aws

Lustre-Benutzerhandbuch

FSx für Lustre

FSx für Lustre: Lustre-Benutzerhandbuch

Table of Contents

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 Geschwindigkeit wichtig ist, wie Machine Learning, High Performance Computing (HPC), Videoverarbeitung und Finanzmodellierung.

Das Open-Source-Lustre-Dateisystem ist für Anwendungen konzipiert, die schnellen Speicher benötigen – wo Ihr Speicher mit Ihrer Datenverarbeitung Schritt halten soll. 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 unter einer Millisekunde, bis zu Hunderten von GBpss Durchsatz 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 die Speichergeschwindigkeit wichtig ist. FSx for Lustre eliminiert die traditionelle Komplexität bei der Einrichtung und Verwaltung von Lustre-Dateisystemen, sodass Sie in wenigen Minuten ein belastbares Hochleistungsdateisystem einrichten und ausführen können. Es bietet auch mehrere Bereitstellungsoptionen, sodass Sie die Kosten für Ihre Anforderungen optimieren 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. Sie bietet read-after-write auch Konsistenz und unterstützt das Sperren von Dateien.

Themen

- Preise für Amazon FSx for Lustre
- Amazon-FSx-for-Lustre-Foren
- Verwenden Sie Amazon FSx for Lustre zum ersten Mal?

Mehrere Bereitstellungsoptionen

Amazon FSx for Lustre bietet eine Auswahl an Scratch- und persistent enDateisystemen, um unterschiedliche Datenverarbeitungsanforderungen zu erfüllen. Scratch-Dateisysteme eignen sich ideal für die temporäre Speicherung und die kurzfristige Verarbeitung von Daten. Daten werden nicht repliziert und bleiben nicht bestehen, wenn ein Dateiserver ausfällt. Persistente Dateisysteme eignen sich ideal für längerfristige Speicherung und durchsatzorientierte Workloads. In persistenten Dateisystemen werden Daten repliziert und Dateiserver 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 SSD-Speichertypen (Solid State Drive) und HDD-Speichertypen (Festplattenlaufwerk), die für unterschiedliche Datenverarbeitungsanforderungen optimiert sind:

- SSD-Speicheroptionen – Wählen Sie für IOPS-intensive Workloads mit niedriger Latenz, die normalerweise kleine, zufällige Dateioperationen haben, eine der SSD-Speicheroptionen aus.
- HDD-Speicheroptionen – Wählen Sie für durchsatzintensive Workloads, die in der Regel große, sequenzielle Dateioperationen haben, eine der HDD-Speicheroptionen aus.

Wenn Sie ein Dateisystem mit der HDD-Speicheroption bereitstellen, können Sie optional einen schreibgeschützten SSD-Cache bereitstellen, der auf 20 Prozent Ihrer HDD-Speicherkapazität dimensioniert ist. Dies bietet Latenzen unter einer Millisekunde und höhere IOPS für häufig aufgerufene Dateien. Sowohl SSD-basierte als auch HDD-basierte Dateisysteme werden mit SSD-basierten Metadatenservern bereitgestellt. Daher werden alle Metadatenoperationen, die die meisten Dateisystemoperationen darstellen, mit Latenzen unter einer Millisekunde bereitgestellt.

Weitere Informationen zur Leistung dieser Speicheroptionen finden Sie unter Leistung von Amazon FSx für Lustre.

FSx für Lustre und Datenrepositories

Sie können FSx-für-Lustre-Dateisysteme mit Daten-Repositorys auf Amazon S3 oder mit On-Premises-Datenspeichern verknüpfen.

FSx-für-Lustre-S3-Daten-Repository-Integration

FSx for Lustre lässt sich in Amazon S3 integrieren, sodass Sie Cloud-Datensätze mit dem Lustre-Hochleistungsdateisystem einfacher verarbeiten können. Wenn ein FSx for Lustre-Dateisystem mit einem Amazon S3-Bucket verknüpft ist, zeigt es S3-Objekte transparent als Dateien an. Amazon FSx importiert Listen aller vorhandenen Dateien in Ihrem S3-Bucket bei der Erstellung des Dateisystems. Amazon FSx kann auch Auflistungen 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 in S3 zu schreiben. Daten-Repository-Aufgaben vereinfachen die Übertragung von Daten und Metadaten zwischen Ihrem Dateisystem von FSx für Lustre und seinem dauerhaften Daten-Repository auf Amazon S3. Weitere Informationen finden Sie unter Verwenden von Datenrepositorys mit Amazon FSx for Lustre und Daten-Repository-Aufgaben.

FSx für Lustre und On-Premises-Datenrepositories

Mit Amazon FSx for Lustre können Sie Ihre Datenverarbeitungs-Workloads von On-Premises in die übertragen, AWS Cloud indem Sie Daten mit AWS Direct Connect oder importierenAWS VPN. Weitere Informationen finden Sie unter Amazon FSx mit Ihren lokalen Daten verwenden.

Zugreifen auf FSx-for-Lustre-Dateisysteme

Sie können die Datenverarbeitungs-Instance-Typen und Linux Amazon Machine Images (AMIs) mischen und abgleichen, die mit einem einzigen FSx-für-Lustre-Dateisystem verbunden sind.

Dateisysteme von Amazon FSx für Lustre sind von Datenverarbeitungs-Workloads aus zugänglich, die auf Amazon Elastic Compute Cloud (Amazon EC2)-Instances, auf Amazon Elastic Container Service (Amazon ECS)-Docker-Containern und Containern ausgeführt werden, die auf Amazon Elastic Kubernetes Service (Amazon EKS) ausgeführt werden.

- Amazon EC2 – Sie greifen über den Open-Source-Lustre-Client von Ihren Amazon EC2-Compute-Instances aus auf Ihr Dateisystem zu. Amazon 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 gemountet wurde, können Sie mit seinen Dateien und Verzeichnissen genauso arbeiten wie mit einem lokalen Dateisystem.

- Amazon EKS – Sie greifen von Containern, die auf Amazon EKS ausgeführt FSx werden, mit dem CSI-Treiber von Open-Source-FSx für Lustre auf Amazon FSx für Lustre zu, wie im Amazon-EKS-Benutzerhandbuch beschrieben. Ihre Container, die auf Amazon EKS ausgeführt werden, können leistungsstarke persistente Volumes (PVs) verwenden, die von Amazon FSx for Lustre unterstützt werden.
- Amazon ECS – Sie greifen von Amazon-ECS-Docker-Containern auf Amazon-ECAmazon EC2FSx 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, einschließlich 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 On-Premises in die übertragen, AWS Cloud indem Sie Daten über AWS Direct Connect oder importierenAWS Virtual Private Network. Sie können von On-Premises 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, Datenverarbeitungs-Instances und Umgebungen, von denen aus Sie auf FSx-for-Lustre-Dateisysteme zugreifen können, finden Sie unter Zugreifen auf Dateisysteme.

