`— Legt die durch Doppelpunkte getrennten UID:GID-Werte fest, die die Benutzer-ID und Gruppen-ID angeben, die der Root-Benutzer verwenden soll. Sie können für jede ID eine ganze Zahl im Bereich von 0 — 4294967294 (0 ist Stamm) angeben. Um Root-Squash zu deaktivieren, geben Sie `0:0` für die UID:GID-Werte an.
 - `NoSquashNids`— Geben Sie die Lustre-Netzwerkennungen (NIDs) von Clients an, für die Root-Squash nicht gilt. Wird verwendet[], um alle Client-NIDs zu entfernen, was bedeutet, dass es keine Ausnahmen für Root-Squash gibt.

Dieser Befehl gibt an, dass Root-Squash aktiviert ist, indem er 65534 als Wert für die Benutzer-ID und Gruppen-ID des Root-Benutzers verwendet wird.

```
$ 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"]}
```

Wenn der Befehl erfolgreich ist, gibt Amazon FSx for Lustre die Antwort im JSON-Format zurück.

Sie können die Root-Squash-Einstellungen Ihres Dateisystems im Übersichtsbereich der Dateisystemdetailseite auf der Amazon FSx-Konsole oder in der Antwort auf einen [describe-file-systems](#) CLI-Befehl (die entsprechende API-Aktion ist [DescribeFileSystems](#)) einsehen.

Status des Dateisystems FSx for Lustre

Sie können den Status eines Amazon FSx-Dateisystems mithilfe der Amazon FSx-Konsole, des AWS CLI Befehls `describe-file-systems` oder der API-Betriebssysteme anzeigen. [DescribeFile](#)

Status des Dateisystems	Beschreibung
VERFÜGBAR	Das Dateisystem befindet sich in einem fehlerfreien Zustand und ist erreichbar und kann verwendet werden.
WIRD ERSTELLT	Amazon FSx erstellt ein neues Dateisystem.
WIRD GELÖSCHT	Amazon FSx löscht ein vorhandenes Dateisystem.
WIRD AKTUALISIERT	Das Dateisystem wird derzeit einem vom Kunden initiierten Update unterzogen.
FALSCH KONFIGURIERT	Das Dateisystem befindet sich in einem ausgefallenen, aber wiederherstellbaren Zustand.
FEHLGESCHLAGEN	Dieser Status kann eine der folgenden Bedeutungen haben: <ul style="list-style-type: none"> • Das Dateisystem ist ausgefallen und Amazon FSx kann es nicht wiederherstellen. • Beim Erstellen eines neuen Dateisystems konnte Amazon FSx das Dateisystem nicht erstellen.

Kennzeichnen Sie Ihre Amazon FSx-Ressourcen

Um Ihnen bei der Verwaltung Ihrer Dateisysteme und anderer Amazon FSx for Lustre-Ressourcen zu helfen, können Sie jeder Ressource Ihre eigenen Metadaten in Form von Tags zuweisen. Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie viele Ressourcen desselben Typs haben

— In diesem Fall können Sie schnell bestimmte Ressourcen basierend auf den zugewiesenen Tags (Markierungen) bestimmen. In diesem Thema werden Tags (Markierungen) und deren Erstellung beschrieben.

Themen

- [Grundlagen zu Tags \(Markierungen\)](#)
- [Markieren Ihrer -Ressourcen](#)
- [Tag-Einschränkungen](#)
- [Berechtigungen und Tag](#)

Grundlagen zu Tags (Markierungen)

Ein Tag ist eine Bezeichnung, die Sie einer AWS Ressource zuweisen. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen.

Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Sie könnten beispielsweise eine Reihe von Tags für die Amazon FSx for Lustre-Dateisysteme Ihres Kontos definieren, mit deren Hilfe Sie den Besitzer und die Stack-Ebene jeder Instance verfolgen können.

Wir empfehlen die Verwendung von Tag (Markierung)-Schlüsseln, die die Anforderungen der jeweiligen Ressourcentypen erfüllen. Die Verwendung einheitlicher Tag-Schlüssel vereinfacht das Verwalten der -Ressourcen. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags (Markierungen) filtern und danach suchen.

Tags haben für Amazon FSx keine semantische Bedeutung und werden ausschließlich als Zeichenfolge interpretiert. Außerdem werden Tags (Markierungen) nicht automatisch Ihren Ressourcen zugewiesen. Sie können Tag (Markierung)-Schlüssel und -Werte bearbeiten und Tags (Markierungen) jederzeit von einer Ressource entfernen. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht null festlegen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben. Wenn Sie eine Ressource löschen, werden alle Tags (Markierungen) der Ressource ebenfalls gelöscht.

Wenn Sie die Amazon FSx for Lustre-API, die AWS CLI oder ein AWS SDK verwenden, können Sie die `TagResource` API-Aktion verwenden, um Tags auf bestehende Ressourcen anzuwenden. Zudem können Sie mit einigen Aktionen zur Ressourcenerstellung Tags beim Erstellen einer Ressource angeben. Wenn Tags (Markierungen) nicht während der Ressourcenerstellung

angewendet werden können, wird die Ressourcenerstellung rückgängig gemacht. Auf diese Weise werden Ressourcen entweder mit Tags (Markierungen) oder überhaupt nicht erstellt und keine Ressourcen verbleiben ohne Tags (Markierungen). Indem Sie Ressourcen zum Erstellungszeitpunkt markieren, müssen Sie anschließend keine benutzerdefinierten Skripts ausführen. Weitere Informationen darüber, wie Sie Benutzern ermöglichen, Ressourcen bei der Erstellung zu markieren, finden Sie unter [Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung](#).

Markieren Ihrer -Ressourcen

Sie können Amazon FSx for Lustre-Ressourcen, die in Ihrem Konto vorhanden sind, taggen. Wenn Sie die Amazon FSx-Konsole verwenden, können Sie Tags auf Ressourcen anwenden, indem Sie die Registerkarte Tags auf dem entsprechenden Ressourcenbildschirm verwenden. Wenn Sie Ressourcen erstellen, können Sie den Namensschlüssel mit einem Wert anwenden, und Sie können Tags Ihrer Wahl anwenden, wenn Sie ein neues Dateisystem erstellen. Die Konsole kann Ressourcen nach dem Name-Tag organisieren, aber dieses Tag hat keine semantische Bedeutung für den Amazon FSx for Lustre-Service.

Sie können tagbasierte Berechtigungen auf Ressourcenebene in Ihren IAM-Richtlinien auf Amazon FSx for Lustre-API-Aktionen anwenden, die das Tagging bei der Erstellung unterstützen, um eine detaillierte Kontrolle über die Benutzer und Gruppen zu implementieren, die Ressourcen bei der Erstellung taggen können. Ihre Ressourcen sind ab Erstellung ordnungsgemäß geschützt. Tags (Markierungen) werden direkt auf Ihre Ressourcen angewendet. Daher treten alle Tag (Markierung)-basierten Berechtigungen auf Ressourcenebene, die die Verwendung von Ressourcen steuern, direkt in Kraft. Ihre Ressourcen können nachverfolgt und genauer erfasst werden. Sie können das Markieren neuer Ressourcen gewährleisten und steuern, welche Tag (Markierung)-Schlüssel und Werte für Ihre Ressourcen festgelegt sind.

Sie können in Ihren IAM-Richtlinien auch Berechtigungen auf Ressourcenebene auf die API-Aktionen `TagResource` und `UntagResource` Amazon FSx for Lustre anwenden, um zu kontrollieren, welche Tag-Schlüssel und -Werte für Ihre vorhandenen Ressourcen festgelegt werden.

Weitere Informationen zum Markieren von Ressourcen für die Fakturierung finden Sie unter [Verwendung von Tags \(Markierungen\) zur Kostenzuordnung](#) im Benutzerhandbuch für AWS Billing .

Tag-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags (Markierungen) pro Ressource: 50

- Jeder Tag (Markierung) muss für jede Ressource eindeutig sein. Jeder Tag (Markierung) kann nur einen Wert haben.
- Maximale Schlüssellänge: 128 Unicode-Zeichen in UTF-8
- Maximale Wertlänge: 256 Unicode-Zeichen in UTF-8
- Die zulässigen Zeichen für Amazon FSx for Lustre-Tags sind: Buchstaben, Zahlen und Leerzeichen, die in UTF-8 dargestellt werden können, sowie die folgenden Zeichen: + - =. _:/@.
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Das `aws :` Präfix ist für die Verwendung reserviert. Wenn der Tag (Markierung) über einen Tag (Markierung)-Schlüssel mit diesem Präfix verfügt, können Sie den Schlüssel oder Wert des Tags (Markierung) nicht bearbeiten oder löschen. Tags (Markierungen) mit dem Präfix `aws :` werden nicht als Ihre Tags (Markierungen) pro Ressourcenlimit angerechnet.

Sie können eine Ressource nicht ausschließlich anhand ihrer Tags löschen. Sie müssen die Ressourcen-ID angeben. Um beispielsweise ein Dateisystem zu löschen, das Sie mit einem Tag-Schlüssel namens `DeleteMe` gekennzeichnet haben, müssen Sie die `DeleteFileSystem` Aktion mit der Dateisystem-Ressourcen-ID verwenden, z. B. `fs-1234567890abcdef0`.

Wenn Sie öffentliche oder gemeinsam genutzte Ressourcen taggen, sind die von Ihnen zugewiesenen Tags nur für Sie verfügbar. Andere haben keinen Zugriff auf diese Tags. Für die Tag-basierte Zugriffskontrolle auf gemeinsam genutzte Ressourcen muss jede Ressource ihren eigenen Satz von Tags zuweisen, um den Zugriff auf die Ressource zu kontrollieren.

Berechtigungen und Tag

Weitere Informationen zu den Berechtigungen, die erforderlich sind, um Amazon FSx-Ressourcen bei der Erstellung zu kennzeichnen, finden Sie unter [Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung](#). Weitere Informationen zur Verwendung von Tags zur Beschränkung des Zugriffs auf Amazon FSx-Ressourcen in IAM-Richtlinien finden Sie unter [Verwenden von mithilfe von von von von von von von von von von von von FSx von mit](#)

Wartungsfenster von Amazon FSx for Lustre

Amazon FSx for Lustre führt routinemäßige Software-Patches für die von ihm verwaltete Lustre-Software durch. Das Wartungsfenster bietet Ihnen die Möglichkeit, zu kontrollieren, an welchem Wochentag und zu welcher Uhrzeit diese Software-Patches durchgeführt werden.

Das Patchen sollte nur einen Bruchteil Ihres 30-minütigen Wartungsfensters in Anspruch nehmen. Während dieser wenigen Minuten ist Ihr Dateisystem vorübergehend nicht verfügbar. Sie wählen das Wartungsfenster bei der Erstellung des Dateisystems. Wenn Sie keine Zeitpräferenz haben, wird ein Standardfenster von 30 Minuten zugewiesen.

FSx for Lustre ermöglicht es Ihnen, Ihr Wartungsfenster nach Bedarf an Ihre Arbeitslast und Betriebsanforderungen anzupassen. Sie können Ihr Wartungsfenster beliebig oft verschieben, vorausgesetzt, dass mindestens einmal alle 14 Tage ein Wartungsfenster geplant ist. Wenn ein Patch veröffentlicht wird und Sie innerhalb von 14 Tagen kein Wartungsfenster geplant haben, wird FSx for Lustre mit der Wartung des Dateisystems fortfahren, um dessen Sicherheit und Zuverlässigkeit zu gewährleisten.

Sie können die Amazon FSx Management Console AWS CLI, AWS API oder eines der AWS SDKs verwenden, um das Wartungsfenster für Ihre Dateisysteme zu ändern.

Um das Wartungsfenster mithilfe der Konsole zu ändern

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Navigationsbereich Dateisysteme aus.
3. Wählen Sie das Dateisystem aus, für das Sie das Wartungsfenster ändern möchten. Die Seite mit den Dateisystemdetails wird angezeigt.
4. Wählen Sie die Registerkarte Wartung. Das Fenster „Einstellungen“ des Wartungsfensters wird angezeigt.
5. Wählen Sie Bearbeiten und geben Sie den neuen Tag und die Uhrzeit ein, an dem das Wartungsfenster beginnen soll.
6. Wählen Sie Speichern, um Ihre Änderungen zu speichern. Die neue Startzeit der Wartung wird im Bereich Einstellungen angezeigt.

Sie können das Wartungsfenster für Ihr Dateisystem mit dem [update-file-system](#) CLI-Befehl ändern. Führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Dateisystem-ID durch die ID für Ihr Dateisystem und das Datum und die Uhrzeit, zu der Sie das Fenster starten möchten.

```
aws fsx update-file-system --file-system-id fs-01234567890123456 --lustre-configuration  
WeeklyMaintenanceStartTime=1:01:30
```

Löschen eines Dateisystems

Sie können ein Amazon FSx for Lustre-Dateisystem mithilfe der Amazon FSx-Konsole AWS CLI, der und der Amazon FSx-API löschen. Bevor Sie ein FSx for Lustre-Dateisystem löschen, sollten Sie es von jeder verbundenen Amazon EC2 EC2-Instance [unmounten](#). [Um auf S3-verknüpften Dateisystemen sicherzustellen, dass alle Ihre Daten vor dem Löschen Ihres Dateisystems in S3 zurückgeschrieben werden, können Sie entweder darauf achten, dass die AgeOfOldestQueuedMessage-Metrik Null ist \(wenn Sie den automatischen Export verwenden\), oder Sie können eine Aufgabe zum Exportieren eines Daten-Repositorys ausführen.](#) Wenn Sie den automatischen Export aktiviert haben und eine Aufgabe zum Exportieren eines Datenrepositorys verwenden möchten, müssen Sie den automatischen Export deaktivieren, bevor Sie die Aufgabe zum Exportieren des Datenrepositorys ausführen.

Um ein Dateisystem nach dem Aushängen aus jeder Amazon EC2 EC2-Instance zu löschen:

- Verwenden der Konsole — Folgen Sie dem unter beschriebenen Verfahren. [Bereinigen von - Ressourcen](#)
- Verwenden der API oder CLI — Verwenden Sie den [DeleteFileSystem-API-Vorgang](#) oder den CLI-Befehl [delete-file-system](#).

Migration zu Amazon FSx for Lustre mit AWS DataSync

Sie können AWS DataSync verwenden, um Daten zwischen FSx for Lustre-Dateisystemen zu übertragen. DataSync ist ein Datenübertragungsdienst, der das Verschieben und Replizieren von Daten zwischen selbstverwalteten Speichersystemen und AWS Speicherdiensten über das Internet vereinfacht, automatisiert und beschleunigt oder. AWS Direct Connect DataSync kann Ihre Dateisystemdaten und Metadaten wie Eigentum, Zeitstempel und Zugriffsberechtigungen übertragen.

So migrieren Sie bestehende Dateien zu FSx for Lustre mit AWS DataSync

Sie können Dateisysteme DataSync mit FSx for Lustre verwenden, um einmalige Datenmigrationen durchzuführen, regelmäßig Daten für verteilte Workloads aufzunehmen und die Replikation für Datenschutz und Wiederherstellung zu planen. Informationen zu bestimmten Übertragungsszenarien finden Sie unter [Wo kann ich meine Daten übertragen?](#) im AWS DataSync Benutzerhandbuch.

Voraussetzungen

Um Daten in Ihr FSx for Lustre-Setup zu migrieren, benötigen Sie einen Server und ein Netzwerk, die die DataSync Anforderungen erfüllen. Weitere Informationen finden Sie unter [Anforderungen für DataSync](#) im AWS DataSync Benutzerhandbuch.

- Sie haben ein Ziel-FSx FSx for Lustre Lustre-Dateisystem erstellt. Weitere Informationen finden Sie unter [Erstellen Sie Ihr FSx for Lustre-Dateisystem](#).
- Die Quell- und Zieldateisysteme sind in derselben Virtual Private Cloud (VPC) verbunden. Das Quelldateisystem kann sich lokal oder in einer anderen Amazon VPC befinden, oder AWS-Konto AWS-Region, es muss sich jedoch in einem Netzwerk befinden, das mit dem des Zieldateisystems über Amazon VPC Peering, Transit Gateway, oder gepeert wird. AWS Direct Connect AWS VPN Weitere Informationen finden Sie unter [Was ist VPC Peering?](#) im Amazon VPC Peering Guide.

Note

DataSync kann nur AWS-Konten zu oder von FSx for Lustre übertragen werden, wenn der andere Übertragungsort Amazon S3 ist.

Grundlegende Schritte für die Migration von Dateien mit DataSync

Das Übertragen von Dateien von einer Quelle zu einem Ziel mithilfe von DataSync umfasst die folgenden grundlegenden Schritte:

- Laden Sie einen Agenten herunter, stellen Sie ihn in Ihrer Umgebung bereit und aktivieren Sie ihn (bei der Übertragung zwischen diesen nicht erforderlich AWS-Services).
- Erstellen Sie einen Quell- und Zielort.
- Erstellen Sie eine Aufgabe.
- Führen Sie die Aufgabe aus, um Dateien von der Quelle zum Ziel zu übertragen.

Weitere Informationen finden Sie in den folgenden Themen im AWS DataSync Benutzerhandbuch:

- [Übertragung zwischen lokalem Speicher und AWS](#)
- [Konfiguration von AWS DataSync Übertragungen mit Amazon FSx for Lustre](#) im AWS DataSync Benutzerhandbuch.
- [Stellen Sie Ihren Agenten auf Amazon EC2 bereit](#)

Überwachung von Amazon FSx for Lustre

Sie können die folgenden automatisierten Überwachungstools verwenden, um Amazon FSx for Lustre zu beobachten und zu melden, wenn etwas nicht stimmt:

- **Überwachung mit Amazon CloudWatch** — CloudWatch sammelt Rohdaten von Amazon FSx for Lustre und verarbeitet sie zu lesbaren, nahezu in Echtzeit verfügbaren Metriken. Sie können einen CloudWatch Alarm erstellen, der eine Amazon SNS SNS-Nachricht sendet, wenn sich der Status des Alarms ändert.
- **Überwachung mithilfe der Lustre-Protokollierung** — Sie können die aktivierten Protokollierungsereignisse für Ihr Dateisystem überwachen. Lustre Logging schreibt diese Ereignisse in Amazon CloudWatch Logs.
- **AWS CloudTrail Protokollüberwachung** — Teilen Sie Protokolldateien zwischen Konten, überwachen CloudTrail Sie Protokolldateien in Echtzeit, indem Sie sie an CloudWatch Logs senden, schreiben Sie Protokollverarbeitungsanwendungen in Java und stellen Sie sicher, dass sich Ihre Protokolldateien nach der Lieferung von CloudTrail nicht geändert haben.

Themen

- [Überwachung mit Amazon CloudWatch](#)
- [Protokollierung mit Amazon CloudWatch Logs](#)
- [Protokollierung von FSx for Lustre-API-Aufrufen mit AWS CloudTrail](#)

Überwachung mit Amazon CloudWatch

Sie können Dateisysteme mit Amazon überwachen CloudWatch, das Rohdaten von Amazon FSx for Lustre sammelt und zu lesbaren Metriken nahezu in Echtzeit verarbeitet. Diese Statistiken werden für einen Zeitraum von 15 Monaten aufbewahrt, sodass Sie auf historische Informationen zugreifen und sich einen besseren Überblick über die Leistung Ihrer Webanwendung oder Ihres Dienstes verschaffen können. Standardmäßig werden Amazon FSx for Lustre-Metriken automatisch alle 1 CloudWatch Minute gesendet. Weitere Informationen zu CloudWatch finden Sie unter [Was ist Amazon CloudWatch?](#) im CloudWatch Amazon-Benutzerhandbuch.

CloudWatch Metriken werden als Roh-Bytes gemeldet. Bytes werden nicht auf eine Dezimalzahl oder ein binäres Vielfaches der Einheit gerundet.

Metriken des Dateisystems

FSx for Lustre veröffentlicht die folgenden Metriken im FSx Namespace in CloudWatch. Für jede Metrik gibt FSx for Lustre einen Datenpunkt pro Festplatte pro Minute aus. Um aggregierte Dateisystemdetails anzuzeigen, können Sie die Statistik verwenden. **Sum** Beachten Sie, dass die Dateiserver hinter Ihren FSx for Lustre-Dateisystemen auf mehrere Festplatten verteilt sind.

Metrik	Beschreibung
DataReadBytes	<p>Die Anzahl der Byte für Lesevorgänge im Dateisystem.</p> <p>Die Sum Statistik gibt die Gesamtzahl der Byte an, die Lesevorgängen während des Zeitraums zugeordnet wurden. Die Minimum Statistik gibt die Mindestanzahl von Byte an, die Lesevorgängen auf einer einzelnen Festplatte zugeordnet sind. Die Maximum Statistik gibt die maximale Anzahl von Byte an, die Lesevorgängen auf der Festplatte zugeordnet sind. Die Average Statistik gibt die durchschnittliche Anzahl von Byte an, die mit Lesevorgängen pro Festplatte verknüpft sind. Die SampleCount Statistik gibt die Anzahl der Festplatten an.</p> <p>Zum Berechnen des durchschnittlichen Durchsatzes (Byte pro Sekunde) für einen Zeitraum dividieren Sie die Sum-Statistik durch die Anzahl von Sekunden in dem Zeitraum.</p> <p>Einheiten:</p> <ul style="list-style-type: none"> • Byte für Sum, Minimum, Maximum und Average. • Anzahl für SampleCount . <p>Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCount</p>
DataWriteBytes	<p>Die Anzahl der Byte für Schreiboperationen im Dateisystem.</p> <p>Die Sum-Statistik ist die Gesamtzahl von Byte, die mit den Schreiboperationen verknüpft sind. Die Minimum Statistik gibt die Mindestanzahl von Byte an, die Schreiboperationen auf einer einzelnen Festplatte zugeordnet sind. Die Maximum Statistik gibt die maximale Anzahl von</p>

Metrik	Beschreibung
	<p>Byte an, die Schreibvorgängen auf der Festplatte zugeordnet sind. Die Average Statistik gibt die durchschnittliche Anzahl von Byte an, die mit Schreibvorgängen pro Festplatte verknüpft sind. Die SampleCount Statistik gibt die Anzahl der Festplatten an.</p> <p>Zum Berechnen des durchschnittlichen Durchsatzes (Byte pro Sekunde) für einen Zeitraum dividieren Sie die Sum-Statistik durch die Anzahl von Sekunden in dem Zeitraum.</p> <p>Einheiten:</p> <ul style="list-style-type: none">• Byte für Sum, Minimum, Maximum und Average.• Anzahl für SampleCount . <p>Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCount</p>

Metrik	Beschreibung
DataReadOperations	<p data-bbox="479 226 909 262">Die Anzahl der Lesevorgänge.</p> <p data-bbox="479 304 1485 577">Die Sum Statistik ist die Gesamtzahl der Lesevorgänge. Die Minimum Statistik gibt die Mindestanzahl von Lesevorgängen auf einer einzelnen Festplatte an. Die Maximum Statistik gibt die maximale Anzahl von Lesevorgängen auf der Festplatte an. Die Average Statistik gibt die durchschnittliche Anzahl von Lesevorgängen pro Festplatte an. Die SampleCount Statistik gibt die Anzahl der Festplatten an.</p> <p data-bbox="479 619 1469 745">Um die durchschnittliche Anzahl von Lesevorgängen (Operationen pro Sekunde) für einen Zeitraum zu berechnen, dividieren Sie die Sum Statistik durch die Anzahl der Sekunden in der Periode.</p> <p data-bbox="479 798 625 829">Einheiten:</p> <ul data-bbox="479 871 1209 976" style="list-style-type: none">• Byte für Sum, Minimum, Maximum und Average.• Anzahl für SampleCount . <p data-bbox="479 1039 1453 1123">Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCount</p>

Metrik	Beschreibung
DataWrite Operations	<p data-bbox="479 226 982 262">Die Anzahl der Schreiboperationen.</p> <p data-bbox="479 306 1495 625">Die Sum Statistik ist die Gesamtzahl der Schreiboperationen. Die Minimum Statistik gibt die Mindestanzahl von Schreibvorgängen auf einer einzelnen Festplatte an. Die Maximum Statistik gibt die maximale Anzahl von Schreibvorgängen auf der Festplatte an. Die Average Statistik gibt die durchschnittliche Anzahl von Schreibvorgängen pro Festplatte an. Die SampleCount Statistik gibt die Anzahl der Festplatten an.</p> <p data-bbox="479 674 1469 800">Um die durchschnittliche Anzahl von Schreibvorgängen (Operationen pro Sekunde) für einen Zeitraum zu berechnen, dividieren Sie die Sum Statistik durch die Anzahl der Sekunden in der Periode.</p> <p data-bbox="479 848 621 884">Einheiten:</p> <ul data-bbox="479 932 1203 1024" style="list-style-type: none">• Byte für Sum, Minimum, Maximum und Average.• Anzahl für SampleCount . <p data-bbox="479 1100 1458 1178">Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCount</p>

Metrik	Beschreibung
MetadataOperations	<p>Die Anzahl der Metadatenoperationen.</p> <p>Die Sum Statistik gibt die Anzahl der Metadatenoperationen an. Die Minimum Statistik gibt die Mindestanzahl von Metadatenoperationen pro Festplatte an. Die Maximum Statistik gibt die maximale Anzahl von Metadatenoperationen pro Festplatte an. Die Average Statistik gibt die durchschnittliche Anzahl von Metadatenoperationen pro Festplatte an. Die SampleCount Statistik gibt die Anzahl der Festplatten an.</p> <p>Um die durchschnittliche Anzahl von Metadatenoperationen (Operationen pro Sekunde) für einen Zeitraum zu berechnen, dividieren Sie die Sum Statistik durch die Anzahl der Sekunden in der Periode.</p> <p>Einheiten:</p> <ul style="list-style-type: none">• Zählen Sie für SumMinimum, MaximumAverage, undSampleCount . <p>Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCount</p>

Metrik	Beschreibung
FreeDataStorageCapacity	<p>Die Menge der verfügbaren Speicherkapazität.</p> <p>Die <code>Sum</code> Statistik gibt die Gesamtzahl der im Dateisystem verfügbaren Byte an. Die <code>Minimum</code> Statistik gibt die Gesamtzahl der Byte an, die auf der größten Festplatte verfügbar sind. Die <code>Maximum</code> Statistik gibt die Gesamtzahl der Byte an, die auf der Festplatte mit dem größten verbleibenden verfügbaren Speicherplatz verfügbar sind. Die <code>Average</code> Statistik gibt die durchschnittliche Anzahl der pro Festplatte verfügbaren Byte an. Die <code>SampleCount</code> Statistik gibt die Anzahl der Festplatten an.</p> <p>Einheiten:</p> <ul style="list-style-type: none">• Bytes für <code>Sum</code>, <code>Minimum</code>, <code>Maximum</code>.• Anzahl für <code>SampleCount</code> . <p>Gültige Statistiken: <code>Sum</code>, <code>Minimum</code>, <code>Maximum</code>, <code>Average</code>, <code>SampleCount</code></p>

Metrik	Beschreibung
LogicalDiskUsage	<p>Die Menge der gespeicherten logischen Daten (unkomprimiert).</p> <p>Die Sum Statistik ist die Gesamtzahl der im Dateisystem gespeicherten logischen Byte. Die Minimum Statistik gibt die geringste Anzahl logischer Byte an, die auf einer Festplatte im Dateisystem gespeichert sind. Die Maximum Statistik ist die größte Anzahl logischer Byte, die auf einer Festplatte im Dateisystem gespeichert sind. Die Average Statistik gibt die durchschnittliche Anzahl der pro Festplatte gespeicherten logischen Byte an. Die SampleCount Statistik gibt die Anzahl der Festplatten an.</p> <p>Einheiten:</p> <ul style="list-style-type: none">• Bytes für Sum, Minimum, Maximum.• Anzahl für SampleCount . <p>Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCount</p>

Metrik	Beschreibung
PhysicalDiskUsage	<p>Die Menge an Speicherplatz, die physisch von Dateisystemdaten belegt wird (komprimiert).</p> <p>Die Sum Statistik gibt die Gesamtzahl der Byte an, die auf Festplatten im Dateisystem belegt sind. Die Minimum Statistik gibt die Gesamtzahl der Byte an, die auf der leersten Festplatte belegt sind. Die Maximum Statistik gibt die Gesamtzahl der Byte an, die auf der vollsten Festplatte belegt sind. Die Average Statistik gibt die durchschnittliche Anzahl der pro Festplatte belegten Byte an. Die SampleCount Statistik gibt die Anzahl der Festplatten an.</p> <p>Einheiten:</p> <ul style="list-style-type: none"> • Bytes für Sum, Minimum, Maximum. • Anzahl für SampleCount . <p>Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCount</p>

Metriken für Metadaten des Dateisystems

FSx for Lustre veröffentlicht die folgenden Metriken für Dateisystem-Metadaten im FSx Namespace in CloudWatch. Diese Metriken verwenden Dimensionen, um detailliertere Messungen Ihrer Metadaten zu ermöglichen. Alle Metadatenmetriken haben die StorageTargetId Dimensionen FileSystemId und. Metriken für Dateisystem-Metadaten werden nur angezeigt, wenn für Ihr Dateisystem eine Metadatenkonfiguration angegeben ist.