Integrationen mit -AWSServices

Amazon FSx for Lustre lässt sich SageMaker als Eingabedatenquelle in Amazon integrieren. Bei Verwendung von SageMaker mit FSx für Lustre werden Ihre Machine-Learning-Trainingsaufträge beschleunigt, indem der erste Download-Schritt von Amazon S3 entfällt. Darüber hinaus werden Ihre Gesamtbetriebskosten (TCO) reduziert, indem das wiederholte Herunterladen häufiger Objekte für iterative Aufträge auf demselben Datensatz vermieden wird, während Sie bei S3-Anforderungskosten sparen. Weitere Informationen finden Sie unter Was ist SageMaker? im Amazon- SageMaker Entwicklerhandbuch. Eine exemplarische Vorgehensweise zur Verwendung von Amazon FSx for Lustre als Datenquelle für SageMakerfinden Sie unter Beschleunigen des Trainings auf Amazon

SageMaker mit Amazon FSx for Lustre und Amazon EFS Dateisystemen im AWS Machine Learning Blog .

FSx for Lustre lässt sich AWS Batch mithilfe von EC2-Startvorlagen in integrieren. AWS Batch ermöglicht es Ihnen, Batch-Computing-Workloads auf der auszuführenAWS Cloud, einschließlich High Performance Computing (HPC), Machine Learning (ML) und anderer asynchroner Workloads. skaliert Instances AWS Batch automatisch und dynamisch basierend auf den Anforderungen an Auftragsressourcen. Weitere Informationen finden Sie unter Was ist AWS Batch? im AWS Batch-Benutzerhandbuch.

FSx for Lustre lässt sich in integrierenAWS ParallelCluster. AWS ParallelCluster ist ein von unterstütztes Open-SourceAWS-Cluster-Verwaltungstool, das zur Bereitstellung und Verwaltung von HPC-Clustern verwendet wird. Es kann während der Clustererstellung automatisch FSx-für-Lustre-Dateisysteme erstellen oder vorhandene Dateisysteme verwenden.

Sicherheits und Compliance

Dateisysteme von FSx für Lustre unterstützen die Verschlüsselung im Ruhezustand und während der Übertragung. Amazon FSx verschlüsselt Dateisystemdaten im Ruhezustand automatisch mit Schlüsseln, die in AWS Key Management Service () verwaltet werdenAWS KMS. Daten während der Übertragung werden in bestimmten auch automatisch auf Dateisystemen verschlüsseltAWS-Regionen, wenn von unterstützten Amazon EC2 aus auf sie zugegriffen wird. Weitere Informationen zur Datenverschlüsselung in FSx for Lustre, einschließlich der AWS-Regionen unterstützten Verschlüsselung von Daten während der Übertragung, finden Sie unter Datenverschlüsselung in Amazon FSx for Lustre. Amazon FSx wurde bewertet, um die ISO-, PCI-DSS- und SOC-Zertifizierungen zu erfüllen, und ist HIPAA-fähig. Weitere Informationen finden Sie unter Sicherheit in FSx for Lustre.

Annahmen

In diesem Leitfaden gehen wir von 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 EC2Dokumentation.
- 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 basierend auf dem Amazon-VPC-Service nicht geändert haben. Wenn Sie dies tun, stellen Sie sicher, dass Sie die erforderlichen Regeln hinzufügen, um Netzwerkdatenverkehr von Ihrer Amazon 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

Bei Amazon FSx for Lustre fallen keine Vorab-Hardware- oder Softwarekosten an. Sie zahlen nur für die verwendeten Ressourcen, ohne Mindestverpflichtungen, Einrichtungskosten oder zusätzliche Gebühren. Informationen zu den Preisen und Gebühren für den Service finden Sie unter Amazon FSx for Lustre – Preise.

Amazon-FSx-for-Lustre-Foren

Wenn bei der Verwendung von Amazon FSx for Lustre Probleme auftreten, überprüfen Sie die Foren .

Verwenden Sie Amazon FSx for Lustre zum ersten Mal?

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

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

Einrichten von Amazon FSx für Lustre

Bevor Sie Amazon FSx for Lustre zum ersten Mal verwenden, führen Sie die Aufgaben im Bei Amazon Web Services registrieren Abschnitt aus. Um das Tutorial „Erste Schritte“ abzuschließen, stellen Sie sicher, dass der Amazon S3-Bucket, den Sie mit Ihrem Dateisystem verknüpfen, über die unter aufgeführten Berechtigungen verfügtHinzufügen von Berechtigungen zur Verwendung von Daten-Repositorys in Amazon S3.

Themen

Bei Amazon Web Services registrieren

Führen Sie die folgenden Schritte ausAWS, um für einzurichten:

1. So melden Sie sich für ein AWS-Konto an
2. Erstellen eines Administratorbenutzers

So melden Sie sich für ein AWS-Konto an

Wenn Sie kein AWS-Konto haben, führen Sie die folgenden Schritte zum Erstellen durch.

Anmeldung für ein 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 ein AWS-Konto anmelden, wird ein Root-Benutzer des AWS-Kontos erstellt. Der Root-Benutzer hat Zugriff auf alle AWS-Services und Ressourcen des Kontos. Als bewährte Sicherheitsmethode weisen Sie einem Administratorbenutzer Administratorzugriff zu und

verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen eine Bestätigungs-E-Mail, sobald die Anmeldung abgeschlossen ist. 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 eines Administratorbenutzers

Nachdem Sie sich für ein AWS-Kontoangemeldet haben, sichern Sie Ihr Root-Benutzer des AWS-Kontos, aktivieren Sie AWS IAM Identity Centerund erstellen Sie einen administrativen Benutzer, damit Sie nicht den Root-Benutzer für alltägliche Aufgaben verwenden.

Schützen Ihres Root-Benutzer des AWS-Kontos

1. Melden Sie sich bei der AWS Management Console als Kontobesitzer 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-AnmeldungBenutzerhandbuch zu .
2. Aktivieren Sie die Multi-Faktor-Authentifizierung (MFA) für den Root-Benutzer.

   Anweisungen dazu finden Sie unter Aktivieren eines virtuellen MFA-Geräts für den Root-Benutzer Ihres AWS-Konto (Konsole) im IAM-Benutzerhandbuch.

Erstellen eines Administratorbenutzers

1. Aktivieren von IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.
2. Im IAM Identity Center gewähren Sie einem administrativen Benutzer administrativen Zugriff.

   Ein Tutorial zur Verwendung von IAM-Identity-Center-Verzeichnis als Identitätsquelle finden Sie unter Benutzerzugriff mit dem standardmäßigen IAM-Identity-Center-Verzeichnis konfigurieren im AWS IAM Identity Center-Benutzerhandbuch.

Anmelden als Administratorbenutzer

- 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 unter Anmelden beim AWS-Zugangsportal im AWS-Anmeldung Benutzerhandbuch zu.

Hinzufügen von Berechtigungen zur Verwendung von Daten-Repositorys 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-Bucket gespeichert sind. Weitere Informationen finden Sie unter Verwenden von Datenrepositorys mit Amazon FSx for Lustre.

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

So betten Sie eine Inline-Richtlinie für eine Rolle mithilfe der Konsole ein

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. Die Dokumentation zur serviceverknüpften Rolle für einen Service finden Sie unter -AWSServices, die mit IAM

funktionieren, und wählen Sie Ja in der Spalte Serviceverknüpfte Rolle für Ihren Service aus.

6. Wählen Sie Erstellen von Richtlinien mit dem visuellen Editor
7. Fügen Sie die folgende Berechtigungsrichtlinienanweisung 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.

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

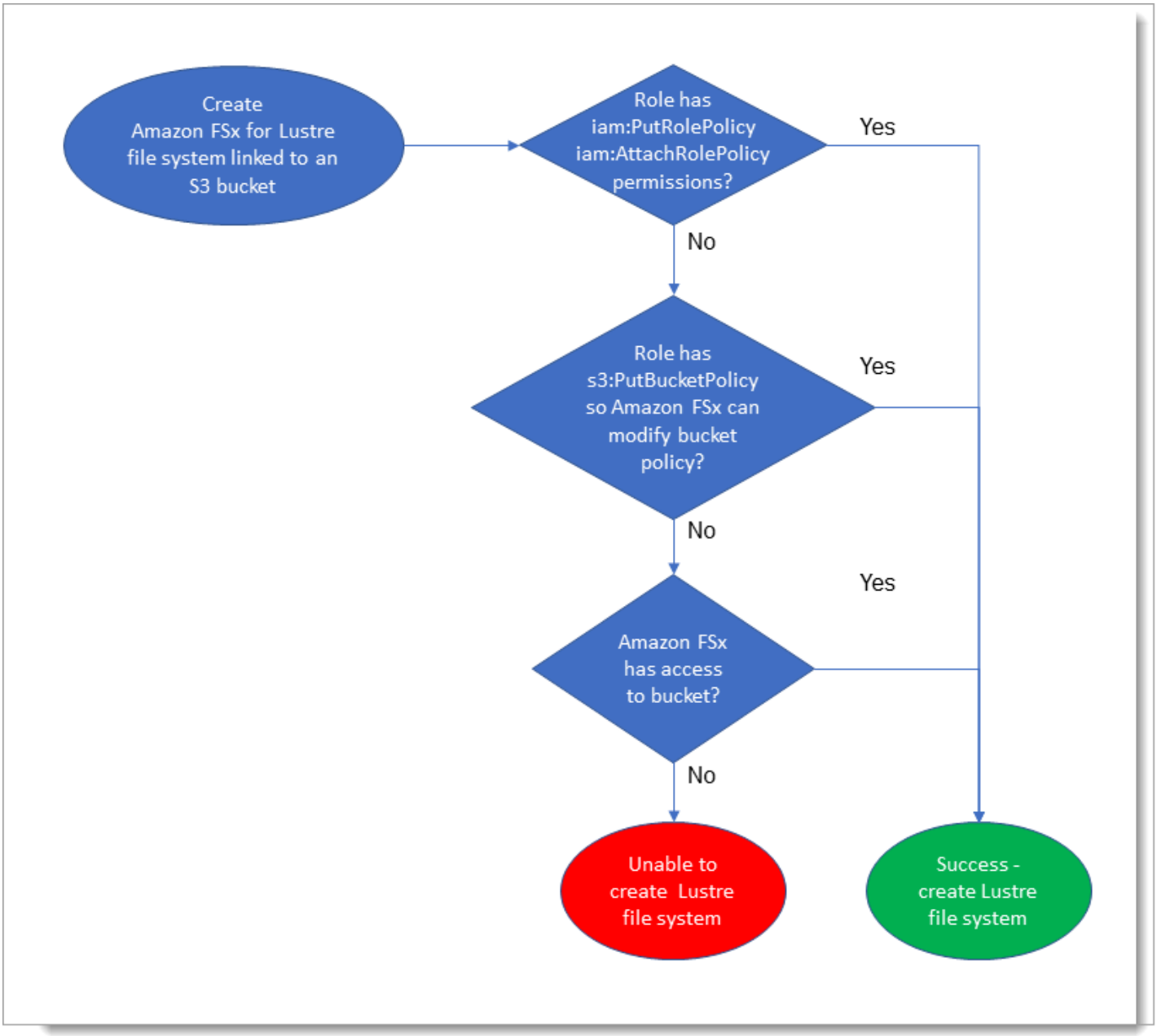
Wenn die IAM-Rolle, die Sie zum Erstellen des FSx for Lustre-Dateisystems verwenden, nicht über die `iam:PutRolePolicy` Berechtigungen `iam:AttachRolePolicy` und verfügt, prüft Amazon FSx, ob es Ihre S3-Bucket-Richtlinie aktualisieren kann. Amazon FSx kann Ihre Bucket-Richtlinie aktualisieren, wenn die -`s3:PutBucketPolicy`Berechtigung in Ihrer IAM-Rolle enthalten ist, damit das Amazon FSx-Dateisystem Daten in Ihren S3-Bucket importieren oder exportieren kann. Wenn die Bucket-Richtlinie geändert werden 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, prüft es, ob die vorhandene Bucket-Richtlinie Amazon FSx Zugriff auf den Bucket gewährt.

Wenn all diese Optionen fehlschlagen, schlägt die Anforderung zum Erstellen des Dateisystems fehl. Das folgende Diagramm veranschaulicht die Prüfungen, die Amazon FSx befolgt, um festzustellen, ob ein Dateisystem auf den S3-Bucket zugreifen kann, mit dem es verknüpft werden soll.



Nächster Schritt

Anweisungen zum Erstellen Ihrer Amazon-FSx-for-Lustre-FSx Ressourcen Erste Schritte mit Amazon FSx for Lustre finden Sie unter .

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 „Erste Schritte“ umfasst die folgenden Schritte.

Themen

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 Einrichten von Amazon FSx für Lustre.
- 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

einer Instance oder Starten Sie Ihre Instance im Amazon EC2 EC2-Benutzerhandbuch für Linux-Instances.

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 und 9.3, Rocky Linux 8.4 bis 8.9, 9.0 und 9.3, 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 den Metadatenserver (MDS) und eine IP-Adresse für jeden Speicherserver (OSS).
  - 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 Bereitstellungsoptionen für das Dateisystem 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 unterBereitstellungsoptionen für FSx-for-Lustre-Dateisysteme.

     Weitere Informationen darüber, AWS-Regionen wo die Verschlüsselung von Daten bei der Übertragung verfügbar ist, finden Sie unterVerschlüsseln 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 kurzfristigere 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 Verwalten der Durchsatzkapazität.