Metrik	Beschreibung
DiskReadOperations	Die Anzahl der Lesevorgänge für den Dateiserver, der auf Speichervolumen zugreift. Der gesamte Datenverkehr wird in dieser Metrik berücksichtigt, einschließlich Hintergrundaufgaben. Jede Minute wird für

Metrik	Beschreibung
	<p>jedes Speichervolumen Ihres Dateisystems eine Metrik ausgegeben.</p> <p>Die Sum Statistik gibt die Gesamtzahl der Lesevorgänge an, die von dem angegebenen Speichervolumen im angegebenen Zeitraum ausgeführt wurden.</p> <p>Die Average Statistik gibt die durchschnittliche Anzahl von Lesevorgängen an, die das angegebene Speichervolumen im angegebenen Zeitraum pro Minute ausgeführt hat.</p> <p>Die Minimum Statistik gibt die niedrigste Anzahl von Lesevorgängen an, die das angegebene Speichervolumen im angegebenen Zeitraum pro Minute ausführt.</p> <p>Die Maximum Statistik gibt die höchste Anzahl von Lesevorgängen an, die das angegebene Speichervolumen im angegebenen Zeitraum pro Minute ausführt.</p> <p>Verwenden Sie die Average Statistik und dividieren Sie das Ergebnis durch 60 (Sekunden), um die durchschnittlichen IOPS auf der Metadaten-Festplatte über den Zeitraum zu berechnen.</p> <p>Einheiten: Anzahl</p> <p>Gültige Statistiken: Sum, Average, und Minimum Maximum</p>

Metrik	Beschreibung
<p><code>DiskWriteOperations</code></p>	<p>Die Anzahl der Schreibvorgänge für den Dateiserver, der auf Speichervolumen zugreift.</p> <p>Die Anzahl der Schreibvorgänge auf diese Speichervolumen. Der gesamte Datenverkehr wird in dieser Metrik berücksichtigt, einschließlich Hintergrundaufgaben. Jede Minute wird für jedes Speichervolumen Ihres Dateisystems eine Metrik ausgegeben.</p> <p>Die Sum Statistik gibt die Gesamtzahl der Schreibvorgänge an, die von dem angegebenen Speichervolumen im angegebenen Zeitraum ausgeführt wurden.</p> <p>Die Average Statistik gibt die durchschnittliche Anzahl von Schreibvorgängen an, die pro Minute von dem angegebenen Speichervolumen im angegebenen Zeitraum ausgeführt wurden.</p> <p>Verwenden Sie die Average Statistik und dividieren Sie das Ergebnis durch 60 (Sekunden), um die durchschnittlichen IOPS auf der Metadaten-Festplatte über den Zeitraum zu berechnen.</p> <p>Einheiten: Anzahl</p> <p>Gültige Statistiken: und Sum Average</p>
<p><code>FileCreateOperations</code></p>	<p>Gesamtzahl der Dateierstellungsvorgänge.</p> <p>Einheit: Anzahl</p>

Metrik	Beschreibung
FileOpenOperations	Gesamtzahl der Operationen zum Öffnen von Dateien. Einheit: Anzahl
FileDeleteOperations	Gesamtzahl der Dateilöschvorgänge. Einheit: Anzahl
StatOperations	Gesamtzahl der Statistikoperationen. Einheit: Anzahl
RenameOperations	Gesamtzahl der Verzeichnisumbenennungen, unabhängig davon, ob es sich um direkte oder verzeichnisübergreifende Umbenennungen handelt. Einheit: Anzahl

AutoImport AutoExport und Metriken

FSx for Lustre veröffentlicht die folgenden AutoImport (automatischer Import) und AutoExport (automatischer Export) Metriken im FSx Namespace in CloudWatch. Diese Metriken verwenden Dimensionen, um detailliertere Messungen Ihrer Daten zu ermöglichen. Alle AutoImport AutoExport Metriken haben die Publisher Dimensionen FileSystemId und.

Metrik	Beschreibung
AgeOfOldestQueuedMessage Dimension: AutoExport	Das Alter der ältesten Nachricht in Sekunden, die darauf wartet, exportiert zu werden. Die Average Statistik gibt das Durchschnittsalter der ältesten Nachricht an, die auf den Export wartet. Die Maximum Statistik gibt an, wie viele Sekunden eine Nachricht maximal

Metrik	Beschreibung
	<p>in der Exportwarteschlange verweilte. Die Minimum Statistik gibt an, wie viele Sekunden eine Nachricht mindestens in der Exportwarteschlange verweilte. Ein Wert von Null gibt an, dass keine Nachrichten darauf warten, exportiert zu werden.</p> <p>Einheiten: Sekunden</p> <p>Gültige Statistiken: Average, Minimum, Maximum</p>
<p>RepositoryRenameOperations</p> <p>Dimension: AutoExport</p>	<p>Die Anzahl der Umbenennungen, die vom Dateisystem als Reaktion auf eine größere Verzeichnisumbenennung verarbeitet wurden.</p> <p>Die Sum Statistik gibt die Gesamtzahl der Umbenennungsvorgänge an, die sich aus einer Verzeichnisumbenennung ergeben. Die Average Statistik gibt die durchschnittliche Anzahl von Umbenennungsvorgängen für das Dateisystem an. Die Maximum Statistik gibt die maximale Anzahl von Umbenennungsvorgängen an, die mit einer Verzeichnisumbenennung im Dateisystem verbunden sind. Die Minimum Statistik gibt die Mindestanzahl von Umbenennungen an, die mit einer Verzeichnisumbenennung im Dateisystem verknüpft sind.</p> <p>Einheiten: Anzahl</p> <p>Gültige Statistiken: Sum,, Minimum Maximum Average</p>

Metrik	Beschreibung
AgeOfOldestQueuedMessage Dimension: AutoImport	<p>Das Alter der ältesten Nachricht in Sekunden, die darauf wartet, importiert zu werden.</p> <p>Die Average Statistik gibt das Durchschnittsalter der ältesten Nachricht an, die darauf wartet, importiert zu werden. Die Maximum Statistik gibt an, wie viele Sekunden eine Nachricht maximal in der Importwarteschlange verweilt. Die Minimum Statistik gibt an, wie viele Sekunden eine Nachricht mindestens in der Importwarteschlange gelebt hat. Ein Wert von Null gibt an, dass keine Nachrichten darauf warten, importiert zu werden.</p> <p>Einheiten: Sekunden</p> <p>Gültige Statistiken: Average, Minimum, Maximum</p>

Abmessungen von Amazon FSx for Lustre

Amazon FSx for Lustre-Metriken verwenden den FSx Namespace und stellen Metriken für die Dimension bereit. `FileSystemId` *Die ID eines Dateisystems kann mithilfe des `describe-file-systems` AWS CLI Befehls ermittelt werden und hat die Form `fs-01234567890123456`.*

Die `StorageTargetId` Dimension ist verfügbar und gibt CloudWatch an, welches MDT (Metadatenziel) die Metriken der Dateisystem-Metadaten veröffentlicht hat. A `StorageTargetId` hat die Form von `MDTxxxx` (zum Beispiel). `MDT0001`

Die `Publisher` Dimension ist in CloudWatch und AWS CLI für die `AutoImport` Metriken `AutoImport` und verfügbar und gibt an, welcher Dienst die Metriken veröffentlicht hat.

So verwenden Sie Amazon FSx for Lustre-Metriken

Die von Amazon FSx for Lustre gemeldeten Metriken bieten Informationen, die Sie auf unterschiedliche Weise analysieren können. Die folgende Liste zeigt einige gängige Verwendungszwecke für die Metriken. Es handelt sich dabei um Vorschläge für den Einstieg und nicht um eine umfassende Liste.

Wie stelle ich fest...	Relevante Metriken (Dimension Metrik)
Der Durchsatz meines Dateisystems?	SUMME (DataReadBytes + DataWriteBytes) /Zeitraum (in Sekunden)
Die IOPS meines Dateisystems?	Gesamtzahl der IOPS = SUMME (DataReadOperations + DataWriteOperations + MetadataOperations) /Zeitraum (in Sekunden)
Die Datenkomprimierungsrate meines Dateisystems?	SUM (LogicalDiskVerwendung)/SUM (PhysicalDiskVerwendung)
Wenn Updates für mein Dateisystem mit meinem S3-Bucket synchronisiert wurden?	AutoExport AgeOfOldestQueuedMessage
Wenn Updates für meinen S3-Bucket mit meinem Dateisystem synchronisiert wurden?	AutoImport AgeOfOldestQueuedMessage

Metrische Mathematik: Datenkomprimierungsverhältnis

Mithilfe metrischer Mathematik können Sie mehrere CloudWatch Metriken abfragen und mathematische Ausdrücke verwenden, um neue Zeitreihen auf der Grundlage dieser Metriken zu erstellen. Sie können die resultierenden Zeitreihen in der CloudWatch Konsole visualisieren und sie zu Dashboards hinzufügen. Weitere Informationen zur metrischen Mathematik finden Sie unter [Verwenden von metrischer Mathematik](#) im CloudWatch Amazon-Benutzerhandbuch.

Dieser metrische mathematische Ausdruck berechnet die Datenkomprimierungsrate Ihres Amazon FSx for Lustre-Dateisystems. Um dieses Verhältnis zu berechnen, rufen Sie zunächst die Summenstatistik der gesamten logischen Festplattennutzung (ohne Komprimierung) ab, die durch die `LogicalDiskUsage` Metrik bereitgestellt wird. Teilen Sie das dann durch die Summenstatistik der gesamten physischen Festplattennutzung (mit Komprimierung), die durch die `PhysicalDiskUsage` Metrik bereitgestellt wird.

Wenn Ihre Logik also wie folgt lautet: Summe von `LogicalDiskUsage` ÷ Summe von `PhysicalDiskUsage`

Dann lauten Ihre CloudWatch metrischen Informationen wie folgt.

ID	Verwendbare Metrik	Statistik	Intervall
m1	<code>LogicalDiskUsage</code>	Summe	1 Minute
m2	<code>PhysicalDiskUsage</code>	Summe	1 Minute

ID und Ausdruck Ihrer Metrikberechnung lauten wie folgt.

ID	Expression
e1	<code>m1/m2</code>

e1 ist das Datenkomprimierungsverhältnis.

Zugriff auf CloudWatch Metriken

Sie können sich Amazon FSx for Lustre-Metriken auf viele Arten CloudWatch ansehen. Sie können sie über die CloudWatch Konsole anzeigen oder über die CloudWatch CLI oder die CloudWatch API darauf zugreifen. Die folgenden Verfahren zeigen, wie Sie mithilfe dieser verschiedenen Tools auf die Metriken zugreifen können.

So zeigen Sie Metriken über die CloudWatch Konsole an

1. Öffnen Sie die [CloudWatch -Konsole](#).

2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den FSx-Namespace aus.
4. (Optional) Geben Sie den Namen einer Metrik in das Suchfeld ein, um sie anzuzeigen.
5. (Optional) Um nach Dimension zu filtern, wählen Sie FileSystem Id aus.

Um auf Metriken von der zuzugreifen AWS CLI

- Verwenden Sie den Befehl [list-metrics](#) mit dem `--namespace "AWS/FSx"`-Namespace. Weitere Informationen finden Sie in der [AWS CLI -Befehlsreferenz](#).

Um über die CloudWatch API auf Metriken zuzugreifen

- Rufen Sie die folgende Seite auf [GetMetricStatistics](#). Weitere Informationen finden Sie unter [Amazon CloudWatch API-Referenz](#).

CloudWatch Alarmer zur Überwachung von Amazon FSx for Lustre erstellen

Sie können einen CloudWatch Alarm erstellen, der eine Amazon SNS SNS-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine Metrik über einen bestimmten, von Ihnen definierten Zeitraum und führt eine oder mehrere Aktionen durch, die vom Wert der Metrik im Vergleich zu einem festgelegten Schwellenwert in einer Reihe von Zeiträumen abhängt. Die Aktion ist eine Benachrichtigung, die an ein Amazon SNS-Thema oder eine Auto Scaling-Richtlinie gesendet wird.


Bei Alarmen werden nur Aktionen für anhaltende Statusänderungen ausgelöst. CloudWatch Alarmer lösen keine Aktionen aus, nur weil sie sich in einem bestimmten Zustand befinden. Der Status muss sich geändert haben und für eine bestimmte Anzahl von Zeiträumen beibehalten worden sein.

Die folgenden Verfahren beschreiben, wie Sie Alarmer für Amazon FSx for Lustre erstellen.

So richten Sie Alarmer mithilfe der Konsole ein CloudWatch


1. Melden Sie sich bei der an AWS Management Console und öffnen Sie die CloudWatch Konsole unter <https://console.aws.amazon.com/cloudwatch/>.
2. Wählen Sie Alarm erstellen aus. Dadurch wird der Assistent zum Erstellen von Alarmen gestartet.

3. Wählen Sie FSx Metrics und blättern Sie durch die Amazon FSx for Lustre-Metriken, um die Metrik zu finden, für die Sie einen Alarm auslösen möchten. Um nur die Amazon FSx for Lustre-Metriken in diesem Dialogfeld anzuzeigen, suchen Sie nach der Dateisystem-ID Ihres Dateisystems. Wählen Sie die Metrik aus, für die ein Alarm erstellt werden soll, und klicken Sie auf Weiter.
4. Wählen Sie im Abschnitt Bedingungen die Bedingungen aus, die Sie für den Alarm verwenden möchten, und klicken Sie auf Weiter.

 Note

Metriken dürfen während der Wartung des Dateisystems nicht veröffentlicht werden. Um unnötige und irreführende Änderungen der Alarmbedingungen zu verhindern und Ihre Alarmer so zu konfigurieren, dass sie gegen fehlende Datenpunkte resistent sind, finden Sie im CloudWatch Amazon-Benutzerhandbuch unter [Konfiguration der Behandlung fehlender Daten durch CloudWatch Alarmer](#).

5. Wenn Sie Ihnen eine E-Mail senden CloudWatch möchten, wenn der Alarmstatus erreicht ist, wählen Sie für Wann immer dieser Alarm die Option Status ist ALARM. Wählen Sie unter Benachrichtigung senden an: ein vorhandenes SNS-Thema aus. Wenn Sie die Option Create topic (Thema erstellen) auswählen, können Sie den Namen und die E-Mail-Adressen für eine neue E-Mail-Abonnementliste einrichten. Diese Liste wird gespeichert und erscheint in diesem Feld für future Alarmer.

 Note

Wenn Sie Create topic verwenden, um ein neues Amazon SNS SNS-Thema zu erstellen, überprüfen Sie die E-Mail-Adressen, bevor Sie ihnen Benachrichtigungen senden. E-Mail Nachrichten werden nur gesendet, wenn der Alarm in einen Alarmzustand wechselt. Wenn dieser Alarmzustands geändert wird, bevor die E-Mail Adressen überprüft wurden, erhalten sie keine Benachrichtigung.

6. Sehen Sie sich im Bereich Alarmvorschau eine Vorschau des Alarms an, den Sie gerade erstellen möchten. Wenn er wie erwartet angezeigt wird, wählen Sie „Alarm erstellen“.

Um einen Alarm einzustellen, verwenden Sie den AWS CLI

- Rufen Sie die folgende Seite auf [put-metric-alarm](#). Weitere Informationen finden Sie in der [AWS CLI -Befehlsreferenz](#).

Um einen Alarm mithilfe der CloudWatch API einzustellen

- Rufen Sie die folgende Seite auf [PutMetricAlarm](#). Weitere Informationen finden Sie unter [Amazon CloudWatch API-Referenz](#).

Protokollierung mit Amazon CloudWatch Logs

FSx for Lustre unterstützt die Protokollierung von Fehler- und Warnereignissen für Datenrepositorys, die mit Ihrem Dateisystem verknüpft sind, in Amazon Logs. CloudWatch

Note

Die Protokollierung mit Amazon CloudWatch Logs ist nur auf Amazon FSx for Lustre-Dateisystemen verfügbar, die am 30. November 2021 nach 15 Uhr PST erstellt wurden.

Themen

- [Überblick über die Protokollierung](#)
- [Ziele protokollieren](#)
- [Verwaltung der Protokollierung](#)
- [Anzeigen von -Protokollen](#)

Überblick über die Protokollierung

Wenn Sie Datenrepositorys mit Ihrem FSx for Lustre-Dateisystem verknüpft haben, können Sie die Protokollierung von Datenrepository-Ereignissen in Amazon Logs aktivieren. CloudWatch Fehler- und Warnereignisse können bei den folgenden Datenrepository-Vorgängen protokolliert werden:

- Automatischer Export
- Aufgaben im Datenrepository

Weitere Informationen zu diesen Vorgängen und zur Verknüpfung mit Datenrepositorien finden Sie unter [Verwenden von Datenrepositorys mit Amazon FSx for Lustre](#).

Sie können die Protokollebenen konfigurieren, die Amazon FSx protokolliert, d. h., ob Amazon FSx nur Fehlerereignisse, nur Warnereignisse oder sowohl Fehler- als auch Warnereignisse protokolliert. Sie können die Ereignisprotokollierung auch jederzeit deaktivieren.

Note

Es wird dringend empfohlen, Protokolle für Dateisysteme zu aktivieren, mit denen ein gewisses Maß an kritischer Funktionalität verknüpft ist.

Ziele protokollieren

Wenn die Protokollierung aktiviert ist, muss FSx for Lustre mit einem Amazon CloudWatch Logs-Ziel konfiguriert werden. Das Ereignisprotokollziel ist eine Amazon CloudWatch Logs-Protokollgruppe, und Amazon FSx erstellt innerhalb dieser Protokollgruppe einen Protokollstream für Ihr Dateisystem. CloudWatch Mit Logs können Sie Audit-Ereignisprotokolle in der CloudWatch Amazon-Konsole speichern, anzeigen und durchsuchen, mithilfe von Logs Insights Abfragen zu den CloudWatch Protokollen ausführen und CloudWatch Alarme oder Lambda-Funktionen auslösen.

Sie wählen das Protokollziel, wenn Sie Ihr FSx for Lustre-Dateisystem erstellen oder danach, indem Sie es aktualisieren. Weitere Informationen finden Sie unter [Verwaltung der Protokollierung](#).

Standardmäßig erstellt und verwendet Amazon FSx eine CloudWatch Standard-Logs-Protokollgruppe in Ihrem Konto als Ziel für das Ereignisprotokoll. Wenn Sie eine benutzerdefinierte CloudWatch Logs-Protokollgruppe als Ziel für das Ereignisprotokoll verwenden möchten, gelten die folgenden Anforderungen für den Namen und den Speicherort des Ereignisprotokollziels:

- Der Name der CloudWatch Logs-Protokollgruppe muss mit dem `/aws/fsx/` Präfix beginnen.
- Wenn Sie beim Erstellen oder Aktualisieren eines Dateisystems auf der Konsole keine bestehende CloudWatch Logs-Protokollgruppe haben, kann Amazon FSx for Lustre einen Standard-Log-Stream in der CloudWatch `/aws/fsx/lustre` Logs-Protokollgruppe erstellen und verwenden. Der Protokollstream wird mit dem Format erstellt `datarepo_file_system_id` (zum Beispieldatarepo_fs-0123456789abcdef0).
- Wenn Sie die Standard-Protokollgruppe nicht verwenden möchten, können Sie über die Konfigurationsoberfläche eine CloudWatch Logs-Protokollgruppe erstellen, wenn Sie Ihr Dateisystem auf der Konsole erstellen oder aktualisieren.

- Die CloudWatch Zielprotokollgruppe muss sich in derselben AWS Partition und AWS-Konto wie Ihr Amazon FSx for Lustre-Dateisystem befinden. AWS-Region

Sie können das Ziel des Ereignisprotokolls jederzeit ändern. Wenn Sie dies tun, werden neue Ereignisprotokolle nur an das neue Ziel gesendet.

Verwaltung der Protokollierung

Sie können die Protokollierung aktivieren, wenn Sie ein neues FSx for Lustre-Dateisystem erstellen oder danach, indem Sie es aktualisieren. Die Protokollierung ist standardmäßig aktiviert, wenn Sie ein Dateisystem von der Amazon FSx-Konsole aus erstellen. Die Protokollierung ist jedoch standardmäßig deaktiviert, wenn Sie ein Dateisystem mit der AWS CLI oder der Amazon FSx-API erstellen.

In vorhandenen Dateisystemen, für die die Protokollierung aktiviert ist, können Sie die Einstellungen für die Ereignisprotokollierung ändern, einschließlich der Protokollebene, für die Ereignisse protokolliert werden sollen, und des Protokollziels. Sie können diese Aufgaben mit der Amazon FSx-Konsole oder der Amazon FSx-API ausführen. AWS CLI

Um die Protokollierung beim Erstellen eines Dateisystems (Konsole) zu aktivieren

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, das [Erstellen Sie Ihr FSx for Lustre-Dateisystem](#) im Abschnitt Erste Schritte beschrieben ist.
3. Öffnen Sie den Abschnitt Protokollierung — optional. Die Protokollierung ist standardmäßig aktiviert.

▼ **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

/aws/fsx/lustre ▼

[Create new](#)

Pricing
Standard Amazon CloudWatch Logs pricing applies based on your usage. [Learn more](#)

4. Fahren Sie mit dem nächsten Abschnitt des Assistenten zum Erstellen von Dateisystemen fort.

Wenn das Dateisystem verfügbar wird, wird die Protokollierung aktiviert.

So aktivieren Sie die Protokollierung beim Erstellen eines Dateisystems (CLI)

1. Verwenden Sie beim Erstellen eines neuen Dateisystems die `LogConfiguration` Eigenschaft zusammen mit dem [CreateFileSystemvorgang](#), um die Protokollierung für das neue Dateisystem zu aktivieren.

```
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. Wenn das Dateisystem verfügbar wird, wird die Protokollierungsfunktion aktiviert.

Um die Protokollierungskonfiguration zu ändern (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Lustre-Dateisystem aus, für das Sie die Protokollierung verwalten möchten.
3. Wählen Sie die Registerkarte Überwachung.
4. Wählen Sie im Bereich „Protokollierung“ die Option „Aktualisieren“.
5. Ändern Sie im Dialogfeld zur Konfiguration der Aktualisierungsprotokollierung die gewünschten Einstellungen.
 - a. Wählen Sie Fehler protokollieren, um nur Fehlerereignisse zu protokollieren, oder Warnungen protokollieren, um nur Warnungereignisse zu protokollieren, oder beides. Die Protokollierung ist deaktiviert, wenn Sie keine Auswahl treffen.
 - b. Wählen Sie ein vorhandenes Ziel für das CloudWatch Logs-Protokoll oder erstellen Sie ein neues.
6. Wählen Sie Speichern.

So ändern Sie die Logging-Konfiguration (CLI)

- Verwenden Sie den [update-file-system](#) CLI-Befehl oder die entsprechende [UpdateFileSystem](#) API-Operation.

```
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"}"
```

Anzeigen von -Protokollen

Sie können die Protokolle einsehen, nachdem Amazon FSx mit der Ausgabe begonnen hat. Sie können die Protokolle wie folgt anzeigen:

- Sie können Protokolle anzeigen, indem Sie zur CloudWatch Amazon-Konsole gehen und die Protokollgruppe und den Protokollstream auswählen, an die Ihre Ereignisprotokolle gesendet werden. Weitere Informationen finden Sie unter [An CloudWatch Logs gesendete Protokolldaten anzeigen](#) im Amazon CloudWatch Logs-Benutzerhandbuch.
- Sie können CloudWatch Logs Insights verwenden, um Ihre Protokolldaten interaktiv zu suchen und zu analysieren. Weitere Informationen finden Sie unter [Analysieren von Protokolldaten mit CloudWatch Logs Insights](#) im Amazon CloudWatch Logs-Benutzerhandbuch.
- Sie können Protokolle auch nach Amazon S3 exportieren. Weitere Informationen finden Sie unter [Exportieren von Protokolldaten nach Amazon S3](#) im Amazon CloudWatch Logs-Benutzerhandbuch.

Informationen zu den Gründen für Fehler finden Sie unter [Datenrepository-Ereignisprotokolle](#).

Protokollierung von FSx for Lustre-API-Aufrufen mit AWS CloudTrail

Amazon FSx for Lustre ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen eines Benutzers, einer Rolle oder eines AWS Dienstes in Amazon FSx for Lustre bereitstellt. CloudTrail erfasst alle API-Aufrufe für Amazon FSx for Lustre als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Amazon FSx for Lustre-Konsole und von Codeaufrufen an Amazon FSx for Lustre-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon FSx for Lustre. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der von gesammelten Informationen können

Sie feststellen CloudTrail, welche Anfrage an Amazon FSx for Lustre gestellt wurde. Sie können auch die IP-Adresse, von der die Anforderung ausging, den Ersteller und den Erstellungszeitpunkt sowie weitere Details bestimmen.

Weitere Informationen CloudTrail dazu finden Sie im [AWS CloudTrail Benutzerhandbuch](#).

Informationen zu Amazon FSx for Lustre in CloudTrail

CloudTrail ist für Ihr AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn API-Aktivitäten in Amazon FSx for Lustre auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen im CloudTrail Ereignisverlauf in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter [Ereignisse mit CloudTrail Ereignisverlauf anzeigen](#).

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS Konto, einschließlich Ereignissen für Amazon FSx for Lustre, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen AWS Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail -Benutzerhandbuch:

- [Übersicht zum Erstellen eines Trails](#)
- [CloudTrail Unterstützte Dienste und Integrationen](#)
- [Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail](#)
- [Empfangen von CloudTrail Protokolldateien aus mehreren Regionen](#) und [Empfangen von CloudTrail Protokolldateien von mehreren Konten](#)

Alle [API-Aufrufe](#) von Amazon FSx for Lustre werden von protokolliert. CloudTrail Beispielsweise generieren Aufrufe der TagResource Operationen CreateFileSystem und Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie im [CloudTrail UserIdentity-Element](#) im AWS CloudTrail Benutzerhandbuch.

Grundlegendes zu Amazon FSx for Lustre-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der den TagResource Vorgang demonstriert, wenn ein Tag für ein Dateisystem von der Konsole aus erstellt wird.

```
{
  "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"
}

```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die UntagResource Aktion demonstriert, wenn ein Tag für ein Dateisystem von der Konsole gelöscht wird.