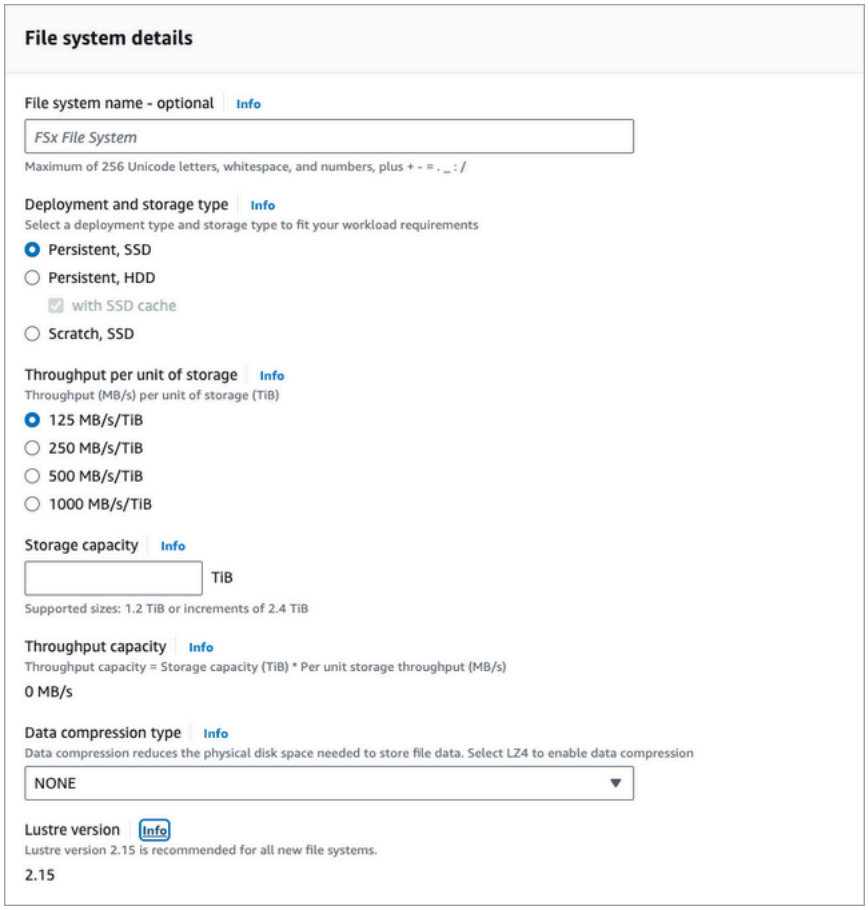
- Stellen Sie unter Speicherkapazität die Speicherkapazität für Ihr Dateisystem in TiB ein:

  - 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 Verwalten der Speicherkapazität.

- Wählen Sie als Datenkomprimierungstyp NONE aus, um die Datenkomprimierung auszuschalten, 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 Abschnitt Netzwerk und Sicherheit die folgenden Netzwerk- und Sicherheitsgruppeninformationen ein:

   - 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 *the_ID_of*	Regel für eingehenden Lustre-Verkehr

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
			_this_security_group	

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

> **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 unterVerwalten 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 Datenrepository-Import/Export 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 Create file system.

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 Einhängepunkt, 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 DescribeFileSystemsAPI-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` 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`.

3. Stellen Sie sicher, dass der Befehl mount erfolgreich war, indem Sie den Inhalt des Verzeichnisses auflisten, in das Sie das Dateisystem `/mnt/fsx` gemountet 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
devtmpf                           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 unterVerknüpfen Sie Ihr Dateisystem mit einem S3-Bucket.

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 unterExportieren 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 Beenden Ihrer Instance im Amazon EC2-Benutzerhandbuch für Linux-Instances.
3. Löschen Sie auf der Amazon FSx for Lustre-Konsole Ihr Dateisystem mit dem folgenden Verfahren:

   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 über mehrere Netzwerkdateiserver hinweg speichert, um die Leistung zu maximieren und Engpässe zu reduzieren. Diese Server haben mehrere Festplatten. Um die Last zu verteilen, fragmentiert Amazon FSx Dateisystemdaten in kleinere Blöcke und verteilt sie mithilfe eines Prozesses, der als Entfernen bezeichnet wird, auf Festplatten und Server. Weitere Informationen zum Daten-Striping von FSx für Lustre finden Sie unter Entfernen von Daten in Ihrem Dateisystem.

Es ist eine bewährte Methode, ein äußerst dauerhaftes langfristiges Daten-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-Daten-Repository. Wenn Sie Ihr FSx-for-Lustre-Dateisystem erstellen, verknüpfen Sie es mit Ihrem S3-Daten-Repository. An diesem Punkt werden die Objekte in Ihrem S3-Bucket als Dateien und Verzeichnisse auf Ihrem FSx-Dateisystem aufgeführt. Amazon FSx kopiert dann automatisch den Dateiinhalt von S3 in Ihr Lustre-Dateisystem, wenn auf dem Amazon-FSx-Dateisystem zum ersten Mal auf eine Datei zugegriffen wird. Nachdem Ihr Datenverarbeitungs-Workload ausgeführt wurde oder jederzeit, können Sie eine Daten-Repository-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.

Bereitstellungsoptionen für das Dateisystem für FSx for Lustre

Amazon FSx for Lustre bietet zwei Optionen für die Bereitstellung des Dateisystems: Scratch und persistent.

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

Sie wählen den Bereitstellungstyp des Dateisystems aus, wenn Sie ein neues Dateisystem mithilfe der AWS Management Console, der 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 .

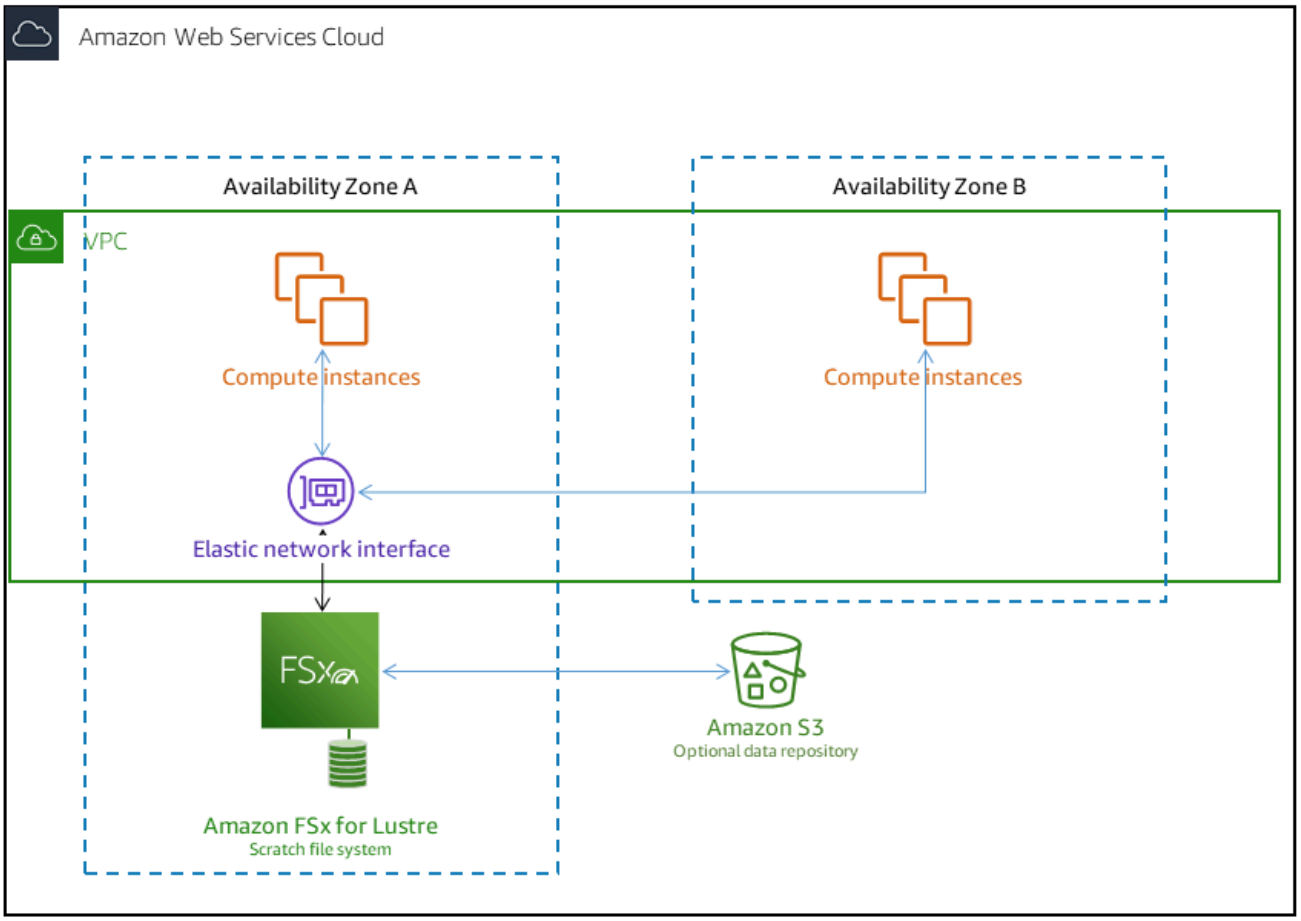
Die Verschlüsselung von Daten im Ruhezustand wird automatisch aktiviert, wenn Sie ein Amazon FSx for Lustre-Dateisystem erstellen, unabhängig vom verwendeten Bereitstellungstyp. Scratch 2 und persistente Dateisysteme verschlüsseln Daten während der Übertragung automatisch, wenn auf sie von Amazon EC2-Instances zugegriffen wird, die die Verschlüsselung während 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 nicht bestehen, wenn ein Dateiserver ausfällt. Scratch-Dateisysteme bieten einen hohen Burst-Durchsatz von bis zu sechsmal dem Basisdurchsatz von 200 MBpss pro TiB Speicherkapazität. Weitere Informationen finden Sie unter Aggregierte Dateisystemleistung.

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

Das folgende Diagramm zeigt die Architektur für ein Amazon FSx for Lustre Scratch-Dateisystem.



Auf einem Scratch-Dateisystem werden Dateiserver nicht ersetzt, wenn sie ausfallen und Daten nicht repliziert werden. Wenn ein Dateiserver oder ein Speicherdatenträger auf einem Scratch-Dateisystem nicht verfügbar ist, ist auf Dateien, die auf anderen Servern gespeichert sind, weiterhin zugegriffen werden kann. Wenn Clients versuchen, auf Daten zuzugreifen, die sich auf dem nicht verfügbaren Server oder der nicht verfügbaren Festplatte befinden, tritt bei Clients ein sofortiger E/A-Fehler auf.

Die folgende Tabelle zeigt die Verfügbarkeit oder Haltbarkeit, für die Scratch-Dateisysteme mit Beispielgrößen im Laufe eines Tages und einer Woche entwickelt wurden. Da größere Dateisysteme mehr Dateiserver und mehr Festplatten haben, erhöhen sich die Wahrscheinlichkeiten von Ausfällen.

Dateigröße (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 %
50,4	22	99,1 %	93,9 %

Persistente Dateisysteme

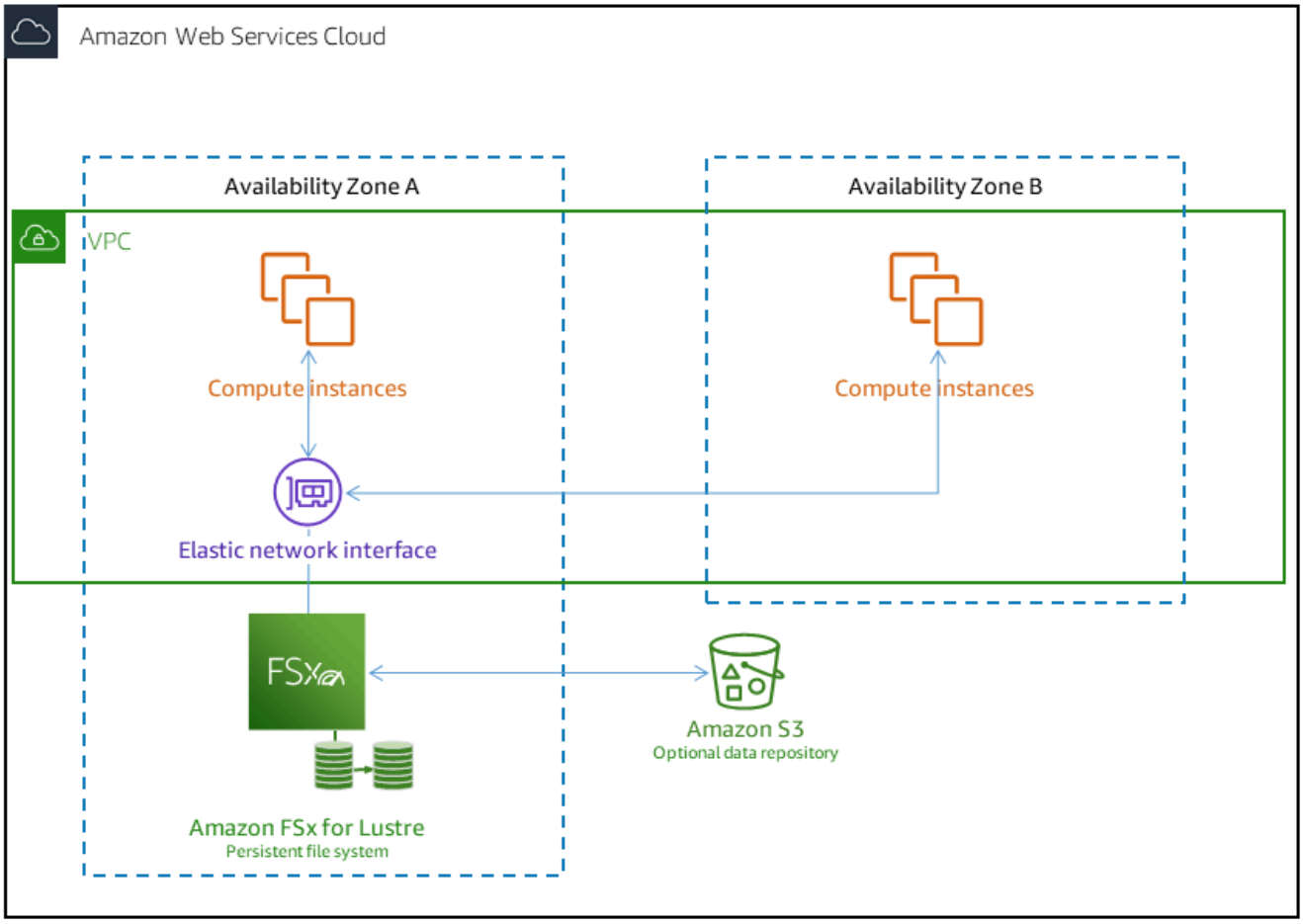
Persistente Dateisysteme sind für längerfristige Speicherung und Workloads konzipiert. Die Dateiserver sind hochverfügbar und Daten werden automatisch innerhalb derselben Availability Zone repliziert, in der sich das Dateisystem befindet. Die an die Dateiserver angefügten Daten-Volumes werden unabhängig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