```

{
  "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"  
}
```


Sicherheit in FSx for Lustre

Cloud-Sicherheit AWS hat höchste Priorität. Als AWS Kunde profitieren Sie von Rechenzentren und Netzwerkarchitekturen, die darauf ausgelegt sind, die Anforderungen der sicherheitssensibelsten Unternehmen zu erfüllen.

Sicherheit ist eine gemeinsame AWS Verantwortung von Ihnen und Ihnen. Das [Modell der geteilten Verantwortung](#) beschreibt dies als Sicherheit der Cloud und Sicherheit in der Cloud:

- Sicherheit der Cloud — AWS ist verantwortlich für den Schutz der Infrastruktur, die AWS Dienste in der Amazon Web Services Cloud ausführt. AWS bietet Ihnen auch Dienste, die Sie sicher nutzen können. Auditoren von Drittanbietern testen und überprüfen die Effektivität unserer Sicherheitsmaßnahmen im Rahmen der [AWS -Compliance-Programme](#) regelmäßig. Weitere Informationen zu den Compliance-Programmen, die für Amazon FSx for Lustre gelten, finden Sie unter [AWS Services in Scope by Compliance](#) Program.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Service, den Sie nutzen. Sie sind auch für andere Faktoren verantwortlich, etwa für die Vertraulichkeit Ihrer Daten, für die Anforderungen Ihres Unternehmens und für die geltenden Gesetze und Vorschriften.

Diese Dokumentation hilft Ihnen zu verstehen, wie Sie das Modell der gemeinsamen Verantwortung bei der Verwendung von Amazon FSx for Lustre anwenden können. In den folgenden Themen erfahren Sie, wie Sie Amazon FSx konfigurieren, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie erfahren auch, wie Sie andere Amazon-Services nutzen können, die Ihnen helfen, Ihre Amazon FSx for Lustre-Ressourcen zu überwachen und zu sichern.

Im Folgenden finden Sie eine Beschreibung der Sicherheitsaspekte bei der Arbeit mit Amazon FSx.

Themen

- [Datenschutz in Amazon FSx for Lustre](#)
- [Identitäts- und Zugriffsmanagement für Amazon FSx for Lustre](#)
- [Zugriffskontrolle für Dateisysteme mit Amazon VPC](#)
- [Amazon VPC-Netzwerk-ACLs](#)
- [Konformitätsvalidierung für Amazon FSx for Lustre](#)
- [Amazon FSx for Lustre und VPC-Schnittstellen-Endpunkte \(AWS PrivateLink\)](#)

Datenschutz in Amazon FSx for Lustre

Das AWS [Modell](#) der gilt für den Datenschutz in Amazon FSx for Lustre. Wie in diesem Modell beschrieben, AWS ist verantwortlich für den Schutz der globalen Infrastruktur, auf der alle Systeme laufen. AWS Cloud Sie sind dafür verantwortlich, die Kontrolle über Ihre in dieser Infrastruktur gehosteten Inhalte zu behalten. Sie sind auch für die Sicherheitskonfiguration und die Verwaltungsaufgaben für die von Ihnen verwendeten AWS-Services verantwortlich. Weitere Informationen zum Datenschutz finden Sie unter [Häufig gestellte Fragen zum Datenschutz](#). Informationen zum Datenschutz in Europa finden Sie im Blog-Beitrag [AWS -Modell der geteilten Verantwortung und in der DSGVO](#) im AWS -Sicherheitsblog.

Aus Datenschutzgründen empfehlen wir, dass Sie AWS-Konto Anmeldeinformationen schützen und einzelne Benutzer mit AWS IAM Identity Center oder AWS Identity and Access Management (IAM) einrichten. So erhält jeder Benutzer nur die Berechtigungen, die zum Durchführen seiner Aufgaben erforderlich sind. Außerdem empfehlen wir, die Daten mit folgenden Methoden schützen:

- Verwenden Sie für jedes Konto die Multi-Faktor-Authentifizierung (MFA).
- Verwenden Sie SSL/TLS, um mit Ressourcen zu kommunizieren. AWS Wir benötigen TLS 1.2 und empfehlen TLS 1.3.
- Richten Sie die API und die Protokollierung von Benutzeraktivitäten mit ein. AWS CloudTrail
- Verwenden Sie AWS Verschlüsselungslösungen zusammen mit allen darin enthaltenen Standardsicherheitskontrollen AWS-Services.
- Verwenden Sie erweiterte verwaltete Sicherheitservices wie Amazon Macie, die dabei helfen, in Amazon S3 gespeicherte persönliche Daten zu erkennen und zu schützen.
- Wenn Sie für den Zugriff AWS über eine Befehlszeilenschnittstelle oder eine API FIPS 140-2-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter [Federal Information Processing Standard \(FIPS\) 140-2](#).

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dies gilt auch, wenn Sie mit Amazon FSx oder anderen AWS-Services über die Konsole AWS CLI, API oder AWS SDKs arbeiten. Alle Daten, die Sie in Tags oder Freitextfelder eingeben, die für Namen verwendet werden, können für Abrechnungs- oder Diagnoseprotokolle verwendet werden. Wenn Sie eine URL für einen externen Server bereitstellen, empfehlen wir dringend, keine Anmeldeinformationen zur Validierung Ihrer Anforderung an den betreffenden Server in die URL einzuschließen.

Themen

- [Datenverschlüsselung in Amazon FSx for Lustre](#)
- [Richtlinie für den Datenverkehr zwischen Netzwerken](#)

Datenverschlüsselung in Amazon FSx for Lustre

Amazon FSx for Lustre unterstützt zwei Formen der Verschlüsselung für Dateisysteme: Verschlüsselung von Daten im Ruhezustand und Verschlüsselung bei der Übertragung. Die Verschlüsselung von Daten im Ruhezustand wird automatisch aktiviert, wenn ein Amazon FSx-Dateisystem erstellt wird. Die Verschlüsselung von Daten während der Übertragung wird automatisch aktiviert, wenn Sie über Amazon [EC2-Instances, die diese Funktion unterstützen, auf ein Amazon FSx-Dateisystem zugreifen](#).

Verwendung von Verschlüsselung

Wenn Ihr Unternehmen Unternehmens- oder behördlichen Richtlinien unterliegt, die die Verschlüsselung von Daten und Metadaten im Ruhezustand vorschreiben, empfehlen wir, ein verschlüsseltes Dateisystem zu erstellen und Ihr Dateisystem mithilfe der Verschlüsselung von Daten während der Übertragung zu mounten.

Weitere Informationen zum Erstellen eines Dateisystems, das im Ruhezustand mithilfe der Konsole verschlüsselt wird, finden Sie unter [Erstellen Sie Ihr Amazon FSx for Lustre-Dateisystem](#).


Themen

- [Verschlüsseln von Daten im Ruhezustand](#)
- [Verschlüsseln von Daten während der Übertragung](#)

Verschlüsseln von Daten im Ruhezustand

Die Verschlüsselung ruhender Daten wird automatisch aktiviert, wenn Sie ein Amazon FSx for Lustre-Dateisystem über die AWS Management Console, die oder programmgesteuert über die AWS CLI Amazon FSx-API oder eines der SDKs erstellen. AWS Ihr Unternehmen erfordert möglicherweise die Verschlüsselung aller Daten, die einer bestimmten Klassifizierung entsprechen oder zu einer speziellen Anwendung oder Umgebung bzw. zu einem speziellen Workload gehören. Wenn Sie ein persistentes Dateisystem erstellen, können Sie den AWS KMS Schlüssel angeben, mit dem die Daten verschlüsselt werden sollen. Wenn Sie ein Scratch-Dateisystem erstellen, werden die Daten mit Schlüsseln verschlüsselt, die von Amazon FSx verwaltet werden. Weitere Informationen zum

Erstellen eines Dateisystems, das im Ruhezustand mithilfe der Konsole verschlüsselt wird, finden Sie unter [Erstellen Sie Ihr Amazon FSx for Lustre-Dateisystem](#).

 Note

Die Infrastruktur AWS für die Schlüsselverwaltung verwendet von den Federal Information Processing Standards (FIPS) 140-2 zugelassene kryptografische Algorithmen. Die Infrastruktur entspricht den Empfehlungen der National Institute of Standards and Technology (NIST) 800-57.

Weitere Informationen zur Verwendung von FSx for Lustre finden Sie AWS KMS unter. [So verwendet Amazon FSx for Lustre AWS KMS](#)

Funktionsweise der Verschlüsselung im Ruhezustand

Auf einem verschlüsselten Dateisystem werden Daten und Metadaten automatisch verschlüsselt, bevor sie auf das Dateisystem geschrieben werden. Umgekehrt werden bei Lesevorgängen Daten und Metadaten entschlüsselt, bevor sie an die Anwendung gesendet werden. Diese Prozesse werden von Amazon FSx for Lustre transparent abgewickelt, sodass Sie Ihre Anwendungen nicht ändern müssen.


Amazon FSx for Lustre verwendet den branchenüblichen AES-256-Verschlüsselungsalgorithmus, um ruhende Dateisystemdaten zu verschlüsseln. Weitere Informationen finden Sie unter [Grundlagen der Kryptographie](#) im AWS Key Management Service -Entwicklerhandbuch.

So verwendet Amazon FSx for Lustre AWS KMS

Amazon FSx for Lustre verschlüsselt Daten automatisch, bevor sie in das Dateisystem geschrieben werden, und entschlüsselt Daten automatisch, wenn sie gelesen werden. Daten werden mit einer XTS-AES-256-Blockchiffre verschlüsselt. Alle Scratch-FSx FSx for Lustre Lustre-Dateisysteme sind im Ruhezustand mit Schlüsseln verschlüsselt, die von verwaltet werden. AWS KMS Amazon FSx for Lustre lässt sich in unsere AWS KMS Schlüsselverwaltung integrieren. Die Schlüssel, die zur Verschlüsselung von Scratch-Dateisystemen im Ruhezustand verwendet werden, sind für jedes Dateisystem einzigartig und werden nach dem Löschen des Dateisystems vernichtet. Für persistente Dateisysteme wählen Sie den KMS-Schlüssel, der zum Verschlüsseln und Entschlüsseln von Daten verwendet wird. Sie geben an, welcher Schlüssel verwendet werden soll, wenn Sie ein persistentes Dateisystem erstellen. Sie können Zuweisungen für diesen KMS-Schlüssel aktivieren, deaktivieren oder widerrufen. Dieser KMS-Schlüssel kann einer der beiden folgenden Typen sein:

- Von AWS verwalteter Schlüssel für Amazon FSx — Dies ist der Standard-KMS-Schlüssel. Die Erstellung und Speicherung eines KMS-Schlüssels wird Ihnen nicht in Rechnung gestellt, es fallen jedoch Nutzungsgebühren an. Weitere Informationen finden Sie unter [AWS Key Management Service Preise](#).
- Kundenverwalteter Schlüssel – Dies ist der flexibelste KMS-Schlüssel, da Sie seine Schlüsselrichtlinien und Berechtigungen für mehrere Benutzer oder Dienste konfigurieren können. Weitere Informationen zum Erstellen von kundenverwalteten Schlüsseln finden Sie unter [Creating Keys](#) im AWS Key Management Service Developer Guide.

Wenn Sie einen vom Kunden verwalteten Schlüssel als KMS-Schlüssel für die Verschlüsselung und Entschlüsselung von Dateidaten verwenden, können Sie die Schlüsselrotation aktivieren. Wenn Sie die Schlüsselrotation aktivieren, AWS KMS wird Ihr Schlüssel automatisch einmal pro Jahr rotiert. Darüber hinaus können Sie bei einem vom Kunden verwalteten Schlüssel (CMK) jederzeit entscheiden, wann Sie den Zugriff auf Ihren vom Kunden verwalteten Schlüssel deaktivieren, wieder aktivieren, löschen oder widerrufen möchten.

 **Important**

Amazon FSx akzeptiert nur KMS-Schlüssel mit symmetrischer Verschlüsselung. Sie können keine asymmetrischen KMS-Schlüssel mit Amazon FSx verwenden.

Die wichtigsten Richtlinien von Amazon FSx für AWS KMS

Schlüsselrichtlinien sind die primäre Methode zur Zugriffssteuerung für KMS-Schlüssel. Weitere Informationen zu wichtigen Richtlinien finden Sie unter [Verwenden von Schlüsselrichtlinien AWS KMS im AWS Key Management Service](#) Entwicklerhandbuch. In der folgenden Liste werden alle AWS KMS—bezogenen Berechtigungen beschrieben, die von Amazon FSx für Dateisysteme mit Verschlüsselung im Ruhezustand unterstützt werden:

- kms:Encrypt – (Optional) Verschlüsselt Klartext in Geheimtext. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.
- kms:Decrypt – (Erforderlich) Entschlüsselt Geheimtext. Geheimtext ist Klartext, der zuvor verschlüsselt wurde. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.
- kms: ReEncrypt — (Optional) Verschlüsselt Daten auf der Serverseite mit einem neuen KMS-Schlüssel, ohne den Klartext der Daten auf der Clientseite offenzulegen. Die Daten werden

zuerst entschlüsselt und dann neu verschlüsselt. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.

- kms: GenerateData KeyWithout Plaintext — (Erforderlich) Gibt einen mit einem KMS-Schlüssel verschlüsselten Datenverschlüsselungsschlüssel zurück. Diese Berechtigung ist in der Standardschlüsselrichtlinie unter kms: GenerateData Key* enthalten.
- kms: CreateGrant — (Erforderlich) Fügt einem Schlüssel einen Grant hinzu, um anzugeben, wer den Schlüssel verwenden kann und unter welchen Bedingungen. Erteilungen sind eine alternative Berechtigungsmethode zu Schlüsselrichtlinien. Weitere Informationen zu Zuschüssen finden Sie unter [Verwendung von Zuschüssen](#) im AWS Key Management Service Entwicklerhandbuch. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.
- kms: DescribeKey — (Erforderlich) Stellt detaillierte Informationen zum angegebenen KMS-Schlüssel bereit. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.
- kms: ListAliases — (Optional) Listet alle Schlüsselalias im Konto auf. Wenn Sie die Konsole verwenden, um ein verschlüsseltes Dateisystem zu erstellen, wird mit dieser Berechtigung die Liste zur Auswahl des KMS-Schlüssels aufgefüllt. Wir empfehlen für eine optimale Benutzererfahrung diese Berechtigung. Diese Berechtigung ist in der Standard-Schlüsselrichtlinie enthalten.

Verschlüsseln von Daten während der Übertragung

Scratch 2- und persistente Dateisysteme können Daten bei der Übertragung automatisch verschlüsseln. Wenn in der folgenden Tabelle ein Häkchen in der Zelle für diesen Bereitstellungstyp vorhanden ist AWS-Region, werden Daten während der Übertragung verschlüsselt, wenn auf das Dateisystem von Amazon EC2 EC2-Instances zugegriffen wird, die Verschlüsselung bei der Übertragung unterstützen, sowie für die gesamte Kommunikation zwischen Hosts innerhalb des Dateisystems. Informationen darüber, welche EC2-Instances Verschlüsselung bei der Übertragung unterstützen, finden Sie unter [Verschlüsselung bei der Übertragung im Amazon EC2-Benutzerhandbuch](#).

Die Verschlüsselung von Daten während der Übertragung für Scratch-2-Dateisysteme und persistente Dateisysteme ist im Folgenden verfügbar. AWS-Regionen

AWS-Region	Scratch_2	Persistent_1	Persistent_2
US East (Ohio)	✓	✓	✓
USA Ost (Nord-Virginia)	✓	✓	✓

AWS-Region	Scratch_2	Persistent_1	Persistent_2
Lokale Zone USA Ost (Atlanta) *			✓
USA West (Oregon)	✓	✓	✓
USA West (Nordkalifornien) *	✓	✓	
Lokale Zone USA West (Los Angeles)	✓	✓	
AWS GovCloud (US-Ost) *	✓	✓	
AWS GovCloud (US-West)	✓	✓	
Kanada (Zentral) *	✓	✓	✓
Kanada West (Calgary) *			✓
Europa (Irland)	✓	✓	✓
Europa (Milan)	✓	✓	
Europa (Frankfurt)	✓	✓	✓
Europa (Paris)	✓	✓	
Europa (London)	✓	✓	✓
Europa (Stockholm) *	✓	✓	✓
Asien-Pazifik (Seoul)	✓	✓	✓
Asien-Pazifik (Singapur)	✓	✓	✓
Asien-Pazifik (Tokio) *	✓	✓	✓
Asien-Pazifik (Mumbai) *	✓	✓	✓
Asien-Pazifik (Hongkong) *	✓	✓	✓
Asien-Pazifik (Sydney) *	✓	✓	✓

AWS-Region	Scratch_2	Persistent_1	Persistent_2
Israel (Tel Aviv) *	✓		✓
Südamerika (São Paulo) *	✓	✓	

Note

* Die Verschlüsselung von Daten während der Übertragung ist für Dateisysteme verfügbar, die nach dem 11. April 2021 erstellt wurden.

Richtlinie für den Datenverkehr zwischen Netzwerken

In diesem Thema wird beschrieben, wie Amazon FSx Verbindungen vom Service zu anderen Standorten sichert.

Verkehr zwischen Amazon FSx und lokalen Clients

Sie haben zwei Verbindungsoptionen zwischen Ihrem privaten Netzwerk und: AWS

- Eine AWS Site-to-Site VPN Verbindung. Weitere Informationen finden Sie unter [Was ist AWS Site-to-Site VPN?](#)
- Eine AWS Direct Connect Verbindung. Weitere Informationen finden Sie unter [Was ist AWS Direct Connect?](#)

Sie können über das Netzwerk auf FSx for Lustre zugreifen, um auf AWS-veröffentlichte API-Operationen zur Ausführung administrativer Aufgaben und auf Lustre-Ports zur Interaktion mit dem Dateisystem zuzugreifen.

Verschlüsselung des API-Datenverkehrs

Um auf AWS veröffentlichte API-Operationen zugreifen zu können, müssen Clients Transport Layer Security (TLS) 1.2 oder höher unterstützen. Wir benötigen TLS 1.2 und empfehlen TLS 1.3. Clients müssen außerdem Cipher Suites mit PFS (Perfect Forward Secrecy) wie DHE (Ephemeral Diffie-Hellman) oder ECDHE (Elliptic Curve Ephemeral Diffie-Hellman) unterstützen. Die meisten modernen Systemen wie Java 7 und höher unterstützen diese Modi. Außerdem müssen Anforderungen mit

einer Zugriffsschlüssel-ID und einem geheimen Zugriffsschlüssel signiert sein, der einem IAM-Prinzipal zugeordnet ist. Oder Sie können [AWS Security Token Service \(STS\)](#) verwenden, um temporäre Sicherheitsanmeldeinformationen zum Signieren von Anfragen zu generieren.

Verschlüsselung des Datenverkehrs

Die Verschlüsselung von Daten während der Übertragung wird von unterstützten EC2-Instances aus aktiviert, die von dort aus auf die Dateisysteme zugreifen. AWS Cloud Weitere Informationen finden Sie unter [Verschlüsseln von Daten während der Übertragung](#). FSx for Lustre bietet keine native Verschlüsselung bei der Übertragung zwischen lokalen Clients und Dateisystemen.

Identitäts- und Zugriffsmanagement für Amazon FSx for Lustre

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service, den Zugriff auf Ressourcen sicher zu AWS kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um Amazon FSx-Ressourcen zu verwenden. IAM ist ein Programm AWS-Service, das Sie ohne zusätzliche Kosten nutzen können.

Themen

- [Zielgruppe](#)
- [Authentifizierung mit Identitäten](#)
- [Verwalten des Zugriffs mit Richtlinien](#)
- [So funktioniert Amazon FSx for Lustre mit IAM](#)
- [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Lustre](#)
- [AWS verwaltete Richtlinien für Amazon FSx](#)
- [Fehlerbehebung bei Identität und Zugriff auf Amazon FSx for Lustre](#)
- [Verwenden von Tags mit Amazon FSx](#)
- [Verwenden von serviceverknüpften Rollen für Amazon FSx](#)

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von der Arbeit ab, die Sie in Amazon FSx ausführen.

Servicebenutzer — Wenn Sie den Amazon FSx-Service für Ihre Arbeit verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen zur Verfügung, die Sie benötigen. Da Sie für Ihre Arbeit mehr Amazon FSx-Funktionen verwenden, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Funktionsweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anfordern müssen. Wenn Sie auf eine Funktion in Amazon FSx nicht zugreifen können, finden Sie weitere Informationen unter [Fehlerbehebung bei Identität und Zugriff auf Amazon FSx for Lustre](#).

Service-Administrator — Wenn Sie in Ihrem Unternehmen für die Amazon FSx-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollen Zugriff auf Amazon FSx. Es ist Ihre Aufgabe, zu bestimmen, auf welche Funktionen und Ressourcen von Amazon FSx Ihre Servicebenutzer zugreifen sollen. Sie müssen dann Anträge an Ihren IAM-Administrator stellen, um die Berechtigungen Ihrer Servicenutzer zu ändern. Lesen Sie die Informationen auf dieser Seite, um die Grundkonzepte von IAM nachzuvollziehen. Weitere Informationen darüber, wie Ihr Unternehmen IAM mit Amazon FSx verwenden kann, finden Sie unter [So funktioniert Amazon FSx for Lustre mit IAM](#)

IAM-Administrator — Wenn Sie ein IAM-Administrator sind, möchten Sie vielleicht mehr darüber erfahren, wie Sie Richtlinien schreiben können, um den Zugriff auf Amazon FSx zu verwalten. Beispiele für identitätsbasierte Amazon FSx-Richtlinien, die Sie in IAM verwenden können, finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Lustre](#)

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen als IAM-Benutzer authentifiziert (angemeldet AWS) sein oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich AWS als föderierte Identität anmelden, indem Sie Anmeldeinformationen verwenden, die über eine Identitätsquelle bereitgestellt wurden. AWS IAM Identity Center (IAM Identity Center) -Benutzer, die Single Sign-On-Authentifizierung Ihres Unternehmens und Ihre Google- oder Facebook-Anmeldeinformationen sind Beispiele für föderierte Identitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie über den Verbund darauf zugreifen AWS, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich beim AWS Management Console oder beim AWS Zugangsportale anmelden. Weitere Informationen zur Anmeldung finden Sie AWS unter [So melden Sie sich bei Ihrem an AWS-Konto](#) im AWS-Anmeldung Benutzerhandbuch.

Wenn Sie AWS programmgesteuert darauf zugreifen, AWS stellt es ein Software Development Kit (SDK) und eine Befehlszeilenschnittstelle (CLI) bereit, mit denen Sie Ihre Anfragen mithilfe Ihrer Anmeldeinformationen kryptografisch signieren können. Wenn Sie keine AWS Tools verwenden, müssen Sie Anfragen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode, um Anfragen selbst zu [signieren, finden Sie im IAM-Benutzerhandbuch unter AWS API-Anfragen](#) signieren.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise, die Multi-Faktor-Authentifizierung (MFA) zu verwenden, um die Sicherheit Ihres Kontos zu erhöhen. Weitere Informationen finden Sie unter [Multi-Faktor-Authentifizierung](#) im AWS IAM Identity Center - Benutzerhandbuch und [Verwenden der Multi-Faktor-Authentifizierung \(MFA\) in AWS](#) im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie ein neues AWS-Konto erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services Ressourcen im Konto hat. Diese Identität wird als AWS-Konto Root-Benutzer bezeichnet. Sie können darauf zugreifen, indem Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, mit denen Sie das Konto erstellt haben. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Schützen Sie Ihre Root-Benutzer-Anmeldeinformationen und verwenden Sie diese, um die Aufgaben auszuführen, die nur der Root-Benutzer ausführen kann. Eine vollständige Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter [Aufgaben, die Root-Benutzer-Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Verbundidentität

Als bewährte Methode sollten menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen den Verbund mit einem Identitätsanbieter verwenden.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensbenutzerverzeichnis, einem Web-Identitätsanbieter AWS Directory Service, dem Identity Center-Verzeichnis oder einem beliebigen Benutzer, der mithilfe AWS-Services von Anmeldeinformationen zugreift, die über eine Identitätsquelle bereitgestellt wurden. Wenn föderierte Identitäten darauf zugreifen AWS-Konten, übernehmen sie Rollen, und die Rollen stellen temporäre Anmeldeinformationen bereit.

Für die zentrale Zugriffsverwaltung empfehlen wir Ihnen, AWS IAM Identity Center zu verwenden. Sie können Benutzer und Gruppen in IAM Identity Center erstellen, oder Sie können eine Verbindung zu einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und diese synchronisieren, um sie in all Ihren AWS-Konten Anwendungen zu verwenden. Informationen zu IAM Identity Center finden Sie unter [Was ist IAM Identity Center?](#) im AWS IAM Identity Center - Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein [IAM-Benutzer](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über spezifische Berechtigungen für eine einzelne Person oder Anwendung verfügt. Wenn möglich, empfehlen wir, temporäre Anmeldeinformationen zu verwenden, anstatt IAM-Benutzer zu erstellen, die langfristige Anmeldeinformationen wie Passwörter und Zugriffsschlüssel haben. Bei speziellen Anwendungsfällen, die langfristige Anmeldeinformationen mit IAM-Benutzern erfordern, empfehlen wir jedoch, die Zugriffsschlüssel zu rotieren. Weitere Informationen finden Sie unter [Regelmäßiges Rotieren von Zugriffsschlüsseln für Anwendungsfälle, die langfristige Anmeldeinformationen erfordern](#) im IAM-Benutzerhandbuch.

Eine [IAM-Gruppe](#) ist eine Identität, die eine Sammlung von IAM-Benutzern angibt. Sie können sich nicht als Gruppe anmelden. Mithilfe von Gruppen können Sie Berechtigungen für mehrere Benutzer gleichzeitig angeben. Gruppen vereinfachen die Verwaltung von Berechtigungen, wenn es zahlreiche Benutzer gibt. Sie könnten beispielsweise einer Gruppe mit dem Namen IAMAdmins Berechtigungen zum Verwalten von IAM-Ressourcen erteilen.

Benutzer unterscheiden sich von Rollen. Ein Benutzer ist einer einzigen Person oder Anwendung eindeutig zugeordnet. Eine Rolle kann von allen Personen angenommen werden, die sie benötigen. Benutzer besitzen dauerhafte Anmeldeinformationen. Rollen stellen temporäre Anmeldeinformationen bereit. Weitere Informationen finden Sie unter [Erstellen eines IAM-Benutzers \(anstatt einer Rolle\)](#) im IAM-Benutzerhandbuch.

IAM-Rollen

Eine [IAM-Rolle](#) ist eine Identität innerhalb Ihres Unternehmens AWS-Konto , die über bestimmte Berechtigungen verfügt. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der übernehmen, AWS Management Console indem Sie die Rollen [wechseln](#). Sie können eine Rolle übernehmen, indem Sie eine AWS CLI oder AWS API-Operation aufrufen oder eine benutzerdefinierte URL verwenden. Weitere Informationen zu Methoden für die Verwendung von Rollen finden Sie unter [Verwenden von IAM-Rollen](#) im IAM-Benutzerhandbuch.

IAM-Rollen mit temporären Anmeldeinformationen sind in folgenden Situationen hilfreich:

- **Verbundbenutzerzugriff** – Um einer Verbundidentität Berechtigungen zuzuweisen, erstellen Sie eine Rolle und definieren Berechtigungen für die Rolle. Wird eine Verbundidentität authentifiziert, so wird die Identität der Rolle zugeordnet und erhält die von der Rolle definierten Berechtigungen. Informationen zu Rollen für den Verbund finden Sie unter [Erstellen von Rollen für externe Identitätsanbieter](#) im IAM-Benutzerhandbuch. Wenn Sie IAM Identity Center verwenden, konfigurieren Sie einen Berechtigungssatz. Wenn Sie steuern möchten, worauf Ihre Identitäten nach der Authentifizierung zugreifen können, korreliert IAM Identity Center den Berechtigungssatz mit einer Rolle in IAM. Informationen zu Berechtigungssätzen finden Sie unter [Berechtigungssätze](#) im AWS IAM Identity Center -Benutzerhandbuch.
- **Temporäre IAM-Benutzerberechtigungen** – Ein IAM-Benutzer oder eine -Rolle kann eine IAM-Rolle übernehmen, um vorübergehend andere Berechtigungen für eine bestimmte Aufgabe zu erhalten.
- **Kontoübergreifender Zugriff** – Sie können eine IAM-Rolle verwenden, um einem vertrauenswürdigen Prinzipal in einem anderen Konto den Zugriff auf Ressourcen in Ihrem Konto zu ermöglichen. Rollen stellen die primäre Möglichkeit dar, um kontoübergreifendem Zugriff zu gewähren. Bei einigen können Sie AWS-Services jedoch eine Richtlinie direkt an eine Ressource anhängen (anstatt eine Rolle als Proxy zu verwenden). Informationen zu den Unterschieden zwischen Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.
- **Serviceübergreifender Zugriff** — Einige AWS-Services verwenden Funktionen in anderen AWS-Services. Wenn Sie beispielsweise einen Aufruf in einem Service tätigen, führt dieser Service häufig Anwendungen in Amazon-EC2 aus oder speichert Objekte in Amazon-S3. Ein Dienst kann dies mit den Berechtigungen des aufrufenden Prinzipals mit einer Servicерolle oder mit einer serviceverknüpften Rolle tun.
- **Forward Access Sessions (FAS)** — Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, in Kombination mit der Anfrage, Anfragen an AWS-Service nachgelagerte Dienste zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

- **Service-Rolle** – Eine Service-Rolle ist eine [IAM-Rolle](#), die ein Service übernimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Service-Rolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.
- **Dienstbezogene Rolle** — Eine dienstbezogene Rolle ist eine Art von Service-Rolle, die mit einer Service-Rolle verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Servicebezogene Rollen erscheinen in Ihrem Dienst AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.
- **Anwendungen, die auf Amazon EC2 ausgeführt werden** — Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und API-Anfragen stellen AWS CLI . AWS Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Um einer EC2-Instance eine AWS Rolle zuzuweisen und sie allen ihren Anwendungen zur Verfügung zu stellen, erstellen Sie ein Instance-Profil, das an die Instance angehängt ist. Ein Instance-Profil enthält die Rolle und ermöglicht, dass Programme, die in der EC2-Instance ausgeführt werden, temporäre Anmeldeinformationen erhalten. Weitere Informationen finden Sie unter [Verwenden einer IAM-Rolle zum Erteilen von Berechtigungen für Anwendungen, die auf Amazon-EC2-Instances ausgeführt werden](#) im IAM-Benutzerhandbuch.

Informationen dazu, wann Sie IAM-Rollen oder IAM-Benutzer verwenden sollten, finden Sie unter [Erstellen einer IAM-Rolle \(anstatt eines Benutzers\)](#) im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an AWS Identitäten oder Ressourcen anhängen. Eine Richtlinie ist ein Objekt, AWS das, wenn es einer Identität oder Ressource zugeordnet ist, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anfrage stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu Struktur und Inhalten von JSON-Richtliniendokumenten finden Sie unter [Übersicht über JSON-Richtlinien](#) im IAM-Benutzerhandbuch.

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das bedeutet, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

IAM-Richtlinien definieren Berechtigungen für eine Aktion unabhängig von der Methode, die Sie zur Ausführung der Aktion verwenden. Angenommen, es gibt eine Richtlinie, die Berechtigungen für die `iam:GetRole`-Aktion erteilt. Ein Benutzer mit dieser Richtlinie kann Rolleninformationen von der AWS Management Console AWS CLI, der oder der AWS API abrufen.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können weiter als Inline-Richtlinien oder verwaltete Richtlinien kategorisiert werden. Inline-Richtlinien sind direkt in einen einzelnen Benutzer, eine einzelne Gruppe oder eine einzelne Rolle eingebettet. Verwaltete Richtlinien sind eigenständige Richtlinien, die Sie mehreren Benutzern, Gruppen und Rollen in Ihrem System zuordnen können AWS-Konto. Zu den verwalteten Richtlinien gehören AWS verwaltete Richtlinien und vom Kunden verwaltete Richtlinien. Informationen dazu, wie Sie zwischen einer verwalteten Richtlinie und einer eingebundenen Richtlinie wählen, finden Sie unter [Auswahl zwischen verwalteten und eingebundenen Richtlinien](#) im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele für ressourcenbasierte Richtlinien sind IAM-Rollen-Vertrauensrichtlinien und Amazon-S3-Bucket-Richtlinien. In Services, die ressourcenbasierte Richtlinien unterstützen, können Service-Administratoren sie verwenden, um den Zugriff auf eine bestimmte Ressource zu steuern. Für die Ressource, an welche die Richtlinie angehängt ist, legt die Richtlinie fest, welche Aktionen ein bestimmter Prinzipal unter welchen Bedingungen für diese Ressource ausführen kann. Sie müssen in einer ressourcenbasierten Richtlinie [einen Prinzipal angeben](#). Zu den Prinzipalen können Konten, Benutzer, Rollen, Verbundbenutzer oder gehören. AWS-Services

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Zugriffssteuerungslisten (ACLs)

Zugriffssteuerungslisten (ACLs) steuern, welche Prinzipale (Kontomitglieder, Benutzer oder Rollen) auf eine Ressource zugreifen können. ACLs sind ähnlich wie ressourcenbasierte Richtlinien, verwenden jedoch nicht das JSON-Richtliniendokumentformat.

Amazon S3 und Amazon VPC sind Beispiele für Services, die ACLs unterstützen. AWS WAF Weitere Informationen“ zu ACLs finden Sie unter [Zugriffskontrollliste \(ACL\) – Übersicht](#) (Access Control List) im Amazon-Simple-Storage-Service-Entwicklerhandbuch.

Weitere Richtlinientypen

AWS unterstützt zusätzliche, weniger verbreitete Richtlinientypen. Diese Richtlinientypen können die maximalen Berechtigungen festlegen, die Ihnen von den häufiger verwendeten Richtlinientypen erteilt werden können.

- **Berechtigungsgrenzen** – Eine Berechtigungsgrenze ist ein erweitertes Feature, mit der Sie die maximalen Berechtigungen festlegen können, die eine identitätsbasierte Richtlinie einer IAM-Entität (IAM-Benutzer oder -Rolle) erteilen kann. Sie können eine Berechtigungsgrenze für eine Entität festlegen. Die daraus resultierenden Berechtigungen sind der Schnittpunkt der identitätsbasierten Richtlinien einer Entität und ihrer Berechtigungsgrenzen. Ressourcenbasierte Richtlinien, die den Benutzer oder die Rolle im Feld `Principal` angeben, werden nicht durch Berechtigungsgrenzen eingeschränkt. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen über Berechtigungsgrenzen finden Sie unter [Berechtigungsgrenzen für IAM-Entitäten](#) im IAM-Benutzerhandbuch.
- **Service Control Policies (SCPs)** — SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OU) in festlegen. AWS Organizations AWS Organizations ist ein Dienst zur Gruppierung und zentralen Verwaltung mehrerer Objekte AWS-Konten , die Ihrem Unternehmen gehören. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. Das SCP schränkt die Berechtigungen für Entitäten in Mitgliedskonten ein, einschließlich der einzelnen Entitäten. Root-Benutzer des AWS-Kontos Weitere Informationen zu Organizations und SCPs finden Sie unter [Funktionsweise von SCPs](#) im AWS Organizations -Benutzerhandbuch.

- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die Sie als Parameter übergeben, wenn Sie eine temporäre Sitzung für eine Rolle oder einen verbundenen Benutzer programmgesteuert erstellen. Die resultierenden Sitzungsberechtigungen sind eine Schnittmenge der auf der Identität des Benutzers oder der Rolle basierenden Richtlinien und der Sitzungsrichtlinien. Berechtigungen können auch aus einer ressourcenbasierten Richtlinie stammen. Eine explizite Zugriffsverweigerung in einer dieser Richtlinien setzt eine Zugriffserlaubnis außer Kraft. Weitere Informationen finden Sie unter [Sitzungsrichtlinien](#) im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn mehrere auf eine Anforderung mehrere Richtlinientypen angewendet werden können, sind die entsprechenden Berechtigungen komplizierter. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie im IAM-Benutzerhandbuch unter [Bewertungslogik für Richtlinien](#).

So funktioniert Amazon FSx for Lustre mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon FSx zu verwalten, sollten Sie sich darüber informieren, welche IAM-Funktionen für Amazon FSx verfügbar sind.

IAM-Funktionen, die Sie mit Amazon FSx for Lustre verwenden können

IAM-Feature	Amazon FSx-Unterstützung
Identitätsbasierte Richtlinien	Ja
Ressourcenbasierte Richtlinien	Nein
Richtlinienaktionen	Ja
Richtlinienressourcen	Ja
Bedingungsschlüssel für die Richtlinie	Ja
ACLs	Nein
ABAC (Tags in Richtlinien)	Ja
Temporäre Anmeldeinformationen	Ja

IAM-Feature	Amazon FSx-Unterstützung
Forward Access Sessions (FAS)	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen allgemeinen Überblick darüber, wie Amazon FSx und andere AWS Services mit den meisten IAM-Funktionen funktionieren, finden Sie im [AWS IAM-Benutzerhandbuch unter Services, die mit IAM funktionieren](#).

Identitätsbasierte Richtlinien für Amazon FSx

Unterstützt Richtlinien auf Identitätsbasis.	Ja
--	----

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Mit identitätsbasierten IAM-Richtlinien können Sie angeben, welche Aktionen und Ressourcen zugelassen oder abgelehnt werden. Darüber hinaus können Sie die Bedingungen festlegen, unter denen Aktionen zugelassen oder abgelehnt werden. Sie können den Prinzipal nicht in einer identitätsbasierten Richtlinie angeben, da er für den Benutzer oder die Rolle gilt, dem er zugeordnet ist. Informationen zu sämtlichen Elementen, die Sie in einer JSON-Richtlinie verwenden, finden Sie in der [IAM-Referenz für JSON-Richtlinienelemente](#) im IAM-Benutzerhandbuch.

Beispiele für identitätsbasierte Richtlinien für Amazon FSx

Beispiele für identitätsbasierte Richtlinien von Amazon FSx finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Lustre](#)

Ressourcenbasierte Richtlinien innerhalb von Amazon FSx

Unterstützt ressourcenbasierte Richtlinien	Nein
--	------

Politische Maßnahmen für Amazon FSx

Unterstützt Richtlinienaktionen

Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Richtlinienaktionen haben normalerweise denselben Namen wie der zugehörige AWS API-Vorgang. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keinen passenden API-Vorgang gibt. Es gibt auch einige Operationen, die mehrere Aktionen in einer Richtlinie erfordern. Diese zusätzlichen Aktionen werden als abhängige Aktionen bezeichnet.

Schließen Sie Aktionen in eine Richtlinie ein, um Berechtigungen zur Durchführung der zugeordneten Operation zu erteilen.

Eine Liste der Amazon FSx-Aktionen finden Sie unter [Von Amazon FSx for Lustre definierte Aktionen](#) in der Service Authorization Reference.

Richtlinienaktionen in Amazon FSx verwenden das folgende Präfix vor der Aktion:

```
fsx
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [  
  "fsx:action1",  
  "fsx:action2"  
]
```

Beispiele für identitätsbasierte Richtlinien von Amazon FSx finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Lustre](#)

Richtlinienressourcen für Amazon FSx

Unterstützt Richtlinienressourcen	Ja
-----------------------------------	----

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das bedeutet die Festlegung, welcher Prinzipal Aktionen für welche Ressourcen unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Anweisungen müssen entweder ein `Resource` oder ein `NotResource`-Element enthalten. Als bewährte Methode geben Sie eine Ressource mit dem zugehörigen [Amazon-Ressourcennamen \(ARN\)](#) an. Sie können dies für Aktionen tun, die einen bestimmten Ressourcentyp unterstützen, der als Berechtigungen auf Ressourcenebene bezeichnet wird.

Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, z. B. Auflistungsoperationen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*" 
```

Eine Liste der Amazon FSx-Ressourcentypen und ihrer ARNs finden Sie unter [Von Amazon FSx for Lustre definierte Ressourcen](#) in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter [Von Amazon FSx for Lustre definierte Aktionen](#).

Beispiele für identitätsbasierte Richtlinien von Amazon FSx finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Lustre](#)

Schlüssel für Richtlinienbedingungen für Amazon FSx

Unterstützt servicespezifische Richtlinienbedingungsschlüssel	Ja
---	----

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal kann Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen.

Das Element `Condition` (oder `Condition block`) ermöglicht Ihnen die Angabe der Bedingungen, unter denen eine Anweisung wirksam ist. Das Element `Condition` ist optional. Sie können bedingte Ausdrücke erstellen, die [Bedingungsoperatoren](#) verwenden, z. B. `ist gleich` oder `kleiner als`, damit die Bedingung in der Richtlinie mit Werten in der Anforderung übereinstimmt.

Wenn Sie mehrere `Condition`-Elemente in einer Anweisung oder mehrere Schlüssel in einem einzelnen `Condition`-Element angeben, wertet AWS diese mittels einer logischen AND-Operation aus. Wenn Sie mehrere Werte für einen einzelnen Bedingungschlüssel angeben, wertet die Bedingung mithilfe einer logischen OR Operation aus. Alle Bedingungen müssen erfüllt werden, bevor die Berechtigungen der Anweisung gewährt werden.

Sie können auch Platzhaltervariablen verwenden, wenn Sie Bedingungen angeben. Beispielsweise können Sie einem IAM-Benutzer die Berechtigung für den Zugriff auf eine Ressource nur dann gewähren, wenn sie mit dessen IAM-Benutzernamen gekennzeichnet ist. Weitere Informationen finden Sie unter [IAM-Richtlinienelemente: Variablen und Tags](#) im IAM-Benutzerhandbuch.

AWS unterstützt globale Bedingungschlüssel und dienstspezifische Bedingungschlüssel. Eine Übersicht aller AWS globalen Bedingungschlüssel finden Sie unter [Kontextschlüssel für AWS globale Bedingungen](#) im IAM-Benutzerhandbuch.

Eine Liste der Amazon FSx-Bedingungschlüssel finden Sie unter [Bedingungschlüssel für Amazon FSx for Lustre](#) in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungschlüssel verwenden können, finden Sie unter [Von Amazon FSx for Lustre definierte Aktionen](#).

Beispiele für identitätsbasierte Richtlinien von Amazon FSx finden Sie unter [Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Lustre](#)

Zugriffskontrolllisten (ACLs) in Amazon FSx

Unterstützt ACLs	Nein
------------------	------

Attributbasierte Zugriffskontrolle (ABAC) mit Amazon FSx

Unterstützt ABAC (Tags in Richtlinien)	Ja
--	----

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen definiert werden. In werden diese AWS Attribute Tags genannt. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und an viele AWS Ressourcen anhängen. Das Markieren von Entitäten und Ressourcen ist der erste Schritt von ABAC. Anschließend entwerfen Sie ABAC-Richtlinien, um Operationen zuzulassen, wenn das Tag des Prinzipals mit dem Tag der Ressource übereinstimmt, auf die sie zugreifen möchten.

ABAC ist in Umgebungen hilfreich, die schnell wachsen, und unterstützt Sie in Situationen, in denen die Richtlinienverwaltung mühsam wird.

Um den Zugriff auf der Grundlage von Tags zu steuern, geben Sie im Bedingungelement einer [Richtlinie Tag-Informationen](#) an, indem Sie die Schlüssel `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`, oder Bedingung `aws:TagKeys` verwenden.

Wenn ein Service alle drei Bedingungsschlüssel für jeden Ressourcentyp unterstützt, lautet der Wert für den Service Ja. Wenn ein Service alle drei Bedingungsschlüssel für nur einige Ressourcentypen unterstützt, lautet der Wert Teilweise.

Weitere Informationen zu ABAC finden Sie unter [Was ist ABAC?](#) im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe [Attributbasierte Zugriffskontrolle \(ABAC\)](#) verwenden im IAM-Benutzerhandbuch.

Weitere Informationen zum Taggen von Amazon FSx-Ressourcen finden Sie unter [Kennzeichnen Sie Ihre Amazon FSx-Ressourcen](#)

Ein Beispiel für eine identitätsbasierte Richtlinie zur Einschränkung des Zugriffs auf eine Ressource auf der Grundlage der Markierungen dieser Ressource finden Sie unter [Verwenden von mithilfe von von von von von von von von von von von von von FSx von mit.](#)

Temporäre Anmeldeinformationen mit Amazon FSx verwenden

Unterstützt temporäre Anmeldeinformationen	Ja
--	----

Einige funktionieren AWS-Services nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, einschließlich Informationen, die mit temporären Anmeldeinformationen AWS-Services [funktionieren AWS-Services](#), [finden Sie im IAM-Benutzerhandbuch unter Diese Option funktioniert mit IAM.](#)

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen AWS Management Console Methode als einem Benutzernamen und einem Passwort anmelden. Wenn Sie beispielsweise AWS über den Single Sign-On-Link (SSO) Ihres Unternehmens darauf zugreifen, werden bei diesem Vorgang automatisch temporäre Anmeldeinformationen erstellt. Sie erstellen auch automatisch temporäre Anmeldeinformationen, wenn Sie sich als Benutzer bei der Konsole anmelden und dann die Rollen wechseln. Weitere Informationen zum Wechseln von Rollen finden Sie unter [Wechseln zu einer Rolle \(Konsole\)](#) im IAM-Benutzerhandbuch.

Mithilfe der AWS API AWS CLI oder können Sie temporäre Anmeldeinformationen manuell erstellen. Sie können diese temporären Anmeldeinformationen dann für den Zugriff verwenden AWS. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter [Temporäre Sicherheitsanmeldeinformationen in IAM](#).

Zugriffssitzungen für Amazon FSx weiterleiten

Unterstützt Forward Access Sessions (FAS)	Ja
---	----

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle verwenden, um Aktionen auszuführen AWS, gelten Sie als Principal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service initiieren. FAS verwendet die Berechtigungen des Prinzipals, der einen aufruft AWS-Service, kombiniert mit der Anforderung, Anfragen an nachgelagerte Dienste AWS-Service zu stellen. FAS-Anfragen werden nur gestellt, wenn ein Dienst eine Anfrage erhält, für deren Abschluss Interaktionen mit anderen AWS-Services oder Ressourcen erforderlich sind. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter [Zugriffssitzungen weiterleiten](#).

Servicerollen für Amazon FSx

Unterstützt Servicerollen	Nein
---------------------------	------

Eine Servicerolle ist eine [IAM-Rolle](#), die ein Service annimmt, um Aktionen in Ihrem Namen auszuführen. Ein IAM-Administrator kann eine Servicerolle innerhalb von IAM erstellen, ändern und löschen. Weitere Informationen finden Sie unter [Erstellen einer Rolle zum Delegieren von Berechtigungen an einen AWS-Service](#) im IAM-Benutzerhandbuch.

⚠ Warning

Das Ändern der Berechtigungen für eine Servicerolle kann die Funktionalität von Amazon FSx beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Amazon FSx Sie dazu anleitet.

Servicebezogene Rollen für Amazon FSx

Unterstützt serviceverknüpfte Rollen	Ja
--------------------------------------	----

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer Service-Amazon FSx-Rolle verknüpft ist. Die Service-Amazon FSx-Rolle kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Weitere Informationen zum Erstellen und Verwalten von serviceverknüpften Amazon FSx-Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#)

Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Lustre

Standardmäßig sind Benutzer und Rollen nicht berechtigt, Amazon FSx-Ressourcen zu erstellen oder zu ändern. Sie können auch keine Aufgaben mithilfe der AWS Management Console, AWS Command Line Interface (AWS CLI) oder AWS API ausführen. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen. Der Administrator kann dann die IAM-Richtlinien zu Rollen hinzufügen, und Benutzer können die Rollen annehmen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter [Erstellen von IAM-Richtlinien](#) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Amazon FSx definierten Aktionen und Ressourcentypen, einschließlich des Formats der ARNs für jeden Ressourcentyp, finden Sie unter [Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FSx for Lustre](#) in der Service Authorization Reference.

Themen

- [Bewährte Methoden für Richtlinien](#)

- [Verwenden der Amazon FSx-Konsole](#)
- [Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer](#)

Bewährte Methoden für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand Amazon FSx-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Beginnen Sie mit AWS verwalteten Richtlinien und wechseln Sie zu Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter [AWS -verwaltete Richtlinien](#) oder [AWS -verwaltete Richtlinien für Auftrags-Funktionen](#) im IAM-Benutzerhandbuch.
- Anwendung von Berechtigungen mit den geringsten Rechten – Wenn Sie mit IAM-Richtlinien Berechtigungen festlegen, gewähren Sie nur die Berechtigungen, die für die Durchführung einer Aufgabe erforderlich sind. Sie tun dies, indem Sie die Aktionen definieren, die für bestimmte Ressourcen unter bestimmten Bedingungen durchgeführt werden können, auch bekannt als die geringsten Berechtigungen. Weitere Informationen zur Verwendung von IAM zum Anwenden von Berechtigungen finden Sie unter [Richtlinien und Berechtigungen in IAM](#) im IAM-Benutzerhandbuch.
- Verwenden von Bedingungen in IAM-Richtlinien zur weiteren Einschränkung des Zugriffs – Sie können Ihren Richtlinien eine Bedingung hinzufügen, um den Zugriff auf Aktionen und Ressourcen zu beschränken. Sie können beispielsweise eine Richtlinienbedingung schreiben, um festzulegen, dass alle Anforderungen mithilfe von SSL gesendet werden müssen. Sie können auch Bedingungen verwenden, um Zugriff auf Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. AWS CloudFormation B. Weitere Informationen finden Sie unter [IAM-JSON-Richtlinienelemente: Bedingung](#) im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON)

und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter [Richtlinienuvalidierung zum IAM Access Analyzer](#) im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter [Konfigurieren eines MFA-geschützten API-Zugriffs](#) im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter [Bewährte Methoden für die Sicherheit in IAM](#) im IAM-Benutzerhandbuch.

Verwenden der Amazon FSx-Konsole

Um auf die Amazon FSx for Lustre-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon FSx-Ressourcen in Ihrem AWS-Konto aufzulisten und anzuzeigen. Wenn Sie eine identitätsbasierte Richtlinie erstellen, die strenger ist als die mindestens erforderlichen Berechtigungen, funktioniert die Konsole nicht wie vorgesehen für Entitäten (Benutzer oder Rollen) mit dieser Richtlinie.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen weiterhin die Amazon FSx-Konsole verwenden können, fügen Sie den Entitäten auch die `AmazonFSxConsoleReadOnlyAccess` AWS verwaltete Richtlinie hinzu. Weitere Informationen finden Sie unter [Hinzufügen von Berechtigungen zu einem Benutzer](#) im IAM-Benutzerhandbuch.

Sie können die `AmazonFSxConsoleReadOnlyAccess` und andere Amazon FSx Managed Service-Richtlinien unter einsehen. [AWS verwaltete Richtlinien für Amazon FSx](#)

Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

In diesem Beispiel wird gezeigt, wie Sie eine Richtlinie erstellen, die IAM-Benutzern die Berechtigung zum Anzeigen der eingebundenen Richtlinien und verwalteten Richtlinien gewährt, die ihrer Benutzeridentität angefügt sind. Diese Richtlinie beinhaltet Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der AWS CLI API oder der AWS

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupForUser",
        "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 verwaltete Richtlinien für Amazon FSx

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele gängige Anwendungsfälle bereitstellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie allen AWS Kunden zur

Verfügung stehen. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie [kundenverwaltete Richtlinien](#) definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

Weitere Informationen finden Sie unter [Von AWS verwaltete Richtlinien](#) im IAM-Benutzerhandbuch.

AmazonF SxServiceRolePolicy

Ermöglicht Amazon FSx, AWS Ressourcen in Ihrem Namen zu verwalten. Weitere Informationen hierzu finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#).

AWS verwaltete Richtlinie: AmazonF SxDeleteServiceLinkedRoleAccess

Sie können AmazonFSxDeleteServiceLinkedRoleAccess nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einem Service verknüpft und wird nur mit der serviceverknüpften Rolle für diesen Service verwendet. Sie können diese Richtlinie nicht anhängen, trennen, ändern oder löschen. Weitere Informationen finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#).

Diese Richtlinie gewährt Administratorberechtigungen, die es Amazon FSx ermöglichen, seine Service Linked Role für Amazon S3 S3-Zugriff zu löschen, die nur von Amazon FSx for Lustre verwendet wird.

Details zu Berechtigungen

Diese Richtlinie beinhaltet Berechtigungen, die es Amazon FSx ermöglichen, den Löschstaus für die FSx Service Linked Role für Amazon S3 S3-Zugriff einzusehen, zu löschen und einzusehen. iam

Die Berechtigungen für diese Richtlinie finden Sie unter [AmazonF SxDeleteServiceLinkedRoleAccess](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonF SxFullAccess

Sie können AmazonF an Ihre SxFullAccess IAM-Entitäten anhängen. Amazon FSx verknüpft diese Richtlinie auch mit einer Servicerolle, die es Amazon FSx ermöglicht, Aktionen in Ihrem Namen durchzuführen.

Bietet vollen Zugriff auf Amazon FSx und Zugriff auf verwandte AWS Services.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Prinzipalen vollen Zugriff auf die Ausführung aller Amazon FSx-Aktionen, mit Ausnahme von `BypassSnaplockEnterpriseRetention`
- `ds`— Ermöglicht Prinzipalen, Informationen über die Verzeichnisse einzusehen. AWS Directory Service
- `ec2`
 - Ermöglicht Prinzipalen das Erstellen von Tags unter den angegebenen Bedingungen.
 - Um eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.
- `iam`— Ermöglicht Prinzipalen, im Namen des Benutzers eine mit dem Amazon FSx Service verknüpfte Rolle zu erstellen. Dies ist erforderlich, damit Amazon FSx AWS Ressourcen im Namen des Benutzers verwalten kann.
- `logs`— Ermöglicht Prinzipalen, Protokollgruppen zu erstellen, Streams zu protokollieren und Ereignisse in Protokollstreams zu schreiben. Dies ist erforderlich, damit Benutzer FSx for Windows File Server Server-Dateisystemzugriff überwachen können, indem sie CloudWatch Audit-Zugriffsprotokolle an Logs senden.
- `firehose`— Ermöglicht Prinzipalen das Schreiben von Datensätzen in eine Amazon Data Firehose. Dies ist erforderlich, damit Benutzer FSx for Windows File Server Server-Dateisystemzugriff überwachen können, indem sie Audit-Zugriffsprotokolle an Firehose senden.