Amazon FSx überwacht kontinuierlich persistente Dateisysteme auf Hardwareausfälle und ersetzt automatisch Infrastrukturkomponenten im Falle eines Ausfalls. Wenn ein Dateiserver auf einem persistenten Dateisystem nicht verfügbar ist, wird er automatisch innerhalb weniger Minuten nach dem Ausfall ersetzt. Während dieser Zeit versuchen Client-Anfragen für Daten auf diesem Server transparent erneut und sind schließlich erfolgreich, nachdem der Dateiserver ersetzt wurde. Daten auf persistenten Dateisystemen werden auf Datenträgern repliziert, und alle ausgefallenen Datenträger werden automatisch transparent ersetzt.

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

Das folgende Diagramm zeigt die Architektur für ein persistentes Dateisystem von Amazon FSx für Lustre mit replizierten, hochverfügbaren Dateiservern und Daten-Volumes innerhalb einer einzigen Availability Zone.

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



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

Persistenter 1-Bereitstellungstyp

Die Bereitstellungstypen Persistent_1 können auf Lustre 2.10 oder 2.12 basieren und SSD-Speichertypen (Solid State Drive) und HDD-Speichertypen (Festplattenlaufwerk) unterstützen. Der Bereitstellungstyp Persistent_1 eignet sich gut für Anwendungsfälle, die eine längerfristige Speicherung erfordern und durchsatzorientierte Workloads haben, die nicht latenzempfindlich sind.

Bei einem Persistent_1-Dateisystem mit SSD-Speicher beträgt der Durchsatz pro Speichereinheit entweder 50, 100 oder 200 MB/s pro Tebibyte (TiB). Für HDD-Speicher beträgt der Durchsatz von Persistent_1 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.

Persistenter 2-Bereitstellungstyp

Persistent_2 ist die neueste Generation des Typs Persistente Bereitstellung und eignet sich am besten für Anwendungsfälle, die längerfristigen Speicher erfordern und latenzempfindliche Workloads haben, die die höchsten IOPS- und Durchsatzwerte erfordern. Die Bereitstellungstypen Persistent_2 basieren auf Lustre v2.12 und unterstützen SSD-Speicher. Sie unterstützen einen höheren Durchsatz pro Einheitenspeicher als Persistent_1-Dateisysteme mit Optionen von 125, 250, 500 und 1000 MB/s/TiB .

Sie können Persistent_2-Bereitstellungstypen mithilfe der Amazon-FSx-KonsoleAWS Command Line Interface, und API erstellen.

Verfügbare Regionen

Die Bereitstellungstypen Persistent_1 und Persistent_2 sind in den folgenden verfügbarAWS-Regionen:

AWS-Region	Persistent_1	Persistent_2
US East (Ohio)	✓	✓
USA Ost (Nord-Virginia)	✓	✓
USA West (Nordkalifornien)	✓	
USA West (Los Angeles)	✓	
USA West (Oregon)	✓	✓
Africa (Cape Town)	✓	
Asien-Pazifik (Hongkong)	✓	✓
Asien-Pazifik (Hyderabad)	✓	

AWS-Region	Persistent_1	Persistent_2
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)	✓	✓
Europe (Frankfurt)	✓	✓
Europa (Irland)	✓	✓
Europa (London)	✓	✓
Europa (Milan)	✓	
Europa (Paris)	✓	
Europa (Spain)	✓	
Europa (Stockholm)	✓	✓
Europa (Zürich)	✓	
Israel (Tel Aviv)	✓	
Naher Osten (Bahrain)	✓	
Naher Osten (VAE)	✓	

AWS-Region	Persistent_1	Persistent_2
Südamerika (São Paulo)	✓	
AWS GovCloud (USA-Ost)	✓	
AWS GovCloud (USA-West)	✓	

Weitere Informationen zur Leistung von FSx für Lustre finden Sie unter Aggregierte Dateisystemleistung.

Verwenden von Datenrepositorys 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 Datenrepositorys 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 Datenrepositorien