Die Berechtigungen für diese Richtlinie finden Sie unter [AmazonF SxFullAccess](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonF SxConsoleFullAccess

Sie können die `AmazonFSxConsoleFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die den vollen Zugriff auf Amazon FSx und den Zugriff auf verwandte AWS Dienste über die AWS Management Console ermöglichen.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Principals, alle Aktionen in der Amazon FSx-Managementkonsole auszuführen, mit Ausnahme von `BypassSnaplockEnterpriseRetention`
- `cloudwatch`— Ermöglicht Principals, CloudWatch Alarmlisten und Metriken in der Amazon FSx-Managementkonsole einzusehen.
- `ds`— Ermöglicht Prinzipalen, Informationen über ein Verzeichnis aufzulisten. AWS Directory Service
- `ec2`
 - Ermöglicht Principals, Tags für Routing-Tabellen zu erstellen, Netzwerkschnittstellen, Routing-Tabellen, Sicherheitsgruppen, Subnetze und die mit einem Amazon FSx-Dateisystem verknüpfte VPC aufzulisten.
 - Ermöglicht Prinzipalen die erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen, die mit einer VPC verwendet werden können.
- `kms`— Ermöglicht Prinzipalen, Aliase für Schlüssel aufzulisten. AWS Key Management Service
- `s3`— Ermöglicht Prinzipalen, einige oder alle Objekte in einem Amazon S3 S3-Bucket aufzulisten (bis zu 1000).
- `iam`— Erteilt die Erlaubnis, eine serviceverknüpfte Rolle zu erstellen, die es Amazon FSx ermöglicht, Aktionen im Namen des Benutzers durchzuführen.

Die Berechtigungen für diese Richtlinie finden Sie unter [AmazonF SxConsoleFullAccess](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonF SxConsoleReadOnlyAccess

Sie können die `AmazonFSxConsoleReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Amazon FSx und verwandten AWS Diensten nur Leseberechtigungen, sodass Benutzer Informationen zu diesen Diensten in der einsehen können. AWS Management Console

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Prinzipalen, Informationen über Amazon FSx-Dateisysteme, einschließlich aller Tags, in der Amazon FSx Management Console einzusehen.
- `cloudwatch`— Ermöglicht Principals, CloudWatch Alarmer und Metriken in der Amazon FSx Management Console einzusehen.
- `ds`— Ermöglicht Prinzipalen das Anzeigen von Informationen über ein AWS Directory Service Verzeichnis in der Amazon FSx Management Console.
- `ec2`
 - Ermöglicht Principals die Anzeige von Netzwerkschnittstellen, Sicherheitsgruppen, Subnetzen und der VPC, die einem Amazon FSx-Dateisystem zugeordnet sind, in der Amazon FSx Management Console.
 - Um eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.
- `kms`— Ermöglicht Prinzipalen, Aliase für AWS Key Management Service Schlüssel in der Amazon FSx Management Console einzusehen.
- `log`— Ermöglicht Principals, die Amazon CloudWatch Logs-Protokollgruppen zu beschreiben, die dem Konto zugeordnet sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit Prinzipale die bestehende Konfiguration für die Dateizugriffsüberwachung für ein FSx for Windows File Server Server-Dateisystem einsehen können.
- `firehose`— Ermöglicht Principals, die Amazon Data Firehose-Lieferdatenströme zu beschreiben, die dem Konto zugeordnet sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit Prinzipale die bestehende Konfiguration für die Dateizugriffsüberwachung für ein FSx for Windows File Server Server-Dateisystem einsehen können.

Die Berechtigungen für diese Richtlinie finden Sie unter [AmazonF SxConsoleReadOnlyAccess](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: AmazonF SxReadOnlyAccess

Sie können die AmazonFSxReadOnlYAccess-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Prinzipalen, Informationen über Amazon FSx-Dateisysteme, einschließlich aller Tags, in der Amazon FSx Management Console einzusehen.
- `ec2`— Bereitstellung einer erweiterten Sicherheitsgruppenvalidierung aller Sicherheitsgruppen, die mit einer VPC verwendet werden können.

Die Berechtigungen für diese Richtlinie finden Sie unter [AmazonF SxReadOnlyAccess](#) im Referenzhandbuch für AWS verwaltete Richtlinien.

Amazon FSx-Updates für AWS verwaltete Richtlinien

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon FSx an, seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf der Amazon FSx-Seite, um automatische Benachrichtigungen über Änderungen an dieser [Dokumentverlauf](#) Seite zu erhalten.

Änderung	Beschreibung	Datum
AmazonF SxServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, <code>ec2:GetSecurityGroupsForVpc</code> die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	09. Januar 2024
AmazonF SxReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, <code>ec2:GetSecurityGroupsForVpc</code> die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	09. Januar 2024
AmazonF SxConsoleReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, <code>ec2:GetSecurityGroupsForVpc</code> die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	09. Januar 2024

Änderung	Beschreibung	Datum
	s ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, <code>ec2:GetSecurityGroupsForVpc</code> die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	09. Januar 2024
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, <code>ec2:GetSecurityGroupsForVpc</code> die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	09. Januar 2024

Änderung	Beschreibung	Datum
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, die es Benutzern ermöglicht, regionsübergreifende und kontoübergreifende Datenreplikation für FSx for OpenZFS-Dateisysteme durchzuführen.	20. Dezember 2023
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, die es Benutzern ermöglicht, regionsübergreifende und kontoübergreifende Datenreplikation für FSx for OpenZFS-Dateisysteme durchzuführen.	20. Dezember 2023
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, um Benutzern die On-Demand-Replikation von Volumes für FSx for OpenZFS-Dateisysteme zu ermöglichen.	26. November 2023
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, um Benutzern die On-Demand-Replikation von Volumes für FSx for OpenZFS-Dateisysteme zu ermöglichen.	26. November 2023

Änderung	Beschreibung	Datum
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, mit denen Benutzer die gemeinsame VPC-Unterstützung für FSx for ONTAP Multi-AZ-Dateisysteme anzeigen, aktivieren und deaktivieren können.	14. November 2023
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, mit denen Benutzer die gemeinsame VPC-Unterstützung für FSx for ONTAP Multi-AZ-Dateisysteme anzeigen, aktivieren und deaktivieren können.	14. November 2023
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Netzwerkkonfigurationen für FSx for OpenZFS Multi-AZ-Dateisysteme zu verwalten.	9. August 2023
AWS verwaltete Richtlinien: SxServiceRolePolicy AmazonF — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat die bestehende <code>cloudwatch:PutMetricData</code> Berechtigung geändert, sodass Amazon FSx CloudWatch Metriken im AWS/FSx Namespace veröffentlicht.	24. Juli 2023

Änderung	Beschreibung	Datum
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat die Richtlinie aktualisiert, um die <code>fsx:*</code> Genehmigung zu entfernen und bestimmte <code>fsx</code> Aktionen hinzuzufügen.	13. Juli 2023
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat die Richtlinie aktualisiert, um die <code>fsx:*</code> Genehmigung zu entfernen und bestimmte <code>fsx</code> Aktionen hinzuzufügen.	13. Juli 2023
AmazonF SxConsole ReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, mit denen Benutzer erweiterte Leistungskennzahlen und empfohlene Aktionen für FSx for Windows File Server Server-Dateisysteme in der Amazon FSx-Konsole einsehen können.	21. September 2022
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, mit denen Benutzer erweiterte Leistungskennzahlen und empfohlene Aktionen für FSx for Windows File Server Server-Dateisysteme in der Amazon FSx-Konsole einsehen können.	21. September 2022

Änderung	Beschreibung	Datum
AmazonF SxReadOnlyAccess — Tracking-Richtlinie gestartet	Diese Richtlinie gewährt Lesezugriff auf alle Amazon FSx-Ressourcen und alle damit verbundenen Tags.	4. Februar 2022
AmazonF SxDeleteServiceLinkedRoleAccess — Tracking-Richtlinie gestartet	Diese Richtlinie gewährt Administratorberechtigungen, die es Amazon FSx ermöglichen, seine Service Linked Role für den Zugriff auf Amazon S3 zu löschen.	7. Januar 2022
AmazonF SxServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Netzwerkkonfigurationen für Amazon FSx for NetApp ONTAP-Dateisysteme zu verwalten.	2. September 2021
AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Tags in EC2-Routing-Tabellen für Scoped-Down-Aufrufe zu erstellen.	2. September 2021
AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Amazon FSx für NetApp ONTAP Multi-AZ-Dateisysteme erstellen kann.	2. September 2021

Änderung	Beschreibung	Datum
<p>AmazonFSxConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie</p>	<p>Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Tags in EC2-Routing-Tabellen für Scoped-Down-Aufrufe zu erstellen.</p>	<p>2. September 2021</p>
<p>AmazonFSxServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie</p>	<p>Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, CloudWatch Log-Streams zu beschreiben und in sie zu schreiben.</p> <p>Dies ist erforderlich, damit Benutzer die Dateizugriffsprüfungsprotokolle für FSx for Windows File Server Server-Dateisysteme mithilfe von CloudWatch Logs anzeigen können.</p>	<p>8. Juni 2021</p>
<p>AmazonFSxServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie</p>	<p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Amazon Data Firehose-Lieferstreams beschreiben und in sie schreiben kann.</p> <p>Dies ist erforderlich, damit Benutzer die Dateizugriff-Audit-Logs für ein FSx for Windows File Server Server-Dateisystem mit Amazon Data Firehose einsehen können.</p>	<p>8. Juni 2021</p>

Änderung	Beschreibung	Datum
<p>AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie</p>	<p>Amazon FSx hat neue Berechtigungen hinzugefügt, die es Prinzipalen ermöglichen, Log-Log-Gruppen zu beschreiben und zu erstellen, Streams zu CloudWatch protokollieren und Ereignisse in Log-Streams zu schreiben.</p> <p>Dies ist erforderlich, damit Prinzipale die Dateizugriffsprüfungsprotokolle für FSx for Windows File Server Server-Dateisysteme mithilfe von CloudWatch Protokollen anzeigen können.</p>	<p>8. Juni 2021</p>
<p>AmazonF SxFullAccess — Aktualisierung einer bestehenden Richtlinie</p>	<p>Amazon FSx hat neue Berechtigungen hinzugefügt, um es Prinzipalen zu ermöglichen, Datensätze zu beschreiben und in eine Amazon Data Firehose zu schreiben.</p> <p>Dies ist erforderlich, damit Benutzer die Dateizugriff-Audit-Logs für ein FSx for Windows File Server Server-Dateisystem mit Amazon Data Firehose einsehen können.</p>	<p>8. Juni 2021</p>

Änderung	Beschreibung	Datum
<p>AmazonF SxConsole FullAccess — Aktualisierung einer bestehenden Richtlinie</p>	<p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon CloudWatch Logs-Protokollgruppen beschreiben können, die dem Konto zugeordnet sind, das die Anfrage gestellt hat.</p> <p>Dies ist erforderlich, damit Prinzipale bei der Konfiguration der Dateizugriffsüberwachung für ein FSx for Windows File Server-Datensystem eine vorhandene CloudWatch Protokollgruppe auswählen können.</p>	8. Juni 2021
<p>AmazonF SxConsole FullAccess — Aktualisierung auf eine bestehende Richtlinie</p>	<p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon Data Firehose-Lieferströme beschreiben können, die mit dem Konto verknüpft sind, das die Anfrage gestellt hat.</p> <p>Dies ist erforderlich, damit Principals bei der Konfiguration der Dateizugriffsüberwachung für ein FSx for Windows File Server-Datensystem einen vorhandenen Firehose-Lieferstream auswählen können.</p>	8. Juni 2021

Änderung	Beschreibung	Datum
<p>AmazonF SxConsole ReadOnlyAccess — Aktualisierung auf eine bestehende Richtlinie</p>	<p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon CloudWatch Logs-Protokollgruppen beschreiben können, die dem Konto zugeordnet sind, das die Anfrage gestellt hat.</p> <p>Dies ist erforderlich, damit Prinzipale die bestehende Konfiguration für die Dateizugriffsüberwachung für ein FSx for Windows File Server Server-Dateisystem einsehen können.</p>	8. Juni 2021
<p>AmazonF SxConsole ReadOnlyAccess — Aktualisierung auf eine bestehende Richtlinie</p>	<p>Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon Data Firehose-Lieferströme beschreiben können, die mit dem Konto verknüpft sind, das die Anfrage gestellt hat.</p> <p>Dies ist erforderlich, damit Prinzipale die bestehende Konfiguration für die Dateizugriffsüberwachung für ein FSx for Windows File Server Server-Dateisystem einsehen können.</p>	8. Juni 2021

Änderung	Beschreibung	Datum
Amazon FSx hat begonnen, Änderungen zu verfolgen	Amazon FSx hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	8. Juni 2021

Fehlerbehebung bei Identität und Zugriff auf Amazon FSx for Lustre

Verwenden Sie die folgenden Informationen, um häufig auftretende Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon FSx und IAM auftreten können.

Themen

- [Ich bin nicht berechtigt, eine Aktion in Amazon FSx durchzuführen](#)
- [Ich bin nicht berechtigt, iam auszuführen: PassRole](#)
- [Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon FSx-Ressourcen ermöglichen](#)

Ich bin nicht berechtigt, eine Aktion in Amazon FSx durchzuführen

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven `my-example-widget`-Ressource anzuzeigen, jedoch nicht über `fsx:GetWidget`-Berechtigungen verfügt.

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

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `fsx:GetWidget`-Aktion auf die `my-example-widget`-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam auszuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon FSx übergeben können.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon FSx auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

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

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine Amazon FSx-Ressourcen ermöglichen

Sie können eine Rolle erstellen, die Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation für den Zugriff auf Ihre Ressourcen verwenden können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Im Fall von Diensten, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (Access Control Lists, ACLs) verwenden, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon FSx diese Funktionen unterstützt, finden Sie unter [So funktioniert Amazon FSx for Lustre mit IAM](#).
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter [Gewähren des Zugriffs auf einen IAM-Benutzer in einem anderen AWS-Konto, den Sie besitzen](#).

- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie [AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte](#).
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter [Gewähren von Zugriff für extern authentifizierte Benutzer \(Identitätsverbund\)](#) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter [So unterscheiden sich IAM-Rollen von ressourcenbasierten Richtlinien](#) im IAM-Benutzerhandbuch.

Verwenden von Tags mit Amazon FSx

Sie können Tags zur Steuerung des Zugriffs auf Amazon FSx-Ressourcen verwenden, um eine attributbasierte Zugriffskontrolle (ABAC) zu implementieren. Um während der Erstellung Tags auf Amazon FSx-Ressourcen anzuwenden, müssen Benutzer über bestimmte AWS Identity and Access Management (IAM) -Berechtigungen verfügen.

Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung

Mit einigen Amazon FSx for Lustre-API-Aktionen zur Erstellung von Tags bei der Erstellung der Ressource angegeben werden. Sie können diese Resource-Tags verwenden, um eine attributbasierte Zugriffskontrolle (ABAC) zu implementieren. Weitere Informationen finden Sie unter [Was ist ABAC für AWS?](#) im IAM-Benutzerhandbuch.

Damit Benutzer diese Möglichkeit erhalten, benötigen sie die die die die die die Ressource wie die die die die Ressource erstellt wird, benötigen sie die die die die Ressource wie die die die die Ressource erstellt wird, wie zum Beispielfsx:CreateFileSystem. Wenn Tags in der Aktion angegeben werden, mit der die Ressource erstellt wird, führt IAM eine zusätzliche Autorisierung für die fsx:TagResource -Aktion aus, um die Berechtigungen der Benutzer zum Erstellen von Tags zu überprüfen. Daher benötigen die Benutzer außerdem die expliziten Berechtigungen zum Verwenden der fsx:TagResource-Aktion.

Die folgende Beispielrichtlinie ermöglicht es Benutzern, Dateisysteme zu erstellen und ihnen während der Erstellung in einem bestimmten Bereich Tags zuzuweisen AWS-Konto.

```
{
  "Statement": [
    {
```

```

    "Effect": "Allow",
    "Action": [
      "fsx:CreateFileSystem",
      "fsx:TagResource"
    ],
    "Resource": [
      "arn:aws:fsx:region:account-id:file-system/*"
    ]
  }
]
}

```

In ähnlicher Weise erlaubt die folgende Richtlinie Benutzern, Backups auf einem bestimmten Dateisystem zu erstellen und ihnen dabei beliebige Tags hinzuzufügen.

```

{
  "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/*"
    }
  ]
}

```

Die `fsx:TagResource`-Aktion wird nur ausgewertet, wenn Tags während der Aktion zur Ressourcenerstellung angewendet werden. Folglich benötigt ein Benutzer, der über die Berechtigungen zum Erstellen einer Ressource verfügt (vorausgesetzt, es bestehen keine Markierungsbedingungen), keine Berechtigungen zur Verwendung der `fsx:TagResource`-Aktion, wenn keine Tags in der Anforderung angegeben werden. Wenn der Benutzer allerdings versucht, eine Ressource mit Tags zu erstellen, schlägt die Anforderung fehl, wenn der Benutzer nicht über die Berechtigungen für die `fsx:TagResource`-Aktion verfügt.

Weitere Informationen über das Markieren von Tags von Amazon FSx-Ressourcen mit Tags von Tags von Tags von Tags von Tags [Kennzeichnen Sie Ihre Amazon FSx-Ressourcen](#) von Amazon Weitere Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf Amazon FSx for Lustre-Ressourcen zur Steuerung des Zugriffs mit Tags [Verwenden von mithilfe von von von von von von von von von von von von von FSx von mit](#) zur Steuerung des Zugriffs auf Amazon FSx for Lustre-Ressourcen

Verwenden von mithilfe von von von von von von von von von von von von von von von von FSx von mit

Um den Zugriff auf Amazon FSx-Ressourcen und -Aktionen zu kontrollieren, können Sie IAM-Richtlinien verwenden, die auf Tags basieren. Sie können diese Steuerung auf zwei Arten bereitstellen:

- Sie können den Zugriff auf Amazon FSx-Ressourcen basierend auf Tags auf diesen -Ressourcen steuern.
- Sie können steuern, welche Tags in einer IAM-Anforderungsbedingung übergeben werden können.

Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf AWS Ressourcen finden Sie im IAM-Benutzerhandbuch unter [Steuern des Zugriffs mithilfe von Tags](#). Weitere Informationen über das Markieren von Amazon FSx-Ressourcen bei der Erstellung von Tags von Tags von Tags von Tags von Tags von Tags [Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung](#) von Amazon FSx-Ressourcen Weitere Informationen über das Markieren von -Ressourcen mit Tags von Tags von -Ressourcen mit Tags [Kennzeichnen Sie Ihre Amazon FSx-Ressourcen](#) von Tags von

Zugriffskontrolle mit Tags auf einer Ressource basierend auf Tags auf einer Ressource.

Um zu steuern, welche Aktionen ein Benutzer oder eine Rolle auf einer Amazon FSx-Ressource ausführen kann, können Sie Tags für die Ressource verwenden. Beispielsweise möchten Sie möglicherweise bestimmte API-Operationen für eine Dateisystemressource zulassen oder verweigern, die auf dem Schlüssel-Wert-Paar des Tags für die Ressource basieren.

Example Beispielrichtlinie — Erstellen Sie ein Dateisystem auf, wenn Sie ein bestimmtes Tag angeben

Diese Richtlinie ermöglicht es dem Benutzer, ein Dateisystem nur zu erstellen, wenn er es mit einem bestimmten Tag-Schlüssel-Wertepaar taggt, in diesem Beispiel `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 Beispielrichtlinie — Backups nur auf Dateisystemen mit einem bestimmten Tag erstellen

Diese Richtlinie erlaubt Benutzern, Backups nur auf Dateisystemen zu erstellen, die mit dem Schlüsselwertpaar gekennzeichnet sind `key=Department, value=Finance`, und das Backup wird mit dem Tag erstellt `Department=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 Beispielrichtlinie — Erstellen Sie ein Dateisystem mit einem bestimmten Tag aus Backups mit einem bestimmten Tag

Diese Richtlinie ermöglicht es Benutzern, Dateisysteme, die mit gekennzeichnet sind, `Department=Finance` nur aus Backups zu erstellen, die mit gekennzeichnet sind `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 Beispielrichtlinie — Dateisysteme mit bestimmten Tags löschen

Diese Richtlinie erlaubt einem Benutzer, nur Dateisysteme zu löschen, die Tags mit Tags mit Tags mit Tags mit Tags mit Tags mit Department=Finance Wenn sie ein letztes Backup erstellen, muss es mit markiert werden Department=Finance. Für Lustre-Dateisysteme benötigen Benutzer die fsx:CreateBackup Berechtigung, das endgültige Backup zu erstellen.

```

{
  "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 Beispielrichtlinie — Erstellen Sie Datenrepository-Aufgaben auf Dateisystemen mit einem bestimmten Tag

Diese Richtlinie ermöglicht es Benutzern, Datenrepository-Aufgaben zu erstellen, die mit `Department=Finance` gekennzeichnet sind, und nur auf Dateisystemen, die mit `Department=Finance` gekennzeichnet sind.

```
{
  "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"
        }
      }
    }
  ]
}
```

Verwenden von serviceverknüpften Rollen für Amazon FSx

Amazon FSx verwendet AWS Identity and Access Management (IAM) [serviceverknüpfte](#) Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon FSx verknüpft

ist. Servicebezogene Rollen sind von Amazon FSx vordefiniert und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Services in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle erleichtert die Einrichtung von Amazon FSx, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon FSx definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, kann nur Amazon FSx seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre Amazon FSx-Ressourcen, da Sie nicht versehentlich die Zugriffsberechtigung für die Ressourcen entfernen können.

Informationen zu anderen Services, die serviceorientierte Rollen unterstützen, finden Sie unter [AWS services that work with IAM](#) (-Services, die mit IAM funktionieren). Suchen Sie nach den Services, für die Yes (Ja) in der Spalte Service-linked roles (Serviceorientierte Rollen) angegeben ist. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Servicebezogene Rollenberechtigungen für Amazon FSx

Amazon FSx verwendet zwei mit Services verknüpfte Rollen `AWSServiceRoleForFSxS3Access_fs-01234567890`, die benannt sind `AWSServiceRoleForAmazonFSx` und bestimmte Aktionen in Ihrem Konto ausführen. Beispiele für diese Aktionen sind die Erstellung elastischer Netzwerkschnittstellen für Ihre Dateisysteme in Ihrer VPC und der Zugriff auf Ihr Daten-Repository in einem Amazon S3 S3-Bucket. Denn `AWSServiceRoleForFSxS3Access_fs-01234567890` diese serviceverknüpfte Rolle wird für jedes Amazon FSx for Lustre-Dateisystem erstellt, das Sie erstellen und das mit einem S3-Bucket verknüpft ist.

`AWSServiceRoleForAmazonFSx` Einzelheiten zu den Berechtigungen

Denn `AWSServiceRoleForAmazonFSx` die Rollenberechtigungsrichtlinie ermöglicht es Amazon FSx, die folgenden administrativen Aktionen im Namen des Benutzers für alle zutreffenden AWS Ressourcen durchzuführen:

Aktualisierungen dieser Richtlinie finden Sie unter [AmazonF SxServiceRolePolicy](#)

Note

Das `AWSServiceRoleForAmazonFSx` wird von allen Amazon FSx-Dateisystemtypen verwendet; einige der aufgelisteten Berechtigungen gelten nicht für FSx for Lustre.

- `ds`— Ermöglicht Amazon FSx, Anwendungen in Ihrem Verzeichnis anzuzeigen, zu autorisieren und deren Autorisierung aufzuheben. AWS Directory Service
- `ec2`— Ermöglicht Amazon FSx, Folgendes zu tun:
 - Netzwerkschnittstellen, die mit einem Amazon FSx-Dateisystem verknüpft sind, anzeigen, erstellen und trennen.
 - Zeigen Sie eine oder mehrere Elastic IP-Adressen an, die mit einem Amazon FSx-Dateisystem verknüpft sind.
 - Sehen Sie sich Amazon-VPCs, Sicherheitsgruppen und Subnetze an, die mit einem Amazon FSx-Dateisystem verknüpft sind.
 - Um eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.
 - Erstellen Sie eine Berechtigung für einen AWS-autorisierten Benutzer, bestimmte Operationen an einer Netzwerkschnittstelle auszuführen.
- `cloudwatch`— Ermöglicht Amazon FSx, metrische Datenpunkte CloudWatch unter dem `AWS/FSx`-Namespace zu veröffentlichen.
- `route53`— Ermöglicht Amazon FSx, eine Amazon VPC mit einer privaten gehosteten Zone zu verknüpfen.
- `logs`— Ermöglicht Amazon FSx, CloudWatch Log-Streams zu beschreiben und in sie zu schreiben. Auf diese Weise können Benutzer Dateizugriffs-Auditprotokolle für ein FSx for Windows File Server Server-Dateisystem an einen CloudWatch Logs-Stream senden.
- `firehose`— Ermöglicht Amazon FSx, Amazon Data Firehose-Lieferstreams zu beschreiben und in sie zu schreiben. Auf diese Weise können Benutzer die Dateizugriffs-Audit-Logs für ein FSx for Windows File Server Server-Dateisystem in einem Amazon Data Firehose-Lieferstream veröffentlichen.

```
{  
  "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-*"
  }
]
}

```

Alle Aktualisierungen dieser Richtlinie werden unter [beschrieben](#). [Amazon FSx-Updates für AWS verwaltete Richtlinien](#)

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann.

Weitere Informationen finden Sie unter [Berechtigungen für dienstverknüpfte Rollen](#) im IAM-Benutzerhandbuch.

AWSServiceRoleForFSxS3Access Einzelheiten zu den Berechtigungen

Denn die Rollenberechtigungsrichtlinie ermöglicht es Amazon FSxAWSServiceRoleForFSxS3Access_ *file-system-id*, die folgenden Aktionen auf einem Amazon S3-Bucket durchzuführen, der das Daten-Repository für ein Amazon FSx for Lustre-Dateisystem hostet.

- s3:AbortMultipartUpload

- s3:DeleteObject
- s3:Get*
- s3:List*
- s3:PutBucketNotification
- s3:PutObject

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter [Serviceverknüpfte Rollenberechtigung](#) im IAM-Benutzerhandbuch.

Eine serviceverknüpfte Rolle für Amazon FSx erstellen

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein Dateisystem in der AWS Management Console, der oder der AWS API erstellen AWS CLI, erstellt Amazon FSx die serviceverknüpfte Rolle für Sie.

Important

Diese serviceverknüpfte Rolle kann in Ihrem Konto erscheinen, wenn Sie eine Aktion in einem anderen Service abgeschlossen haben, der die von dieser Rolle unterstützten Features verwendet. Weitere Informationen finden Sie unter [Eine neue Rolle ist in meinem IAM-Konto erschienen](#).

Wenn Sie diese serviceverknüpfte Rolle löschen und sie dann erneut erstellen müssen, können Sie dasselbe Verfahren anwenden, um die Rolle in Ihrem Konto neu anzulegen. Wenn Sie ein Dateisystem erstellen, erstellt Amazon FSx die serviceverknüpfte Rolle erneut für Sie.

Bearbeitung einer serviceverknüpften Rolle für Amazon FSx

Amazon FSx erlaubt Ihnen nicht, diese serviceverknüpften Rollen zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollename nach dem Erstellen einer serviceverknüpften Rolle nicht mehr geändert werden. Sie können jedoch die Beschreibung der Rolle mit IAM bearbeiten. Weitere Informationen finden Sie unter [Bearbeiten einer serviceverknüpften Rolle](#) im IAM-Benutzerhandbuch.

Löschen einer serviceverknüpften Rolle für Amazon FSx

Wenn Sie ein Feature oder einen Dienst, die bzw. der eine serviceverknüpfte Rolle erfordert, nicht mehr benötigen, sollten Sie diese Rolle löschen. Auf diese Weise haben Sie keine ungenutzte juristische Stelle, die nicht aktiv überwacht oder verwaltet wird. Sie müssen jedoch alle Ihre Dateisysteme und Backups löschen, bevor Sie die serviceverknüpfte Rolle manuell löschen können.

Note

Wenn der Amazon FSx-Service die Rolle verwendet, wenn Sie versuchen, die Ressourcen zu löschen, schlägt das Löschen möglicherweise fehl. Wenn dies passiert, warten Sie einige Minuten und versuchen Sie es erneut.

So löschen Sie die serviceverknüpfte Rolle mit IAM

Verwenden Sie die IAM-Konsole, die IAM-CLI oder die IAM-API, um die serviceverknüpfte Rolle zu löschen. `AWSServiceRoleForAmazonFSx` Weitere Informationen finden Sie unter [Löschen einer serviceverknüpften Rolle](#) im IAM-Leitfaden.

Unterstützte Regionen für serviceverknüpfte Amazon FSx-Rollen

Amazon FSx unterstützt die Verwendung von serviceverknüpften Rollen in allen Regionen, in denen der Service verfügbar ist. Weitere Informationen finden Sie unter [AWS Regionen und Endpunkte](#).

Zugriffskontrolle für Dateisysteme mit Amazon VPC

Auf ein Amazon FSx-Dateisystem kann über eine elastic network interface zugegriffen werden, die sich in der Virtual Private Cloud (VPC) befindet, die auf dem Amazon VPC-Service basiert, den Sie mit Ihrem Dateisystem verknüpfen. Sie greifen auf Ihr Amazon FSx-Dateisystem über seinen DNS-Namen zu, der der Netzwerkschnittstelle des Dateisystems zugeordnet ist. Nur Ressourcen innerhalb der zugehörigen VPC oder einer Peer-VPC können auf die Netzwerkschnittstelle Ihres Dateisystems zugreifen. Weitere Informationen finden Sie unter [Was ist Amazon VPC?](#) im Amazon VPC-Benutzerhandbuch.

⚠ Warning

Sie dürfen die elastic network interface von Amazon FSx nicht ändern oder löschen. Das Ändern oder Löschen der Netzwerkschnittstelle kann zu einem dauerhaften Verbindungsverlust zwischen Ihrer VPC und Ihrem Dateisystem führen.

Amazon VPC-Sicherheitsgruppen

Um den Netzwerkverkehr, der über die Netzwerkschnittstelle Ihres Dateisystems innerhalb Ihrer VPC fließt, weiter zu kontrollieren, verwenden Sie Sicherheitsgruppen, um den Zugriff auf Ihre Dateisysteme zu beschränken. Eine Sicherheitsgruppe fungiert als virtuelle Firewall, um den Datenverkehr für die zugehörigen Ressourcen zu kontrollieren. In diesem Fall ist die zugehörige Ressource die Netzwerkschnittstelle Ihres Dateisystems. Sie verwenden auch VPC-Sicherheitsgruppen, um den Netzwerkverkehr für Ihre Lustre-Clients zu steuern.

Steuern des Zugriffs mithilfe von Regeln für eingehenden und ausgehenden Datenverkehr

Um eine Sicherheitsgruppe zur Steuerung des Zugriffs auf Ihr Amazon FSx-Dateisystem und Ihre Lustre-Clients zu verwenden, fügen Sie die eingehenden Regeln zur Steuerung des eingehenden Datenverkehrs und die ausgehenden Regeln zur Steuerung des ausgehenden Datenverkehrs von Ihrem Dateisystem und Lustre-Clients hinzu. Stellen Sie sicher, dass Ihre Sicherheitsgruppe über die richtigen Regeln für den Netzwerkverkehr verfügt, um die Dateifreigabe Ihres Amazon FSx-Dateisystems einem Ordner auf Ihrer unterstützten Compute-Instance zuzuordnen.

Weitere Informationen zu Sicherheitsgruppenregeln finden Sie unter [Sicherheitsgruppenregeln](#) im Amazon EC2 EC2-Benutzerhandbuch.

Um eine Sicherheitsgruppe für Ihr Amazon FSx-Dateisystem zu erstellen

1. Öffnen Sie die Amazon EC2 EC2-Konsole unter <https://console.aws.amazon.com/ec2>.
2. Wählen Sie im Navigationsbereich Sicherheitsgruppen aus.
3. Wählen Sie Create Security Group aus.
4. Geben Sie einen Namen und eine Beschreibung für die Sicherheitsgruppe an.
5. Wählen Sie für VPC die mit Ihrem Amazon FSx-Dateisystem verknüpfte VPC aus, um die Sicherheitsgruppe innerhalb dieser VPC zu erstellen.

6. Wählen Sie Create (Erstellen) aus, um die Sicherheitsgruppe zu erstellen.

Als Nächstes fügen Sie der Sicherheitsgruppe, die Sie gerade erstellt haben, Regeln für eingehenden Datenverkehr hinzu, um den Lustre-Verkehr zwischen Ihren FSx for Lustre-Dateiservern zu aktivieren.

Um Ihrer Sicherheitsgruppe Regeln für eingehenden Datenverkehr hinzuzufügen

1. Wählen Sie die Sicherheitsgruppe aus, die Sie gerade erstellt haben, falls sie noch nicht ausgewählt ist. Wählen Sie unter Actions (Aktionen) die Option Edit inbound rules (Eingangsregeln bearbeiten) aus.
2. Fügen Sie die folgenden Regeln für eingehenden Datenverkehr hinzu.

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-ID der Sicherheitsgruppe ein, die Sie gerade erstellt haben	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre-Dateiservern
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppen ein, die Ihren	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre-Dateiservern und Lustre-Clients

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
			Lustre-Clients zugeordnet sind	
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-ID der Sicherheitsgruppe ein, die Sie gerade erstellt haben	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre Lustre-Dateiservern
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppen ein, die Ihren Lustre-Clients zugeordnet sind	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre-Dateiservern und Lustre-Clients

3. Wählen Sie Speichern, um die neuen Regeln für eingehenden Datenverkehr zu speichern und anzuwenden.

Standardmäßig lassen Sicherheitsgruppenregeln den gesamten ausgehenden Datenverkehr zu (All, 0.0.0.0/0). Wenn Ihre Sicherheitsgruppe nicht den gesamten ausgehenden Datenverkehr zulässt, fügen Sie Ihrer Sicherheitsgruppe die folgenden ausgehenden Regeln hinzu. Diese Regeln ermöglichen den Verkehr zwischen FSx for Lustre-Dateiservern und Lustre-Clients sowie zwischen Lustre-Dateiservern.

So fügen Sie Ihrer Sicherheitsgruppe Regeln für ausgehenden Datenverkehr hinzu

1. Wählen Sie dieselbe Sicherheitsgruppe aus, zu der Sie gerade die Regeln für eingehenden Datenverkehr hinzugefügt haben. Wählen Sie für Aktionen die Option Regeln für ausgehenden Datenverkehr bearbeiten aus.
2. Fügen Sie die folgenden Regeln für ausgehenden Datenverkehr hinzu.

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-ID der Sicherheitsgruppe ein, die Sie gerade erstellt haben	Lustre-Verkehr zwischen FSx for Lustre-Dateiservern zulassen
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppe ein, die Ihren Lustre-Clients zugeordnet ist	Lustre-Verkehr zwischen FSx for Lustre-Dateiservern und Lustre-Clients zulassen
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
			die Sicherheitsgruppen-ID der Sicherheitsgruppe ein, die Sie gerade erstellt haben	Lustre-Da teiservern
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-ID der Sicherheitsgruppe ein, die Ihren Lustre-Clients zugeordnet sind	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre-Da teiservern und Lustre-Clients

3. Wählen Sie Speichern, um die neuen Regeln für ausgehende Nachrichten zu speichern und anzuwenden.

So verknüpfen Sie eine Sicherheitsgruppe mit Ihrem Amazon FSx-Dateisystem

1. Öffnen Sie die Amazon FSx-Konsole unter <https://console.aws.amazon.com/fsx/>.
2. Wählen Sie im Konsolen-Dashboard Ihr Dateisystem aus, um dessen Details einzusehen.
3. Wählen Sie auf der Registerkarte Netzwerk und Sicherheit die Netzwerkschnittstellen-IDs Ihres Dateisystems aus (z. B. ENI-01234567890123456). Dadurch werden Sie zur Amazon EC2 EC2-Konsole weitergeleitet.
4. Wählen Sie jede Netzwerkschnittstellen-ID aus. Jede Aktion öffnet eine neue Instanz der Amazon EC2 EC2-Konsole in Ihrem Browser. Wählen Sie für jede Sicherheitsgruppe die Option Sicherheitsgruppen für Aktionen ändern aus.
5. Wählen Sie im Dialogfeld „Sicherheitsgruppen ändern“ die zu verwendenden Sicherheitsgruppen aus und klicken Sie auf Speichern.

VPC-Sicherheitsgruppenregeln für Lustre-Clients

Sie verwenden VPC-Sicherheitsgruppen, um den Zugriff auf Ihre Lustre-Clients zu kontrollieren, indem Sie eingehende Regeln zur Steuerung des eingehenden Datenverkehrs und ausgehende Regeln zur Steuerung des ausgehenden Datenverkehrs von Ihren Lustre-Clients hinzufügen. Stellen Sie sicher, dass Ihre Sicherheitsgruppe über die richtigen Regeln für den Netzwerkverkehr verfügt, um sicherzustellen, dass Lustre-Verkehr zwischen Ihren Lustre-Clients und Ihren Amazon FSx-Dateisystemen fließen kann.

Fügen Sie den Sicherheitsgruppen, die auf Ihre Lustre-Clients angewendet werden, die folgenden Regeln für eingehenden Datenverkehr hinzu.

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppen ein, die auf Ihre Lustre-Clients angewendet werden	Ermöglicht Lustre-Verkehr zwischen Lustre-Clients
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppen ein, die Ihren FSx for Lustre-Data	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre-Data-Servern und Lustre-Clients

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
			teisystemen zugeordnet sind	
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppen ein, die auf Ihre Lustre-Clients angewendet werden	Ermöglicht Lustre-Verkehr zwischen Lustre-Clients
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppen ein, die Ihren FSx for Lustre-Datensystemen zugeordnet sind	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre-Datenservern und Lustre-Clients

Fügen Sie den Sicherheitsgruppen, die auf Ihre Lustre-Clients angewendet werden, die folgenden Regeln für ausgehenden Datenverkehr hinzu.

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppen ein, die auf Ihre Lustre-Clients angewendet werden	Ermöglicht Lustre-Verkehr zwischen Lustre-Clients
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppen ein, die Ihren FSx for Lustre-Datensystemen zugeordnet sind	Lustre-Verkehr zwischen FSx for Lustre-Datensystemen und Lustre-Clients zulassen
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppen ein, die auf Ihre Lustre-Clients	Ermöglicht Lustre-Verkehr zwischen Lustre-Clients

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
			angewendet werden	
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-IDs der Sicherheitsgruppen ein, die Ihren FSx for Lustre-Datensystemen zugeordnet sind	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre-Datenservern und Lustre-Clients

Amazon VPC-Netzwerk-ACLs

Eine weitere Möglichkeit, den Zugriff auf das Dateisystem in Ihrer VPC zu sichern, besteht darin, Netzwerkzugriffskontrolllisten (Netzwerk-ACLs) einzurichten. Netzwerk-ACLs sind von Sicherheitsgruppen getrennt, verfügen jedoch über ähnliche Funktionen, um den Ressourcen in Ihrer VPC eine zusätzliche Sicherheitsebene hinzuzufügen. Weitere Informationen zur Implementierung der Zugriffskontrolle mithilfe von Netzwerk-ACLs finden Sie unter [Steuern des Datenverkehrs zu Subnetzen mithilfe von Netzwerk-ACLs](#) im Amazon VPC-Benutzerhandbuch.


Konformitätsvalidierung für Amazon FSx for Lustre

Informationen darüber, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter [AWS-Services Umfang nach Compliance-Programm unter Umfang nach Compliance-Programm AWS-Services](#) das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter [AWS Compliance-Programme AWS](#).

Sie können Prüfberichte von Drittanbietern unter heruntergeladen AWS Artifact. Weitere Informationen finden Sie unter [Berichte heruntergeladen unter](#).

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften ab. AWS stellt die folgenden Ressourcen zur Verfügung, die Sie bei der Einhaltung der Vorschriften unterstützen:

- [Schnellstartanleitungen zu Sicherheit und Compliance](#) — In diesen Bereitstellungsleitfäden werden architektonische Überlegungen erörtert und Schritte für die Implementierung von Basisumgebungen beschrieben AWS , bei denen Sicherheit und Compliance im Mittelpunkt stehen.
- [Architecting for HIPAA Security and Compliance on Amazon Web Services](#) — In diesem Whitepaper wird beschrieben, wie Unternehmen HIPAA-fähige Anwendungen erstellen AWS können.

 Note

AWS-Services Nicht alle sind HIPAA-fähig. Weitere Informationen finden Sie in der [Referenz für HIPAA-berechtigte Services](#).

- [AWS Compliance-Ressourcen](#) — Diese Sammlung von Arbeitsmappen und Leitfäden gilt möglicherweise für Ihre Branche und Ihren Standort.
- [AWS Leitfäden zur Einhaltung von Vorschriften für Kunden](#) — Verstehen Sie das Modell der gemeinsamen Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Verfahren zur Sicherung zusammengefasst AWS-Services und die Leitlinien den Sicherheitskontrollen in verschiedenen Frameworks (einschließlich des National Institute of Standards and Technology (NIST), des Payment Card Industry Security Standards Council (PCI) und der International Organization for Standardization (ISO)) zugeordnet.
- [Evaluierung von Ressourcen anhand von Regeln](#) im AWS Config Entwicklerhandbuch — Der AWS Config Service bewertet, wie gut Ihre Ressourcenkonfigurationen den internen Praktiken, Branchenrichtlinien und Vorschriften entsprechen.
- [AWS Security Hub](#) — Auf diese AWS-Service Weise erhalten Sie einen umfassenden Überblick über Ihren internen Sicherheitsstatus. AWS Security Hub verwendet Sicherheitskontrollen, um Ihre AWS -Ressourcen zu bewerten und Ihre Einhaltung von Sicherheitsstandards und bewährten Methoden zu überprüfen. Eine Liste der unterstützten Services und Kontrollen finden Sie in der [Security-Hub-Steuerungsreferenz](#).
- [Amazon GuardDuty](#) — Dies AWS-Service erkennt potenzielle Bedrohungen für Ihre Workloads AWS-Konten, Container und Daten, indem es Ihre Umgebung auf verdächtige und böswillige Aktivitäten überwacht. GuardDuty kann Ihnen helfen, verschiedene Compliance-Anforderungen

wie PCI DSS zu erfüllen, indem es die in bestimmten Compliance-Frameworks vorgeschriebenen Anforderungen zur Erkennung von Eindringlingen erfüllt.

- [AWS Audit Manager](#)— Auf diese AWS-Service Weise können Sie Ihre AWS Nutzung kontinuierlich überprüfen, um das Risikomanagement und die Einhaltung von Vorschriften und Industriestandards zu vereinfachen.

Amazon FSx for Lustre und VPC-Schnittstellen-Endpunkte (AWS PrivateLink)

Sie können die Sicherheitslage Ihrer VPC verbessern, indem Sie Amazon FSx so konfigurieren, dass es einen VPC-Endpunkt mit Schnittstelle verwendet. Interface VPC-Endpoints werden von einer Technologie unterstützt [AWS PrivateLink](#), mit der Sie privat auf Amazon FSx-APIs zugreifen können, ohne dass ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder eine Verbindung erforderlich ist. AWS Direct Connect Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Amazon FSx-APIs zu kommunizieren. Der Verkehr zwischen Ihrer VPC und Amazon FSx verlässt das AWS Netzwerk nicht.

Jeder Schnittstellen-VPC-Endpunkt wird durch eine oder mehrere elastische Netzwerkschnittstellen in Ihren Subnetzen repräsentiert. Eine Netzwerkschnittstelle stellt eine private IP-Adresse bereit, die als Einstiegspunkt für den Datenverkehr zur Amazon FSx-API dient.

Überlegungen zu VPC-Endpunkten mit Amazon FSx-Schnittstelle

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Amazon FSx einrichten, sollten Sie die [Eigenschaften und Einschränkungen von Interface VPC-Endpunkten](#) im Amazon VPC-Benutzerhandbuch lesen.

Sie können alle Amazon FSx-API-Operationen von Ihrer VPC aus aufrufen. Sie können beispielsweise ein FSx for Lustre-Dateisystem erstellen, indem Sie die CreateFileSystem API von Ihrer VPC aus aufrufen. Die vollständige Liste der Amazon FSx-APIs finden Sie unter [Aktionen](#) in der Amazon FSx-API-Referenz.

Überlegungen zum VPC-Peering

Sie können andere VPCs mithilfe von VPC-Peering mit der VPC über Schnittstellen-VPC-Endpunkte verbinden. VPC-Peering ist eine Netzwerkverbindung zwischen zwei VPCs. Sie können eine VPC-

Peering-Verbindung zwischen Ihren eigenen beiden VPCs oder mit einer VPC in einer anderen herstellen. AWS-Konto Die VPCs können sich auch in zwei verschiedenen Versionen befinden. AWS-Regionen

Der Verkehr zwischen Peer-VPCs verbleibt im AWS Netzwerk und durchquert nicht das öffentliche Internet. Sobald VPCs miteinander verbunden sind, können Ressourcen wie Amazon Elastic Compute Cloud (Amazon EC2) -Instances in beiden VPCs über Schnittstellen-VPC-Endpunkte, die in einer der VPCs erstellt wurden, auf die Amazon FSx-API zugreifen.

Erstellen eines VPC-Schnittstellen-Endpunkts für Amazon FSx API

Sie können einen VPC-Endpunkt für die Amazon FSx-API entweder mit der Amazon VPC-Konsole oder mit () erstellen. AWS Command Line Interface AWS CLI Weitere Informationen finden Sie unter [Erstellen eines Schnittstellen-VPC-Endpunkts](#) im Amazon VPC-Benutzerhandbuch.

Eine vollständige Liste der Amazon FSx-Endpunkte finden Sie unter [Amazon FSx-Endpunkte und Kontingente](#) in der. Allgemeine Amazon Web Services-Referenz

Verwenden Sie eine der folgenden Methoden, um einen VPC-Schnittstellen-Endpunkt für Amazon FSx zu erstellen:

- **com.amazonaws.*region*.fsx**— Erzeugt einen Endpunkt für Amazon FSx-API-Operationen.
- **com.amazonaws.*region*.fsx-fips**— Erstellt einen Endpunkt für die Amazon FSx-API, der dem [Federal Information Processing Standard \(FIPS\) 140-2](#) entspricht.

Um die private DNS-Option zu verwenden, müssen Sie die `enableDnsSupport` Attribute `enableDnsHostnames` und für Ihre VPC festlegen. Weitere Informationen finden Sie unter [DNS-Unterstützung für Ihre VPC anzeigen und aktualisieren](#) im Amazon VPC-Benutzerhandbuch.

Mit Ausnahme AWS-Regionen von China können Sie, wenn Sie privates DNS für den Endpunkt aktivieren, API-Anfragen an Amazon FSx mit dem VPC-Endpunkt stellen AWS-Region, indem Sie beispielsweise seinen Standard-DNS-Namen für verwenden. `fsx.us-east-1.amazonaws.com` Für China (Peking) und China (Ningxia) AWS-Regionen können Sie API-Anfragen mit dem VPC-Endpunkt jeweils mit `fsx-api.cn-north-1.amazonaws.com.cn` und `fsx-api.cn-northwest-1.amazonaws.com.cn` stellen.

Weitere Informationen finden Sie unter [Zugreifen auf einen Service über einen Schnittstellen-VPC-Endpunkt](#) im Amazon VPC-Benutzerhandbuch.

Erstellen einer VPC-Endpunktrichtlinie für Amazon FSx

Um den Zugriff auf die Amazon FSx-API weiter zu kontrollieren, können Sie optional eine AWS Identity and Access Management (IAM-) Richtlinie an Ihren VPC-Endpunkt anhängen. Die Richtlinie legt Folgendes fest:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter [Steuerung des Zugriffs auf Services mit VPC-Endpunkten](#) im Amazon-VPC-Benutzerhandbuch.

Kontingente

Im Folgenden erfahren Sie mehr über Kontingente bei der Arbeit mit Amazon FSx for Lustre.

Themen

- [Kontingente, die Sie erhöhen können](#)
- [Ressourcenkontingente für jedes Dateisystem](#)
- [Weitere Überlegungen](#)

Kontingente, die Sie erhöhen können

Im Folgenden finden Sie die Kontingente für Amazon FSx for Lustre pro AWS Konto und AWS Region, die Sie erhöhen können.

Ressource	Standard	Beschreibung
Dateisysteme Lustre Persisten t_1	100	Die maximale Anzahl von Amazon FSx for Lustre Persistent_1-Dateisystemen, die Sie in diesem Konto erstellen können.
Dateisysteme Lustre Persisten t_2	100	Die maximale Anzahl von Amazon FSx for Lustre Persistent_2-Dateisystemen, die Sie in diesem Konto erstellen können.
Lustre-Persistent-HDD-Speicherkapazität (pro Dateisystem)	102000	Die maximale Festplattenspeicherkapazität (in GiB), die Sie für ein persistentes Dateisystem von Amazon FSx für Lustre konfigurieren können.

Ressource	Standard	Beschreibung
Lustre Persistent_1 Dateispeicherkapazität	100800	Die maximale Speicherkapazität (in GiB), die Sie für alle Amazon FSx for Lustre Persistent_1-Dateisysteme in diesem Konto konfigurieren können.
Lustre Persistent_2 Dateispeicherkapazität	100800	Die maximale Speicherkapazität (in GiB), die Sie für alle Amazon FSx for Lustre Persistent_2 Dateisysteme in diesem Konto konfigurieren können.
Lustre-Scratch-Dateisysteme	100	Die maximale Anzahl der Dateisysteme von Amazon FSx für Lustre scratch, die Sie in diesem Konto erstellen können.
Lustre-Scratch-Speicherkapazität	100800	Die maximale Speicherkapazität (in GiB), die Sie für alle Dateisysteme von Amazon FSx für Lustre scratch in diesem Konto konfigurieren können.
Lustre-Backups	500	Die maximale Anzahl der vom Benutzer initiierten Backups, die Sie für alle Dateisysteme von Amazon FSx für Lustre in diesem Konto haben können.

So fordern Sie eine Kontingenterhöhung an

1. Öffnen Sie die [Service Quotas-Konsole](#).
2. Wählen Sie im Navigationsbereich AWS -Services.
3. Wählen Sie Amazon FSx.
4. Wählen Sie ein Kontingent.
5. Wählen Sie „Kontingenterhöhung beantragen“ und folgen Sie den Anweisungen, um eine Kontingenterhöhung zu beantragen.
6. Um den Status der Kontingentanfrage einzusehen, wählen Sie im Navigationsbereich der Konsole die Option Kontingentanforderungsverlauf aus.

Weitere Informationen finden Sie unter [Beantragen einer Kontingenterhöhung](#) im Service-Quotas-Benutzerhandbuch.

Ressourcenkontingente für jedes Dateisystem

Im Folgenden sind die Beschränkungen der Amazon FSx for Lustre-Ressourcen für jedes Dateisystem in einer AWS Region aufgeführt.

Ressource	Limit pro Dateisystem
Maximale Anzahl von Tags	50
Maximale Aufbewahrungsdauer für automatisierte Backups	90 Tage
Maximale Anzahl laufender Backup-Kopie-Anfragen an eine einzelne Zielregion pro Konto.	5
Anzahl der Dateiaktualisierungen aus dem verknüpften S3-Bucket pro Dateisystem	10 Millionen pro Monat
Mindestspeicherkapazität, SSD-Dateisysteme	1,2 TiB
Mindestspeicherkapazität, HDD-Dateisysteme	6 TiB
Minimaler Durchsatz pro Speichereinheit, SSD	50 Mbit/s

Ressource	Limit pro Dateisystem
Maximaler Durchsatz pro Speichereinheit, SSD	1000 Mbit/s
Minstdurchsatz pro Speichereinheit, HDD	12 MBps
Maximaler Durchsatz pro Speichereinheit, HDD	40 Mbit/s

Weitere Überlegungen

Beachten Sie außerdem Folgendes:

- Sie können jede Taste AWS Key Management Service (AWS KMS) auf bis zu 125 Amazon FSx for Lustre-Dateisystemen verwenden.
- Eine Liste der AWS Regionen, in denen Sie Dateisysteme erstellen können, finden Sie unter [Amazon FSx Endpoints and Quotas in der](#) Allgemeinen AWS-Referenz

Fehlerbehebung

Verwenden Sie die folgenden Informationen, um Probleme zu lösen, die bei der Arbeit mit Amazon FSx for Lustre-Dateisystemen auftreten können.

Wenn Sie auf Probleme stoßen, die im Folgenden nicht aufgeführt sind, versuchen Sie, eine Frage im [Amazon FSx for Lustre-Forum](#) zu stellen.

Themen

- [Der Versuch, ein FSx for Lustre-Dateisystem zu erstellen, schlägt fehl](#)
- [Behebung von Problemen beim Einhängen des Dateisystems](#)
- [Sie können nicht auf Ihr Dateisystem zugreifen](#)
- [Der Zugriff auf einen S3-Bucket konnte beim Erstellen einer Datenrepository-Zuordnung nicht validiert werden](#)
- [Das Umbenennen von Verzeichnissen dauert sehr lange](#)
- [Fehlerbehebung bei einem falsch konfigurierten verknüpften S3-Bucket](#)
- [Fehlerbehebung bei Speicherproblemen](#)
- [Behebung von FSx for Lustre CSI-Treiberproblemen](#)

Der Versuch, ein FSx for Lustre-Dateisystem zu erstellen, schlägt fehl

Es gibt eine Reihe möglicher Ursachen, wenn eine Anfrage zur Erstellung eines Dateisystems fehlschlägt, wie in den folgenden Themen beschrieben.

Aufgrund einer falsch konfigurierten Sicherheitsgruppe kann kein Dateisystem erstellt werden

Das Erstellen eines FSx for Lustre-Dateisystems schlägt mit der folgenden Fehlermeldung fehl:

```
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
```

Maßnahme

Stellen Sie sicher, dass die VPC-Sicherheitsgruppe, die Sie für den Erstellungsvorgang verwenden, wie unter beschrieben konfiguriert ist. [Zugriffskontrolle für Dateisysteme mit Amazon VPC](#) Sie müssen die Sicherheitsgruppe so einrichten, dass eingehender Datenverkehr über die Ports 988 und 1018-1023 von der Sicherheitsgruppe selbst oder vom gesamten Subnetz CIDR zugelassen wird, was erforderlich ist, damit die Dateisystemhosts miteinander kommunizieren können.

Es kann kein Dateisystem erstellt werden, das mit einem S3-Bucket verknüpft ist

Wenn das Erstellen eines neuen Dateisystems, das mit einem S3-Bucket verknüpft ist, fehlschlägt und eine Fehlermeldung ähnlich der folgenden angezeigt wird.

```
User: arn:aws:iam::012345678901:user/username is not authorized to perform:  
iam:PutRolePolicy on resource: resource ARN
```

Dieser Fehler kann auftreten, wenn Sie versuchen, ein mit einem Amazon S3 S3-Bucket verknüpftes Dateisystem ohne die erforderlichen IAM-Berechtigungen zu erstellen. Die erforderlichen IAM-Berechtigungen unterstützen die serviceverknüpfte Rolle Amazon FSx for Lustre, die für den Zugriff auf den angegebenen Amazon S3 S3-Bucket in Ihrem Namen verwendet wird.

Maßnahme

Stellen Sie sicher, dass Ihre IAM-Entität (Benutzer, Gruppe oder Rolle) über die entsprechenden Berechtigungen zum Erstellen von Dateisystemen verfügt. Dazu gehört das Hinzufügen der Berechtigungsrichtlinie, die die serviceverknüpfte Rolle Amazon FSx for Lustre unterstützt. Weitere Informationen finden Sie unter [Hinzufügen von Berechtigungen zur Verwendung von Datenrepositories in Amazon S3](#).

Weitere Informationen zu serviceverknüpften Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#).

Behebung von Problemen beim Einhängen des Dateisystems

Es gibt eine Reihe möglicher Ursachen, wenn ein Befehl zum Einhängen eines Dateisystems fehlschlägt, wie in den folgenden Themen beschrieben.

Das Einhängen des Dateisystems schlägt sofort fehl

Der Befehl zum Einhängen des Dateisystems schlägt sofort fehl. Der folgende Code zeigt ein Beispiel dafür.