Wenn Sie Amazon FSx for Lustre mit Datenrepositorys verwenden, können Sie große Mengen an Dateidaten in einem Hochleistungsdateisystem aufnehmen und verarbeiten, indem Sie automatische Import- und Import-Datenrepository-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-Objektdaten — 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. `755` 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 unterDateien 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":"1595002920000000000ns" , "file-owner":"500" , "file-
   permissions":"0100664","file-group":"500" , \
         "file-mtime":"1595002920000000000ns"}'
   ```

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": "bAlhCoWq7aIEjc3R6Myc6UOb8sHHtJkR",
       "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
3rnxfbmv-MDT0000_UUID       34.4G        6.1M       34.4G   0% /fsx[MDT:0]
3rnxfbmv-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.

Verknüpfen Sie Ihr Dateisystem mit einem S3-Bucket

Sie können Ihr Amazon FSx for Lustre-Dateisystem mit Datenrepositorys in Amazon S3 verknüpfen. Sie können den Link bei der Erstellung des Dateisystems oder jederzeit 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 angeben`s3://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 eines 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 Daten-Repositorys in Amazon S3

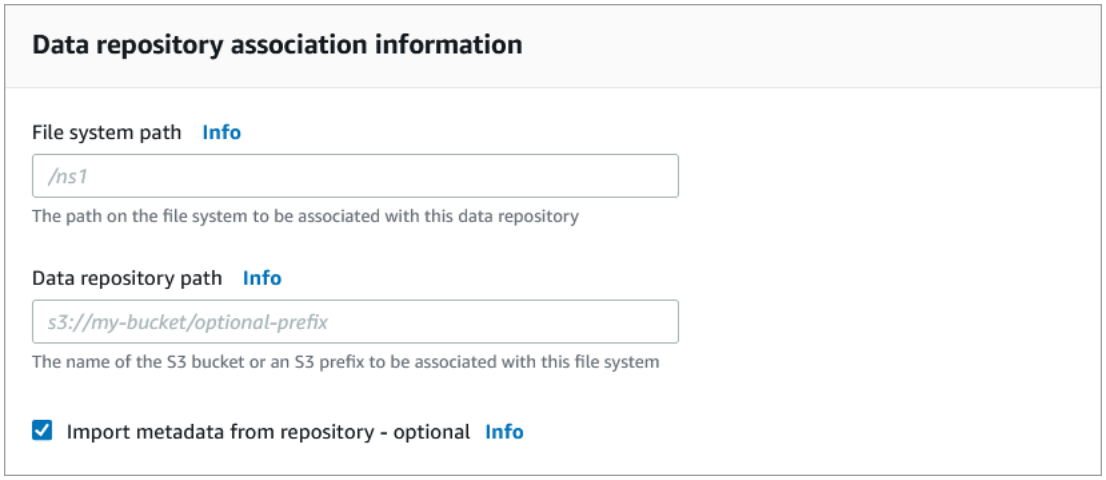
> **Note**
>
> Datenrepositorys können nicht mit Dateisystemen verknüpft werden, für die Dateisystem-Backups aktiviert sind. Deaktivieren Sie Backups, bevor Sie eine Verbindung zu einem Daten-Repository herstellen.