```
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?
```

Dieser Fehler kann auftreten, wenn Sie beim Mounten eines persistenten Dateisystems oder eines Scratch-2-Dateisystems mithilfe des mount Befehls nicht den richtigen mountname Wert verwenden. Sie können den mountname Wert aus der Antwort des [describe-file-systems](#) AWS CLI Befehls oder der [DescribeFileSystems](#)API-Operation abrufen.

Das Mounting des Dateisystems hängt und schlägt dann mit einem Timeout-Fehler fehl

Der Mounting-Befehl des Dateisystems hängt eine oder zwei Minuten lang und schlägt dann mit einem Timeout-Fehler fehl.

Der folgende Code zeigt ein Beispiel dafür.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx

[2+ minute wait here]
Connection timed out
```

Dieser Fehler kann auftreten, weil die Sicherheitsgruppen für die Amazon EC2 EC2-Instance oder das Dateisystem nicht richtig konfiguriert sind.

Maßnahme

Stellen Sie sicher, dass Ihre Sicherheitsgruppen für das Dateisystem die unter angegebenen Regeln für eingehenden Datenverkehr haben. [Amazon VPC-Sicherheitsgruppen](#)

Automatisches Mounting schlägt fehl und die Instance reagiert nicht

In einigen Fällen schlägt das automatische Mounten für ein Dateisystem möglicherweise fehl und Ihre Amazon EC2 EC2-Instance reagiert möglicherweise nicht mehr.

Dieses Problem kann auftreten, wenn die `_netdev` Option nicht deklariert wurde. Wenn `_netdev` es fehlt, reagiert Ihre Amazon EC2 EC2-Instance möglicherweise nicht mehr. Der Grund dafür ist, dass zuerst das Netzwerk auf der Datenverarbeitungs-Instance gestartet worden sein muss. Die Netzwerkdateisysteme müssen danach initialisiert werden.

Maßnahme

Wenn dieses Problem auftritt, wenden Sie sich an AWS Support.

Das Einhängen des Dateisystems schlägt beim Systemstart fehl

Das Einhängen des Dateisystems schlägt beim Systemstart fehl. Die Montage erfolgt automatisiert mit `/etc/fstab`. Wenn das Dateisystem nicht gemountet ist, wird im Syslog für den Zeitraum, in dem die Instanz gestartet wurde, der folgende Fehler angezeigt.

```
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
```

Dieser Fehler kann auftreten, wenn Port 988 nicht verfügbar ist. Wenn die Instanz für das Mounten von NFS-Dateisystemen konfiguriert ist, ist es möglich, dass die NFS-Mounts ihren Client-Port an Port 988 binden

Maßnahme

Sie können dieses Problem umgehen, indem Sie die Optionen des NFS-Clients `noresvport` und `noauto` der Mount-Optionen nach Möglichkeit anpassen.

Das Einhängen des Dateisystems mithilfe des DNS-Namens schlägt fehl

Falsch konfigurierte DNS-Namen (Domain Name Service) können zu Fehlern beim Einhängen des Dateisystems führen, wie in den folgenden Szenarien gezeigt.

Szenario 1: Eine Dateisystembereitstellung, die einen DNS-Namen (Domain Name Service) verwendet, schlägt fehl. Der folgende Code zeigt ein Beispiel dafür.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: Can't parse NID
```

```
'file_system_dns_name@tcp:/mountname'
```

Maßnahme

Überprüfen Sie Ihre Virtual Private Cloud (VPC) -Konfiguration. Wenn Sie eine benutzerdefinierte VPC verwenden, müssen Sie sicherstellen, dass die DNS-Einstellungen aktiviert sind.

Weitere Informationen finden Sie unter [Verwendung von DNS in Ihrer VPC](#) im Amazon VPC Benutzerhandbuch.

Gehen Sie wie folgt vor, um im mount Befehl einen DNS-Namen anzugeben:

- Stellen Sie sicher, dass sich die Amazon EC2 EC2-Instance in derselben VPC wie Ihr Amazon FSx for Lustre-Dateisystem befindet.
- Connect Ihre Amazon EC2 EC2-Instance innerhalb einer VPC, die für die Nutzung des von Amazon bereitgestellten DNS-Servers konfiguriert ist. Weitere Informationen finden Sie unter [DHCP Options Sets](#) im Amazon VPC-Benutzerhandbuch.
- Stellen Sie sicher, dass in der Amazon VPC der verbindenden Amazon EC2 EC2-Instance DNS-Hostnamen aktiviert sind. Weitere Informationen finden Sie unter [Aktualisieren der DNS-Unterstützung für Ihre VPC](#) im Amazon VPC-Benutzerhandbuch.

Szenario 2: Ein Dateisystem-Mount, der einen DNS-Namen (Domain Name Service) verwendet, schlägt fehl. Der folgende Code zeigt ein Beispiel dafür.

```
mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: mount file_system_dns_name@tcp:/mountname at /mnt/fsx failed: Input/
output error Is the MGS running?
```

Maßnahme

Stellen Sie sicher, dass auf die VPC-Sicherheitsgruppen des Clients die richtigen Regeln für ausgehenden Datenverkehr angewendet werden. Diese Empfehlung gilt insbesondere dann, wenn Sie die Standardsicherheitsgruppe nicht verwenden oder wenn Sie die Standardsicherheitsgruppe geändert haben. Weitere Informationen finden Sie unter [Amazon VPC-Sicherheitsgruppen](#).

Sie können nicht auf Ihr Dateisystem zugreifen

Es gibt eine Reihe möglicher Ursachen dafür, dass Sie nicht auf Ihr Dateisystem zugreifen können. Jede hat ihre eigene Auflösung, wie folgt.

Die Elastic IP-Adresse, die an die elastic network interface des Dateisystems angehängt ist, wurde gelöscht

Amazon FSx unterstützt nicht den Zugriff auf Dateisysteme über das öffentliche Internet. Amazon FSx trennt automatisch jede Elastic IP-Adresse, bei der es sich um eine öffentliche IP-Adresse handelt, die über das Internet erreichbar ist und die an die elastic network interface eines Dateisystems angehängt wird.

Die elastic network interface des Dateisystems wurde geändert oder gelöscht

Sie dürfen die elastic network interface des Dateisystems nicht ändern oder löschen. Das Ändern oder Löschen der Netzwerkschnittstelle kann zu einem dauerhaften Verbindungsverlust zwischen Ihrer VPC und Ihrem Dateisystem führen. Erstellen Sie ein neues Dateisystem und ändern oder löschen Sie die FSx elastic network interface nicht. Weitere Informationen finden Sie unter [Zugriffskontrolle für Dateisysteme mit Amazon VPC](#).

Der Zugriff auf einen S3-Bucket konnte beim Erstellen einer Datenrepository-Zuordnung nicht validiert werden

Das Erstellen einer Data Repository Association (DRA) über die Amazon FSx-Konsole oder mithilfe des `create-data-repository-association` CLI-Befehls ([CreateDataRepositoryAssociation](#) entspricht der entsprechenden API-Aktion) schlägt mit der folgenden Fehlermeldung fehl.

```
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

Der obige Fehler kann auch auftreten, wenn Sie ein Scratch 1-, Scratch 2- oder Persistent 1-Dateisystem erstellen, das mit einem Datenrepository (S3-Bucket oder Präfix) verknüpft ist, indem Sie die Amazon FSx-Konsole oder den `create-file-system` CLI-Befehl verwenden ([CreateFileSystem](#) ist die entsprechende API-Aktion).

Maßnahme

Wenn sich das FSx for Lustre-Dateisystem in demselben Konto wie der S3-Bucket befindet, bedeutet dieser Fehler, dass die IAM-Rolle, die Sie für die Erstellungsanforderung verwendet haben, nicht über die erforderlichen Berechtigungen für den Zugriff auf den S3-Bucket verfügt. Stellen Sie sicher, dass die IAM-Rolle über die in der Fehlermeldung aufgeführten Berechtigungen verfügt. Diese Berechtigungen unterstützen die serviceverknüpfte Rolle Amazon FSx for Lustre, die für den Zugriff auf den angegebenen Amazon S3 S3-Bucket in Ihrem Namen verwendet wird.

Wenn sich das FSx for Lustre-Dateisystem in einem anderen Konto als der S3-Bucket befindet (kontoübergreifender Fall), sollte zusätzlich zur Sicherstellung, dass die von Ihnen verwendete IAM-Rolle über die erforderlichen Berechtigungen verfügt, die S3-Bucket-Richtlinie so konfiguriert werden, dass sie den Zugriff von dem Konto aus ermöglicht, in dem FSx for Lustre erstellt wurde. Im Folgenden finden Sie ein Beispiel für eine Bucket-Richtlinie:

```
{
  "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-*"
          ]
        }
      }
    }
  ]
}
```

```
}  
  }  
    }  
      ]  
        }
```

Weitere Informationen zu kontoübergreifenden S3-Bucket-Berechtigungen finden Sie unter [Beispiel 2: Bucket-Besitzer, der kontoübergreifende Bucket-Berechtigungen gewährt](#) im Amazon Simple Storage Service-Benutzerhandbuch.

Das Umbenennen von Verzeichnissen dauert sehr lange

Frage

Ich habe ein Verzeichnis in einem Dateisystem umbenannt, das mit einem Amazon S3 S3-Bucket verknüpft ist, und habe den automatischen Export aktiviert. Warum dauert es lange, bis die Dateien in diesem Verzeichnis im S3-Bucket umbenannt werden?

Antwort

Wenn Sie ein Verzeichnis im Dateisystem umbenennen, erstellt FSx for Lustre neue S3-Objekte für alle Dateien und Verzeichnisse in dem Verzeichnis, das umbenannt wurde. Die Zeit, die benötigt wird, um die Verzeichnisumbenennung auf S3 zu übertragen, steht in direktem Zusammenhang mit der Anzahl der Dateien und Verzeichnisse, die von dem umzubenennenden Verzeichnis abstammen.

Fehlerbehebung bei einem falsch konfigurierten verknüpften S3-Bucket

In einigen Fällen kann der verknüpfte S3-Bucket eines FSx for Lustre-Dateisystems einen falsch konfigurierten Lebenszyklusstatus des Datenrepositorys aufweisen.

Mögliche Ursache

Dieser Fehler kann auftreten, wenn Amazon FSx nicht über die erforderlichen AWS Identity and Access Management (IAM-) Berechtigungen verfügt, die für den Zugriff auf das Linked Data Repository erforderlich sind. Die erforderlichen IAM-Berechtigungen unterstützen die serviceverknüpfte Rolle Amazon FSx for Lustre, die für den Zugriff auf den angegebenen Amazon S3 S3-Bucket in Ihrem Namen verwendet wird.

Maßnahme

1. Stellen Sie sicher, dass Ihre IAM-Entität (Benutzer, Gruppe oder Rolle) über die entsprechenden Berechtigungen zum Erstellen von Dateisystemen verfügt. Dazu gehört das Hinzufügen der Berechtigungsrichtlinie, die die serviceverknüpfte Rolle Amazon FSx for Lustre unterstützt. Weitere Informationen finden Sie unter [Hinzufügen von Berechtigungen zur Verwendung von Datenrepositoys in Amazon S3](#).
2. Aktualisieren Sie mithilfe der Amazon FSx CLI oder API die Dateisysteme AutoImportPolicy mit dem `update-file-system` CLI-Befehl ([UpdateFileSystem](#) entspricht der entsprechenden API-Aktion) wie folgt.

```
aws fsx update-file-system \  
--file-system-id fs-0123456789abcdef0 \  
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Weitere Informationen zu serviceverknüpften Rollen finden Sie unter [Verwenden von serviceverknüpften Rollen für Amazon FSx](#).

Mögliche Ursache

Dieser Fehler kann auftreten, wenn das verknüpfte Amazon S3 S3-Daten-Repository über eine bestehende Konfiguration für Ereignisbenachrichtigungen mit Ereignistypen verfügt, die sich mit der Amazon FSx-Konfiguration für Ereignisbenachrichtigungen überschneiden (`s3:ObjectCreated:*`, `s3:ObjectRemoved:*`).

Dies kann auch der Fall sein, wenn die Konfiguration der Amazon FSx-Ereignisbenachrichtigung auf dem verknüpften S3-Bucket gelöscht oder geändert wurde.

Maßnahme

1. Entfernen Sie alle vorhandenen Ereignisbenachrichtigungen auf dem verknüpften S3-Bucket, die einen oder beide Ereignistypen verwenden, die die FSx-Ereigniskonfiguration verwendet, `s3:ObjectCreated:*` und `s3:ObjectRemoved:*`.
2. Bitte stellen Sie sicher, dass in Ihrem verknüpften S3-Bucket eine Konfiguration für S3-Ereignisbenachrichtigungen mit dem Namen `FSx`, den Ereignistypen `s3:ObjectCreated:*` und `s3:ObjectRemoved:*` dem Senden an das SNS-Thema mit vorhanden ist.
ARN: *topic_arn_returned_in_API_response*
3. Wenden Sie die Konfiguration der FSx-Ereignisbenachrichtigung erneut auf den S3-Bucket an, indem Sie die Amazon FSx-CLI oder -API verwenden, um die Dateisysteme zu

aktualisieren. AutoImportPolicy Tun Sie dies mit dem update-file-system CLI-Befehl ([UpdateFileSystem](#) entspricht der entsprechenden API-Aktion) wie folgt.

```
aws fsx update-file-system \  
--file-system-id fs-0123456789abcdef0 \  
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Fehlerbehebung bei Speicherproblemen

In einigen Fällen können Speicherprobleme mit Ihrem Dateisystem auftreten. Sie können diese Probleme mithilfe von lfs Befehlen wie dem lfs migrate Befehl beheben.

Schreibfehler, da auf dem Speicherziel kein Speicherplatz verfügbar ist

Sie können die Speichernutzung Ihres Dateisystems mithilfe des lfs df -h Befehls überprüfen, wie unter beschrieben [Speicherlayout des Dateisystems](#). Das filesystem_summary Feld gibt die gesamte Speichernutzung des Dateisystems an.

Wenn die Festplattenauslastung des Dateisystems bei 100% liegt, sollten Sie erwägen, die Speicherkapazität Ihres Dateisystems zu erhöhen. Weitere Informationen finden Sie unter [Verwaltung der Speicherkapazität](#).

Wenn die Speicherauslastung des Dateisystems nicht zu 100% beträgt und Sie immer noch Schreibfehler erhalten, kann es sein, dass die Datei, in die Sie schreiben, auf einem vollen OST gestreift wird.

Maßnahme

- Wenn viele Ihrer OSTs voll sind, erhöhen Sie die Speicherkapazität Ihres Dateisystems. Suchen Sie nach unsymmetrischem Speicher auf OSTs, indem Sie den Anweisungen im Abschnitt folgen. [Unausgeglichener Speicher auf OSTs](#)
- Wenn Ihre OSTs nicht voll sind, optimieren Sie die Puffergröße für Dirty Page auf dem Client, indem Sie die folgende Optimierung auf alle Ihre Client-Instances anwenden:

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

Unausgeglichener Speicher auf OSTs

Amazon FSx for Lustre verteilt neue Datei-Stripes gleichmäßig auf alle OSTs. Ihr Dateisystem kann jedoch aufgrund von I/O-Mustern oder dem Dateispeicherlayout immer noch aus dem Gleichgewicht geraten. Dies kann dazu führen, dass einige Speicherziele voll werden, während andere relativ leer bleiben.

Sie verwenden den `lfs migrate` Befehl, um Dateien oder Verzeichnisse von OSTs mit mehr Speicherplatz in weniger volle zu verschieben. Sie können den `lfs migrate` Befehl entweder im Blockmodus oder im Blockmodus verwenden.

- Der Blockmodus ist der Standardmodus für den `lfs migrate` Befehl. Bei der Ausführung im Blockmodus wird vor der Datenmigration `lfs migrate` zunächst eine Gruppensperre für die Dateien und Verzeichnisse eingerichtet, um Änderungen an den Dateien zu verhindern. Die Sperre wird dann aufgehoben, wenn die Migration abgeschlossen ist. Indem der Blockmodus verhindert, dass andere Prozesse die Dateien ändern, verhindert er, dass diese Prozesse die Migration unterbrechen. Der Nachteil ist, dass das Verhindern der Änderung einer Datei durch eine Anwendung zu Verzögerungen oder Fehlern bei der Anwendung führen kann.
- Der blockfreie Modus ist für den `lfs migrate` Befehl mit der `-n` Option aktiviert. Wenn sie `lfs migrate` im blockfreien Modus ausgeführt werden, können andere Prozesse die Dateien, die migriert werden, trotzdem ändern. Wenn ein Prozess eine Datei ändert, bevor die Migration `lfs migrate` abgeschlossen ist, schlägt die Migration dieser Datei `lfs migrate` fehl und die Datei behält ihr ursprüngliches Stripe-Layout.

Wir empfehlen Ihnen, den Modus ohne Blockierung zu verwenden, da es weniger wahrscheinlich ist, dass er Ihre Anwendung beeinträchtigt.

Maßnahme

1. Starten Sie eine relativ große Client-Instance (z. B. den Amazon EC2 `c5n.4xlarge` EC2-Instance-Typ), um sie im Dateisystem zu mounten.
2. Bevor Sie das Skript für den Nichtblockmodus oder das Blockmodus-Skript ausführen, führen Sie zunächst die folgenden Befehle auf jeder Client-Instance aus, um den Vorgang zu beschleunigen:

```
sudo lctl set_param 'mdc.*.max_rpcs_in_flight=60'  
sudo lctl set_param 'mdc.*.max_mod_rpcs_in_flight=59'
```

3. Starten Sie eine Bildschirmsitzung und führen Sie das Skript für den Nichtblockmodus oder das Blockmodus-Skript aus. Achten Sie darauf, die entsprechenden Variablen in den Skripten zu ändern:

- Skript im Nicht-Blockmodus:

```
#!/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

```

- Blockmodus-Skript:
 - Ersetzen Sie die Werte in OSTs durch die Werte Ihrer OSTs.
 - Geben Sie einen Integer-Wert für `annproc`, um die Anzahl der Max-Procs-Prozesse festzulegen, die parallel ausgeführt werden sollen. Der Amazon EC2 `c5n.4xlarge` EC2-Instance-Typ hat beispielsweise 16 vCPUs, sodass Sie 16 (oder einen Wert < 16) für verwenden können. `nproc`
 - Geben Sie Ihren Mount-Verzeichnispfad in ein. `mnt_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

```

Hinweise

- Wenn Sie feststellen, dass die Leistung der Lesevorgänge des Dateisystems beeinträchtigt wird, können Sie die Migrationen jederzeit mit `ctrl-c` oder `kill -9` beenden und die Anzahl der

Threads (`nproc`Wert) wieder auf einen niedrigeren Wert (z. B. 8) reduzieren und die Migration der Dateien fortsetzen.

- Der `lfs migrate` Befehl schlägt bei einer Datei fehl, die auch vom Client-Workload geöffnet wird. Es wird ein Fehler ausgegeben und zur nächsten Datei übergegangen. Daher ist es möglich, dass das Skript keine Dateien migrieren kann, wenn auf viele Dateien zugegriffen wird, und dies wird angezeigt, da die Migration sehr langsam voranschreitet.
- Sie können die OST-Nutzung mit einer der folgenden Methoden überwachen
 - Führen Sie bei der Client-Installation den folgenden Befehl aus, um die OST-Nutzung zu überwachen und die OST-Datei mit einer Auslastung von mehr als 85% zu finden:

```
lfs df -h |grep '( 8[5-9]| 9[1-9]|100)%'
```

- Überprüfen Sie die CloudWatch Amazon-Metrik `OST FreeDataStorageCapacity`, überprüfen Sie `Minimum`. Wenn Ihr Skript OSTs findet, die zu über 85% voll sind, verwenden Sie `ctrl-c` oder, um die Migration `kill -9` zu beenden, wenn die Metrik fast 15% beträgt.
- Sie können auch erwägen, die Stripe-Konfiguration Ihres Dateisystems oder eines Verzeichnisses zu ändern, sodass neue Dateien auf mehrere Speicherziele verteilt werden. Weitere Informationen finden Sie unter [Daten in Ihrem Dateisystem entfernen](#).

Behebung von FSx for Lustre CSI-Treiberproblemen

Wenn Sie Probleme mit dem FSx for Lustre CSI-Treiber für Container haben, die auf Amazon EKS ausgeführt werden, finden Sie weitere Informationen unter [Troubleshooting CSI Driver \(Common Issues\)](#), verfügbar unter: GitHub

Zusätzliche Informationen

Dieser Abschnitt enthält eine Referenz der unterstützten, aber veralteten Amazon-FSx-Funktionen.

Themen

- [Einrichten eines benutzerdefinierten Backup-Zeitplans](#)

Einrichten eines benutzerdefinierten Backup-Zeitplans

Wir empfehlen, zu verwenden AWS Backup, um einen benutzerdefinierten Backup-Zeitplan für Ihr Dateisystem einzurichten. Die hier bereitgestellten Informationen dienen Referenzzwecken, wenn Sie Backups häufiger planen müssen als bei Verwendung von AWS Backup.

Wenn diese Option aktiviert ist, erstellt Amazon FSx während eines täglichen Sicherungsfensters automatisch einmal täglich eine Sicherung Ihres Dateisystems. Amazon FSx erzwingt einen Aufbewahrungszeitraum, den Sie für diese automatischen Backups angeben. Es unterstützt auch vom Benutzer initiierte Backups, sodass Sie jederzeit Backups erstellen können.

Im Folgenden finden Sie die Ressourcen und die Konfiguration für die Bereitstellung der benutzerdefinierten Backup-Planung. Die benutzerdefinierte Backup-Planung führt vom Benutzer initiierte Backups auf einem Amazon FSx for Lustre-Dateisystem nach einem von Ihnen definierten benutzerdefinierten Zeitplan durch. Beispiele können einmal alle sechs Stunden, einmal pro Woche usw. sein. Dieses Skript konfiguriert auch das Löschen von Backups, die älter als der angegebene Aufbewahrungszeitraum sind.

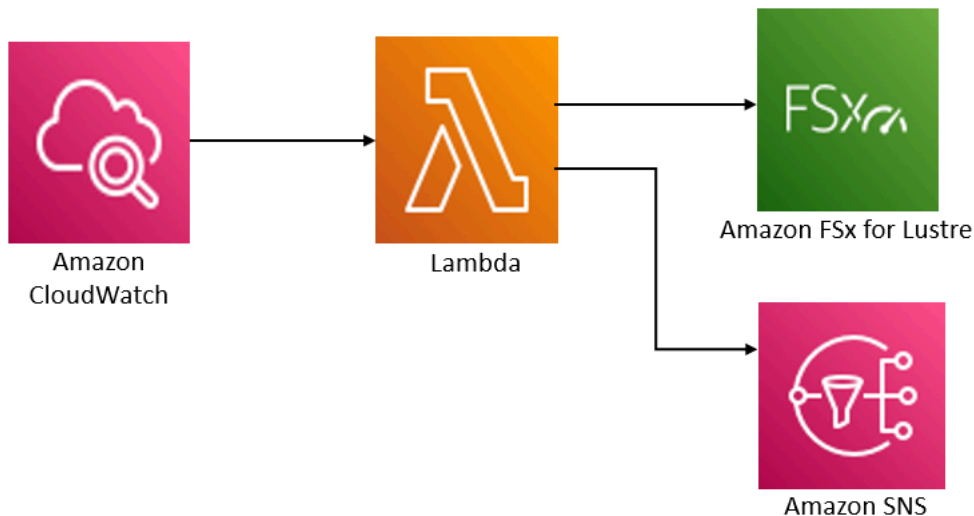
Die Lösung stellt automatisch alle erforderlichen Komponenten bereit und verwendet die folgenden Parameter:

- Das Dateisystem
- Ein CRON-Zeitplanmuster für die Durchführung von Backups
- Der Aufbewahrungszeitraum für Backups (in Tagen)
- Die Sicherungsnamen-Tags

Weitere Informationen zu CRON-Zeitplanmustern finden Sie unter [Zeitplanausdrücke für Regeln](#) im Amazon CloudWatch -Benutzerhandbuch.

Übersicht über die Architektur

Durch die Bereitstellung dieser Lösung werden die folgenden Ressourcen in der erstellten AWS Cloud.



Diese Lösung führt Folgendes aus:

1. Die AWS CloudFormation Vorlage stellt ein CloudWatch Ereignis, eine Lambda-Funktion, eine Amazon SNS-Warteschlange und eine IAM-Rolle bereit. Die IAM-Rolle erteilt der Lambda-Funktion die Berechtigung zum Aufrufen der API-Operationen von Amazon FSx für Lustre.
2. Das CloudWatch Ereignis wird während der ersten Bereitstellung nach einem Zeitplan ausgeführt, den Sie als CRON-Muster definieren. Dieses Ereignis ruft die Lambda-Funktion des Backup-Managers der Lösung auf, die den Amazon-FSx-for-LustreCreateBackup-API-Vorgang aufruft, um ein Backup zu initiieren.
3. Der Backup-Manager ruft eine Liste der vorhandenen vom Benutzer initiierten Backups für das angegebene Dateisystem mit `abDescribeBackups`. Anschließend werden Sicherungen gelöscht, die älter als der Aufbewahrungszeitraum sind, den Sie bei der ersten Bereitstellung angeben.
4. Der Backup-Manager sendet bei einem erfolgreichen Backup eine Benachrichtigung an die Amazon SNS-Warteschlange, wenn Sie die Option auswählen, während der ersten Bereitstellung benachrichtigt zu werden. Im Falle eines Fehlers wird immer eine Benachrichtigung gesendet.

AWS CloudFormation-Vorlage

Diese Lösung verwendet AWS CloudFormation, um die Bereitstellung der benutzerdefinierten Backup-Planungslösung von Amazon FSx für Lustre zu automatisieren. Um diese Lösung zu verwenden, laden Sie die [fsx-scheduled-backup.template](#)-AWS CloudFormationVorlage herunter.

Automatisierte Bereitstellung

Mit dem folgenden Verfahren wird diese benutzerdefinierte Backup-Planungslösung konfiguriert und bereitgestellt. Die Bereitstellung dauert etwa fünf Minuten. Bevor Sie beginnen, müssen Sie die ID eines Amazon FSx for Lustre-Dateisystems haben, das in einer Amazon Virtual Private Cloud (Amazon VPC) in Ihrem AWS Konto ausgeführt wird. Weitere Informationen zum Erstellen dieser Ressourcen finden Sie unter [Erste Schritte mit Amazon FSx for Lustre](#).

Note

Bei der Implementierung dieser Lösung wird die Abrechnung für die zugehörigen AWS Services berechnet. Weitere Informationen finden Sie auf den Seiten mit den Preisdetails für diese Services.

So starten Sie den benutzerdefinierten Sicherungslösungs-Stack

1. Laden Sie die [fsx-scheduled-backup.template](#)-AWS CloudFormationVorlage herunter. Weitere Informationen zum Erstellen eines -AWS CloudFormationStacks finden Sie unter [Erstellen eines Stacks auf der -AWS CloudFormationKonsole](#) im AWS CloudFormation -Benutzerhandbuch.

Note

Standardmäßig wird diese Vorlage in der AWS Region USA Ost (Nord-Virginia) gestartet. Amazon FSx for Lustre ist derzeit nur in bestimmten verfügbarAWS-Regionen. Sie müssen diese Lösung in einer -AWSRegion starten, in der Amazon FSx for Lustre verfügbar ist. Weitere Informationen finden Sie im Abschnitt Amazon FSx von [AWS-Regionen und Endpunkte](#) im Allgemeine AWS-Referenz.

2. Überprüfen Sie für Parameter die Parameter für die Vorlage und ändern Sie sie entsprechend den Anforderungen Ihres Dateisystems. Diese Lösung verwendet die folgenden Standardwerte.

Parameter	Standard	Beschreibung
Dateisystem-ID von Amazon FSx für Lustre	Kein Standardwert	Die Dateisystem-ID für das Dateisystem, das Sie sichern möchten.

Parameter	Standard	Beschreibung
CRON-Zeitplanmuster für Backups.	0 0/4 * * ? *	Der Zeitplan für die Ausführung des CloudWatch Ereignisses, der ein neues Backup auslöst und alte Backups außerhalb des Aufbewahrungszeitraums löscht.
Aufbewahrung von Backups (Tage)	7	Die Anzahl der Tage, für die vom Benutzer initiierte Backups aufbewahrt werden sollen. Die Lambda-Funktion löscht vom Benutzer initiierte Backups, die älter als diese Anzahl von Tagen sind.
Name für Backups	Vom Benutzer geplante Sicherung	Der Name für diese Backups, der in der Spalte Backup Name der Amazon FSx for Lustre Management Console angezeigt wird.
Backup-Benachrichtigungen	Ja	Wählen Sie aus, ob Sie benachrichtigt werden möchten, wenn Backups erfolgreich initiiert werden. Bei einem Fehler wird immer eine Benachrichtigung gesendet.
E-Mail-Adresse	Kein Standardwert	Die E-Mail-Adresse, an der die SNS-Benachrichtigungen abonniert werden sollen.

3. Wählen Sie Weiter aus.
4. Wählen Sie für Optionen die Option Weiter aus.

- Überprüfen und bestätigen Sie für Review die Einstellungen. Sie müssen das Kontrollkästchen aktivieren, um zu bestätigen, dass die Vorlage IAM-Ressourcen erstellt.
- Wählen Sie Create aus, um den Stack bereitzustellen.

Sie können den Status des Stacks in der AWS CloudFormation-Konsole in der Spalte Status anzeigen. Sie sollten in etwa fünf Minuten den Status CREATE_COMPLETE sehen.

Zusätzliche Optionen

Sie können die von dieser Lösung erstellte Lambda-Funktion verwenden, um benutzerdefinierte geplante Backups von mehr als einem Amazon FSx for Lustre-Dateisystem durchzuführen. Die Dateisystem-ID wird an die Funktion Amazon FSx for Lustre im Eingabe-JSON für das CloudWatch Ereignis übergeben. Der an die Lambda-Funktion übergebene Standard-JSON-Code lautet wie folgt, wobei die Werte für `FileSystemId` und von den Parametern übergeben `SuccessNotification` werden, die beim Starten des AWS CloudFormationStacks angegeben wurden.

```
{
  "start-backup": "true",
  "purge-backups": "true",
  "filesystem-id": "${FileSystemId}",
  "notify_on_success": "${SuccessNotification}"
}
```

Um Backups für ein zusätzliches Amazon FSx for Lustre-Dateisystem zu planen, erstellen Sie eine weitere CloudWatch Ereignisregel. Dazu verwenden Sie die Ereignisquelle planen, wobei die von dieser Lösung erstellte Lambda-Funktion das Ziel ist. Wählen Sie Konstant (JSON-Text) unter Eingabe konfigurieren aus. Ersetzen Sie für die JSON-Eingabe einfach die Dateisystem-ID des Amazon FSx for Lustre-Dateisystems, das gesichert werden soll, anstelle von `${FileSystemId}`. Ersetzen Sie außerdem entweder Yes oder No anstelle von `${SuccessNotification}` im obigen JSON.

Alle zusätzlichen CloudWatch Ereignisregeln, die Sie manuell erstellen, sind nicht Teil des benutzerdefinierten Lösungs-AWS CloudFormationStacks für geplante Backups von Amazon FSx for Lustre. Daher werden sie nicht entfernt, wenn Sie den Stack löschen.

Dokumentverlauf

- API-Version: 01.03.2018
- Letzte Aktualisierung der Dokumentation: 6. Juni 2024

In der folgenden Tabelle werden wichtige Änderungen am Amazon FSx for Lustre-Benutzerhandbuch beschrieben. Um Benachrichtigungen über Dokumentationsaktualisierungen zu erhalten, können Sie den RSS-Feed abonnieren.

Änderung	Beschreibung	Datum
Support zur Steigerung der Metadaten-Performance hinzugefügt	Sie können jetzt ein FSx for Lustre Persistent_2 Dateisystem mit einer Metadatenkonfiguration erstellen, die die Möglichkeit bietet, die Metadaten-Performance zu erhöhen. Weitere Informationen finden Sie unter Leistung von Dateisystem-Metadaten und Verwaltung der Leistung von Metadaten.	6. Juni 2024
Zusätzliche AWS-Regionen Unterstützung für den Bereitstellungstyp Persistent_2 hinzugefügt	Persistent_2 SSD FSx for Lustre Lustre-Dateisysteme sind jetzt in der lokalen Zone US East (Atlanta) verfügbar. Weitere Informationen finden Sie unter Verfügbare Regionen.	29. Mai 2024
Lustre-Client-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 9.4 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL)	16. Mai 2024

	<p>9.4 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Lustre-Clients.</p>	
<p>Zusätzliche AWS-Regionen Unterstützung für den Bereitstellungstyp Persistent_2 hinzugefügt</p>	<p>Persistent_2 SSD FSx for Lustre Lustre-Dateisysteme sind jetzt in Kanada West (Calgary) erhältlich. AWS-Region Weitere Informationen finden Sie unter Verfügbare Regionen.</p>	3. Mai 2024
<p>Lustre-Client-Unterstützung für Amazon Linux 2023 hinzugefügt</p>	<p>Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen Amazon Linux 2023 ausgeführt wird. Weitere Informationen finden Sie unter Installation des Lustre-Clients.</p>	25. März 2024
<p>Lustre-Client-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.9 hinzugefügt</p>	<p>Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.9 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Lustre-Clients.</p>	9. Januar 2024

- [Amazon FSx hat die verwalteten Richtlinien von AmazonFSxFull Access, AmazonFSxConsoleFullAccess, AmazonFSxConsoleReadOnly Access SxReadOnlyAccess und AmazonFSaktualisiert SxService RolePolicy AWS](#)
- Amazon FSx hat die Richtlinien von AmazonFSFull Access, AmazonF, AmazonFSxConsoleFullAccess, AmazonFSxRead OnlyAccess SxConsole ReadOnly Access und AmazonFSxService RolePolicy aktualisiert, um die Berechtigung hinzuzufügen. `ec2:GetSecurityGroupsForVpc` Weitere Informationen finden Sie unter [Amazon FSx-Updates für AWS verwaltete Richtlinien](#).
9. Januar 2024
- [Lustre-Client-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux \(RHEL\) 9.0 und 9.3 hinzugefügt](#)
- Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 9.0 und 9.3 ausgeführt werden. [Weitere Informationen finden Sie unter Installation des Lustre-Clients](#).
20. Dezember 2023
- [Amazon FSx for Lustre hat die verwalteten Richtlinien von AmazonFSxFullAccess und AmazonFSaktualisiert SxConsole FullAccess AWS](#)
- Amazon FSx hat die AmazonFSxFullAccess - und SxConsole FullAccess AmazonF-Richtlinien aktualisiert, um die Aktion hinzuzufügen. `ManageCrossAccountDataReplication` Weitere Informationen finden Sie unter [Amazon FSx-Updates für AWS verwaltete Richtlinien](#).
20. Dezember 2023

[Amazon FSx hat die von AmazonF SxFullAccess und von AmazonF verwalteten Richtlinien aktualisiert SxConsole FullAccess AWS](#)

Amazon FSx hat die SxConsoleFullAccess Richtlinien von AmazonF SxFullAccess und AmazonF aktualisiert, um die Genehmigung hinzuzufügen. `fsx:CopySnapshotAndUpdateVolume` Weitere Informationen finden Sie unter [Amazon FSx-Updates für AWS verwaltete Richtlinien](#).

26. November 2023

[Support für die Skalierung der Durchsatzkapazität hinzugefügt](#)

Sie können jetzt die Durchsatzkapazität für bestehende persistente SSD-basierte Dateisysteme von FSx for Lustre ändern, wenn sich Ihre Durchsatzanforderungen ändern. [Weitere Informationen finden Sie unter Verwaltung der Durchsatzkapazität](#).

16. November 2023

[Amazon FSx hat die von AmazonF SxFullAccess und von AmazonF verwalteten Richtlinien aktualisiert SxConsole FullAccess AWS](#)

Amazon FSx hat die AmazonF SxFullAccess - und SxConsole FullAccess AmazonF-Richtlinien aktualisiert, um die Berechtigungen und hinzuzufügen. `fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` Weitere Informationen finden Sie unter [Amazon FSx-Updates für AWS verwaltete Richtlinien](#).

14. November 2023

[Support für Projektkontingente hinzugefügt](#)

Sie können jetzt Speicherkontingente für Projekte erstellen. Ein Projektkontingent gilt für alle Dateien oder Verzeichnisse, die einem Projekt zugeordnet sind. Weitere Informationen finden Sie unter [Speicherkontingente](#).

29. August 2023

[Support für Lustre Version 2.15 hinzugefügt](#)

Alle FSx for Lustre-Datensysteme basieren jetzt auf Lustre-Version 2.15, wenn sie mit der Amazon FSx-Konsole erstellt wurden. Weitere Informationen finden Sie unter [Schritt 1: Erstellen Sie Ihr Amazon FSx for Lustre-Datensystem](#).

29. August 2023

[Zusätzliche AWS-Regionen Unterstützung für den Bereitstellungstyp Persistent_2 hinzugefügt](#)

Persistent_2 FSx for Lustre Lustre-Datensysteme sind jetzt in Israel (Tel Aviv) verfügbar. AWS-Region Weitere Informationen finden Sie unter [Bereitstellungsoptionen für FSx for Lustre-Datensysteme](#).

24. August 2023

[Support für Release-Daten-Repository-Aufgaben hinzugefügt](#)

FSx for Lustre bietet jetzt Release-Daten-Repository-Aufgaben, um archivierte Dateien aus einem Dateisystem freizugeben, das mit einem S3-Datenrepository verknüpft ist. Beim Freigeben einer Datei werden die Dateiliste und die Metadaten beibehalten, aber die lokale Kopie des Inhalts dieser Datei wird entfernt. Weitere Informationen finden Sie unter [Verwenden von Datenrepository-Aufgaben zur Freigabe von Dateien](#).

9. August 2023

[Amazon FSx hat die von AmazonFSxService RolePolicy AWS verwaltete Richtlinie aktualisiert](#)

Amazon FSx hat die `cloudwatch:PutMetricData` Erlaubnis im `SxService RolePolicy` AmazonFSx aktualisiert. Weitere Informationen finden Sie unter [Amazon FSx-Updates für AWS verwaltete Richtlinien](#).

24. Juli 2023

[Amazon FSx hat die verwaltete AmazonFSxFull AWS Access-Richtlinie aktualisiert](#)

Amazon FSx hat die `SxFullAccess` AmazonFSx-Richtlinie aktualisiert, um die `fsx:*` Genehmigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen. Weitere Informationen finden Sie in der [AmazonFSxFull Access-Richtlinie](#).

13. Juli 2023

[Amazon FSx hat die von AmazonF SxConsole FullAccess AWS verwaltete Richtlinie aktualisiert](#)

Amazon FSx hat die SxConsoleFullAccess AmazonF-Richtlinie aktualisiert, um die `fsx:*` Genehmigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen. Weitere Informationen finden Sie unter [SxConsoleFullAccessAmazonF-Richtlinie](#).

13. Juli 2023

[Lustre-Client-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux \(RHEL\) 8.8 hinzugefügt](#)

Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.8 ausgeführt werden. [Weitere Informationen finden Sie unter Installation des Lustre-Clients](#).

25. Mai 2023

[Support für AutoImport und AutoExport Metriken hinzugefügt](#)

FSx for Lustre bietet jetzt CloudWatch Amazon-Metriken, die automatische Import- und Exportaktualisierungen für Dateisysteme überwachen, die mit Datenrepositorys verknüpft sind. Weitere Informationen finden Sie unter [Überwachung mit Amazon CloudWatch](#).

31. März 2023

[DRA-Unterstützung für die Bereitstellungstypen Persistent_1 und Scratch_2 hinzugefügt](#)

Sie können jetzt Datenrepository-Verknüpfungen erstellen, um Datenrepositories mit Lustre 2.12-Dateisystemen mit den Bereitstellungstypen Persistent_1 oder Scratch_2 zu verknüpfen. Weitere Informationen finden Sie unter [Verwenden von Datenrepositories mit Amazon FSx for Lustre](#).

29. März 2023

[Lustre-Client-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux \(RHEL\) 8.7 hinzugefügt](#)

Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.7 ausgeführt werden. [Weitere Informationen finden Sie unter Installation des Lustre-Clients](#).

5. Dezember 2022

[Zusätzliche AWS-Regionen Unterstützung für den Bereitstellungstyp Persistent_2 hinzugefügt](#)

Persistent_2 SSD FSx der nächsten Generation für Lustre-Dateisysteme sind jetzt in Europa (Stockholm), Asien-Pazifik (Hongkong), Asien-Pazifik (Mumbai) und Asien-Pazifik (Seoul) erhältlich. AWS-Regionen Weitere Informationen finden Sie unter [Bereitstellungsoptionen für FSx for Lustre-Dateisysteme](#).

10. November 2022

Lustre-Client-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.6 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.6 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Lustre-Clients.	8. September 2022
Lustre-Client-Unterstützung für Ubuntu 22 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen Ubuntu 22.04 ausgeführt wird. Weitere Informationen finden Sie unter Installation des Lustre-Clients.	28. Juli 2022
Lustre-Client-Unterstützung für Rocky Linux hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen Rocky Linux ausgeführt wird. Weitere Informationen finden Sie unter Installation des Lustre-Clients.	8. Juli 2022
Support für Lustre Root Squash hinzugefügt	Sie können jetzt die Lustre-Root-Squash-Funktion verwenden, um den Zugriff auf Root-Ebene von Clients einzuschränken, die versuchen, als Root auf Ihr FSx for Lustre-Dateisystem zuzugreifen. Weitere Informationen finden Sie unter Lustre Root Squash.	25. Mai 2022

[Zusätzliche AWS-Regionen Unterstützung für den Bereitstellungstyp Persistent_2 hinzugefügt](#)

Persistent_2 SSD FSx der nächsten Generation für Lustre-Dateisysteme sind jetzt in Europa (London), im asiatisch-pazifischen Raum (Singapur) und im asiatisch-pazifischen Raum (Sydney) erhältlich. AWS-Regionen Weitere Informationen finden Sie unter [Bereitstellungsoptionen für FSx for Lustre-Dateisysteme](#).

19. April 2022

[Support für die Migration von Dateien AWS DataSync zu Ihren Amazon FSx for Lustre-Dateisystemen hinzugefügt.](#)

Sie können es jetzt verwenden AWS DataSync , um Dateien von vorhandenen Dateisystemen auf FSx for Lustre-Dateisysteme zu migrieren. Weitere Informationen finden Sie unter [So migrieren Sie bestehende Dateien mithilfe von FSx for Lustre](#). AWS DataSync

5. April 2022

[Support für AWS PrivateLink Schnittstellen-VPC-Endpunkte hinzugefügt](#)

Sie können jetzt Schnittstellen-VPC-Endpunkte verwenden, um von Ihrer VPC aus auf die Amazon FSx-API zuzugreifen, ohne Datenverkehr über das Internet zu senden. Weitere Informationen finden Sie unter [Amazon FSx und Interface VPC-Endpoints](#).

5. April 2022

[Support für Lustre DRA Queuing hinzugefügt](#)

Sie können jetzt eine DRA (Data Repository Association) erstellen, wenn Sie ein FSx for Lustre-Dateisystem erstellen. Die Anfrage wird in die Warteschlange gestellt und der DRA wird erstellt, sobald das Dateisystem verfügbar ist. Weitere Informationen finden Sie unter [Ihr Dateisystem mit einem S3-Bucket verknüpfen](#).

28. Februar 2022

[Lustre-Client-Unterstützung für CentOS und Red Hat Enterprise Linux \(RHEL\) 8.5 hinzugefügt](#)

Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS und Red Hat Enterprise Linux (RHEL) 8.5 ausgeführt werden. [Weitere Informationen finden Sie unter Installation des Lustre-Clients](#).

20. Dezember 2021

[Support für den Export von Änderungen aus FSx for Lustre in ein Linked Data Repository](#)

Sie können FSx for Lustre jetzt so konfigurieren, dass neue, geänderte und gelöschte Dateien automatisch aus Ihrem Dateisystem in ein verknüpftes Amazon S3 S3-Daten-Repository exportiert werden. Sie können Datenrepository-Aufgaben verwenden, um Daten und Metadatenänderungen in das Daten-Repository zu exportieren. Sie können auch Links zu mehreren Datenrepositories konfigurieren. Weitere Informationen finden Sie unter [Exportieren von Änderungen in das Datenrepository](#).

30. November 2021

[Support für Lustre-Logging hinzugefügt](#)

Sie können FSx for Lustre jetzt so konfigurieren, dass Fehler- und Warnereignisse für Datenrepositories, die mit Ihrem Dateisystem verknüpft sind, in Amazon Logs protokolliert werden. CloudWatch
Weitere Informationen finden Sie unter [Protokollierung mit Amazon CloudWatch Logs](#).

30. November 2021

[Persistente SSD-Dateisysteme unterstützen einen höheren Durchsatz und eine geringere Speicherkapazität](#)

Persistent SSD FSx for Lustre Lustre-Dateisysteme der nächsten Generation bieten höhere Durchsatzoptionen und eine geringere Mindestspeicherkapazität. Weitere Informationen finden Sie unter [Bereitstellungsoptionen für FSx for Lustre-Dateisysteme](#).

30. November 2021

[Support für Lustre Version 2.12 hinzugefügt](#)

Sie können jetzt Lustre Version 2.12 wählen, wenn Sie ein FSx for Lustre-Dateisystem erstellen. Weitere Informationen finden Sie unter [Schritt 1: Erstellen Sie Ihr Amazon FSx for Lustre-Dateisystem](#).

5. Oktober 2021

[Lustre-Client-Unterstützung für CentOS und Red Hat Enterprise Linux \(RHEL\) 8.4 hinzugefügt](#)

Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS und Red Hat Enterprise Linux (RHEL) 8.4 ausgeführt werden. [Weitere Informationen finden Sie unter Installation des Lustre-Clients](#).

9. Juni 2021

[Support für Datenkomprimierung hinzugefügt](#)

Sie können jetzt die Datenkomprimierung aktivieren, wenn Sie ein FSx for Lustre-Dateisystem erstellen. Sie können die Datenkomprimierung auch auf einem vorhandenen FSx for Lustre-Dateisystem aktivieren oder deaktivieren. Weitere Informationen finden Sie unter [Lustre-Datenkomprimierung](#).

27. Mai 2021

[Support für das Kopieren von Backups hinzugefügt](#)

Sie können jetzt Amazon FSx verwenden, um Backups innerhalb derselben AWS-Konto zu einer anderen AWS-Region (regionsübergreifende Kopien) oder innerhalb derselben AWS-Region (regionsinterne Kopien) zu kopieren. [Weitere Informationen finden Sie unter Backups kopieren](#).

12. April 2021

[Lustre-Client-Unterstützung für Lustre-Dateisätze](#)

Der FSx for Lustre-Client unterstützt jetzt die Verwendung von Dateisätzen, um nur eine Teilmenge des Dateisystem-Namespaces einzuhängen. [Weitere Informationen finden Sie unter Mounten bestimmter Dateisätze](#).

18. März 2021

Support für den Zugriff von Clients über nicht private IP-Adressen hinzugefügt	Sie können von einem lokalen Client aus auf FSx for Lustre-Dateisysteme zugreifen, indem Sie nicht private IP-Adressen verwenden. Weitere Informationen finden Sie unter Mounten von Amazon FSx-Dateisystemen vor Ort oder über eine Peering-Amazon VPC.	17. Dezember 2020
Lustre-Client-Unterstützung für ARM-basiertes CentOS 7.9 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS 7.9 auf ARM-Basis ausgeführt wird. Weitere Informationen finden Sie unter Installation des Lustre-Clients.	17. Dezember 2020
Lustre-Client-Unterstützung für CentOS und Red Hat Enterprise Linux (RHEL) 8.3 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS und Red Hat Enterprise Linux (RHEL) 8.3 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Lustre-Clients.	16. Dezember 2020
Support für die Skalierung von Speicher- und Durchsatzkapazität hinzugefügt	Sie können jetzt die Speicher- und Durchsatzkapazität für bestehende FSx for Lustre-Dateisysteme erhöhen, wenn sich Ihre Speicher- und Durchsatzanforderungen ändern. Weitere Informationen finden Sie unter Speicher- und Durchsatzkapazität verwalten.	24. November 2020

[Support für Speicherkontingente hinzugefügt](#)

Sie können jetzt Speicherkontingente für Benutzer und Gruppen erstellen. Speicherkontingente begrenzen den Speicherplatz und die Anzahl der Dateien, die ein Benutzer oder eine Gruppe auf Ihrem FSx for Lustre-Dateisystem verbrauchen kann. Weitere Informationen finden Sie unter [Speicherkontingente](#).

9. November 2020

[Amazon FSx ist jetzt integriert mit AWS Backup](#)

Sie können jetzt zusätzlich AWS Backup zur Verwendung der nativen Amazon FSx-Backups Ihre FSx-Dateisysteme sichern und wiederherstellen. Weitere Informationen finden Sie unter [Verwenden AWS Backup mit Amazon FSx](#).

9. November 2020

[Support für die HDD-Speicheroptionen \(Festplattenlaufwerk\) hinzugefügt](#)

Zusätzlich zur SSD-Speicheroption (Solid State Drive) unterstützt FSx for Lustre jetzt die Speicheroption HDD (Hard Disk Drive). Sie können Ihr Dateisystem so konfigurieren, dass HDD für durchsatzintensive Workloads verwendet wird, die typischerweise große, sequentielle Dateioperationen beinhalten. [Weitere Informationen finden Sie unter Mehrere Speicheroptionen](#).

12. August 2020

[Support für den Import von Änderungen am Linked Data Repository in FSx for Lustre](#)

Sie können Ihr FSx for Lustre-Dateisystem jetzt so konfigurieren, dass neue Dateien, die nach der Erstellung des Dateisystems zu einem verknüpften Datenrepository hinzugefügt wurden, und Dateien, die sich dort geändert haben, automatisch importiert werden. Weitere Informationen finden Sie unter [Automatisches Importieren von Updates aus dem Daten-Repository](#).

23. Juli 2020

[Lustre-Client-Unterstützung für SUSE Linux SP4 und SP5 hinzugefügt](#)

Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen SUSE Linux SP4 und SP5 ausgeführt werden. [Weitere Informationen finden Sie unter Installation des Lustre-Clients](#).

20. Juli 2020

[Lustre-Client-Unterstützung für CentOS und Red Hat Enterprise Linux \(RHEL\) 8.2 hinzugefügt](#)

Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen CentOS und Red Hat Enterprise Linux (RHEL) 8.2 ausgeführt werden. [Weitere Informationen finden Sie unter Installation des Lustre-Clients](#).

20. Juli 2020

[Support für automatische und manuelle Dateisystem-Backups hinzugefügt](#)

Sie können jetzt automatische tägliche Backups und manuelle Backups von Dateisystemen erstellen, die nicht mit einem dauerhaften Amazon S3 S3-Daten-Repository verknüpft sind. Weitere Informationen finden Sie unter [Arbeiten mit Sicherungen](#).

23. Juni 2020

[Zwei neue Bereitstellungstypen für Dateisysteme wurden veröffentlicht](#)

Scratch-Dateisysteme sind für die temporäre Speicherung und kurzfristige Verarbeitung von Daten konzipiert. Persistente Dateisysteme sind für die längerfristige Speicherung und für Workloads konzipiert. Weitere Informationen finden Sie unter [FSx for Lustre Deployment Options](#).

12. Februar 2020

[Support für POSIX-Metadaten hinzugefügt](#)

FSx for Lustre behält die zugehörigen POSIX-Metadaten beim Import und Export von Dateien in ein verknüpftes dauerhaftes Daten-Repository auf Amazon S3 bei. Weitere Informationen finden Sie unter [Unterstützung von POSIX-Metadaten](#) für Daten-Repositorys.

23. Dezember 2019

<u>Neue Funktion für Datenrepository-Aufgaben veröffentlicht</u>	Sie können jetzt mithilfe von Datenrepository-Aufgaben geänderte Daten und zugehörige POSIX-Metadaten in ein verknüpftes dauerhaftes Daten-Repository auf Amazon S3 exportieren. Weitere Informationen finden Sie unter <u>Übertragung von Daten und Metadaten mithilfe von Datenrepository-Aufgaben.</u>	23. Dezember 2019
<u>Zusätzliche AWS-Region Unterstützung hinzugefügt</u>	FSx for Lustre ist jetzt in der Region Europa (London) verfügbar. AWS-Region <u>Informationen zu den regionsspezifischen Grenzwerten von FSx for Lustre finden Sie unter Grenzwerte.</u>	9. Juli 2019
<u>Zusätzliche Unterstützung hinzugefügt AWS-Region</u>	FSx for Lustre ist jetzt im asiatisch-pazifischen Raum (Singapur) erhältlich. AWS-Region <u>Informationen zu den regionsspezifischen Grenzwerten von FSx for Lustre finden Sie unter Grenzwerte.</u>	26. Juni 2019
<u>Lustre-Client-Unterstützung für Amazon Linux und Amazon Linux 2 hinzugefügt</u>	Der FSx for Lustre-Client unterstützt jetzt Amazon EC2 EC2-Instances, auf denen Amazon Linux und Amazon Linux 2 ausgeführt werden. Weitere Informationen finden Sie unter <u>Installation des Lustre-Clients.</u>	11. März 2019

[Unterstützung für benutzerdefinierte Datenexportpfade hinzugefügt](#)

Benutzer haben jetzt die Möglichkeit, die ursprünglichen Objekte in Ihrem Amazon S3 S3-Bucket zu überschreiben oder die neuen oder geänderten Dateien in ein von Ihnen festgelegtes Präfix zu schreiben. Mit dieser Option haben Sie zusätzliche Flexibilität, FSx for Lustre in Ihre Datenverarbeitungs-Workflows zu integrieren. Weitere Informationen finden Sie unter [Daten in Ihren Amazon S3 S3-Bucket exportieren](#).

6. Februar 2019

[Das Standardlimit für den gesamten Speicherplatz wurde erhöht](#)

Der standardmäßige Gesamtspeicher für alle FSx for Lustre-Dateisysteme wurde auf 100.800 GiB erhöht. Weitere Informationen finden Sie unter [Limits](#).

11. Januar 2019

[Amazon FSx for Lustre ist jetzt allgemein verfügbar](#)

Amazon FSx for Lustre ist ein vollständig verwaltetes Dateisystem, das für rechenintensive Workloads wie Hochleistungsdatenverarbeitung, maschinelles Lernen und Medienverarbeitungsworkflows optimiert ist.

28. November 2018

Die vorliegende Übersetzung wurde maschinell erstellt. Im Falle eines Konflikts oder eines Widerspruchs zwischen dieser übersetzten Fassung und der englischen Fassung (einschließlich infolge von Verzögerungen bei der Übersetzung) ist die englische Fassung maßgeblich.