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

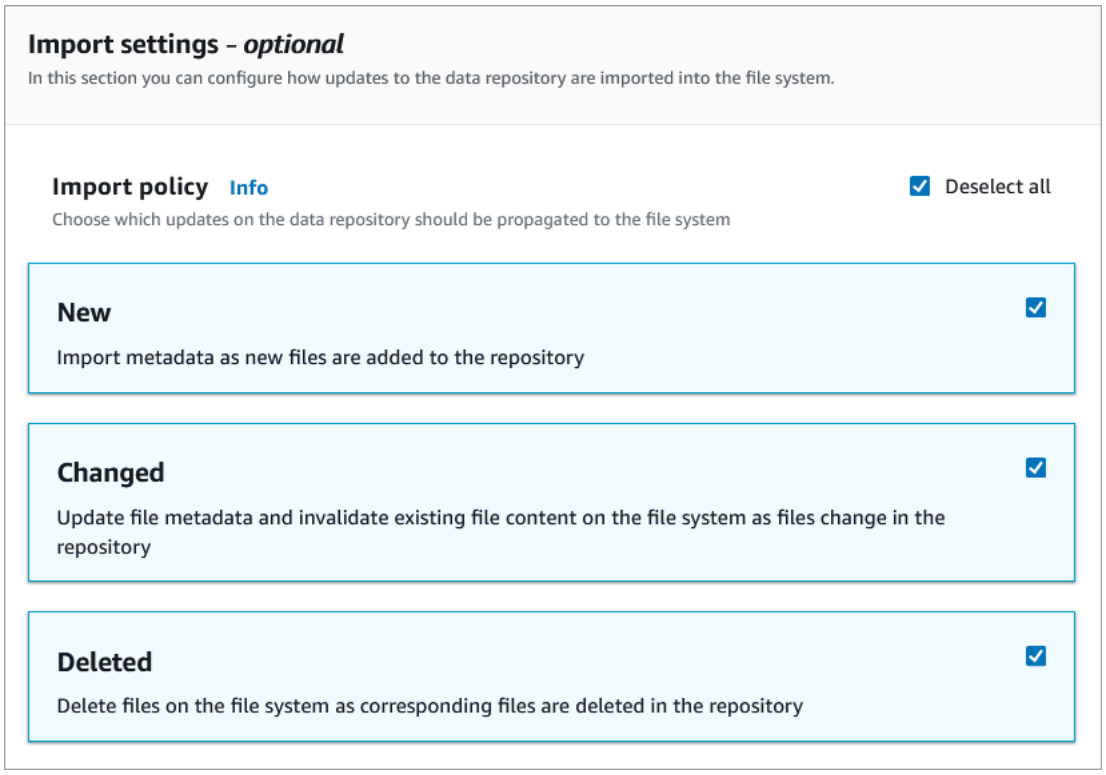
1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, das Erstellen Sie Ihr FSx for Lustre-Dateisystem im Abschnitt Erste Schritte beschrieben ist.

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.

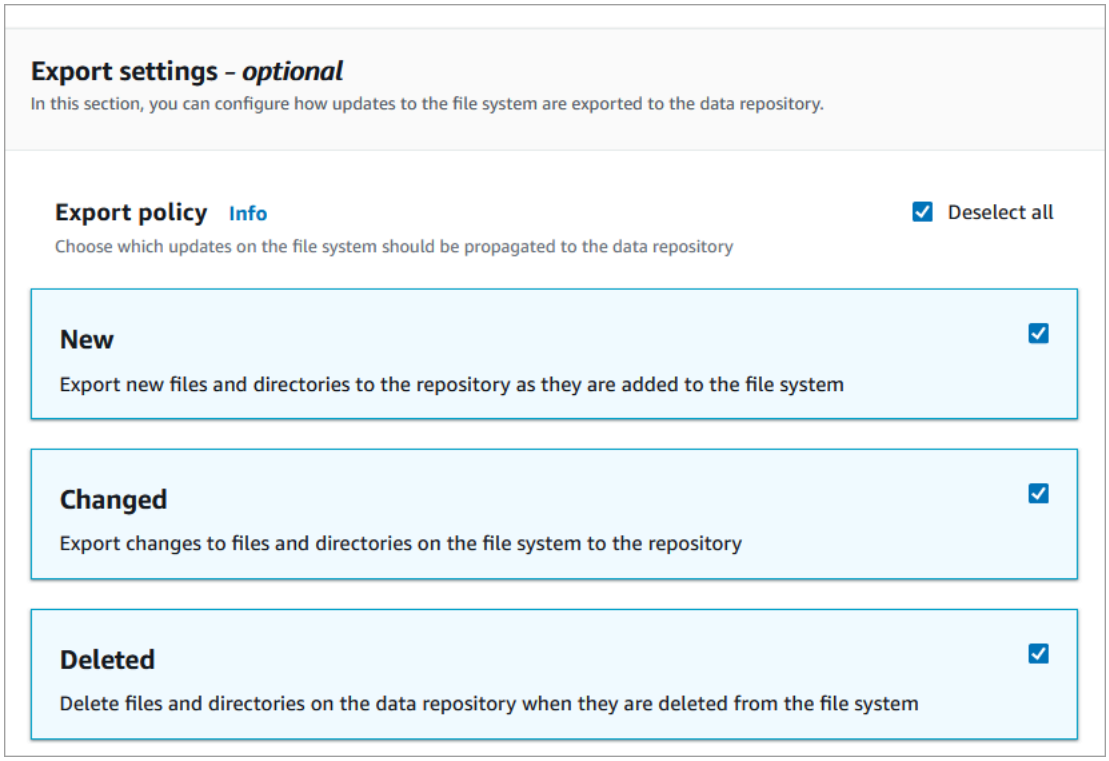


6. Legen Sie für Importeinstellungen — optional — eine Importrichtlinie fest, die festlegt, wie Ihre Datei- und Verzeichnislisten auf dem neuesten Stand gehalten werden, wenn Sie Objekte in Ihrem S3-Bucket hinzufügen, ändern oder löschen. Wählen Sie beispielsweise Neu aus, um Metadaten für neue Objekte,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



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 unterExportieren Sie Updates automatisch in Ihren S3-Bucket.



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

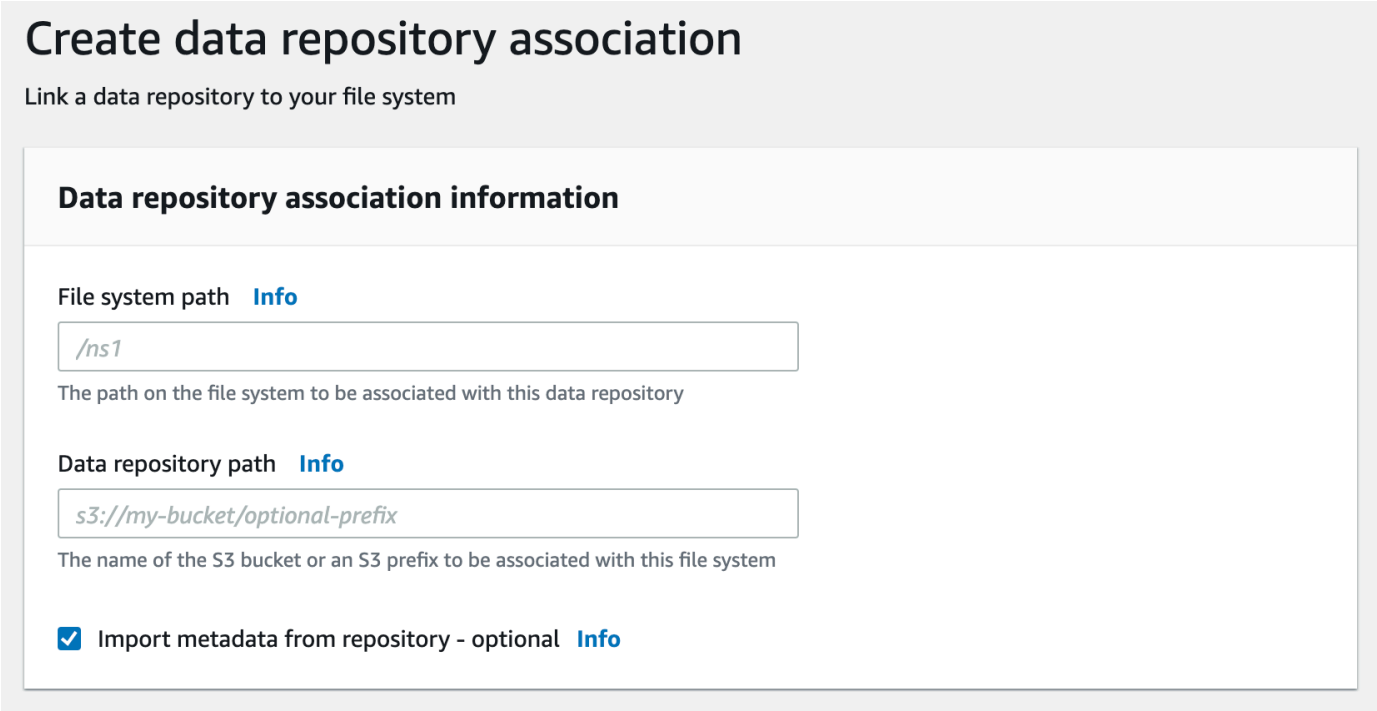
Um einen S3-Bucket mit einem vorhandenen Dateisystem (Konsole) zu verknüpfen

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

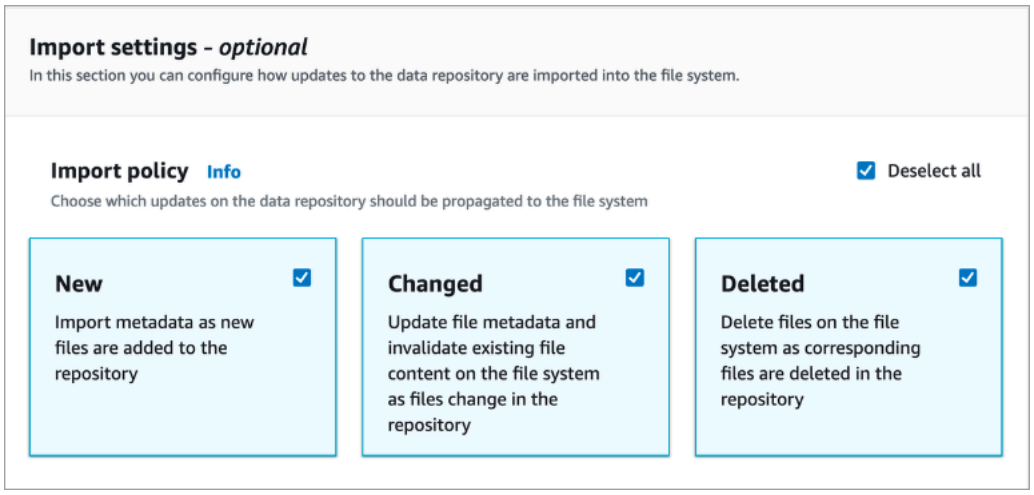
Dateisystempfade haben. Wenn beispielsweise ein Daten-Repository dem Dateisystempfad `/ns1` zugeordnet ist, können Sie kein anderes Daten-Repository mit dem Dateisystempfad `/ns1/ns2` verknüpfen. Die Einstellung für den Dateisystempfad muss für alle Datenrepository-Verknüpfungen für das Dateisystem eindeutig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

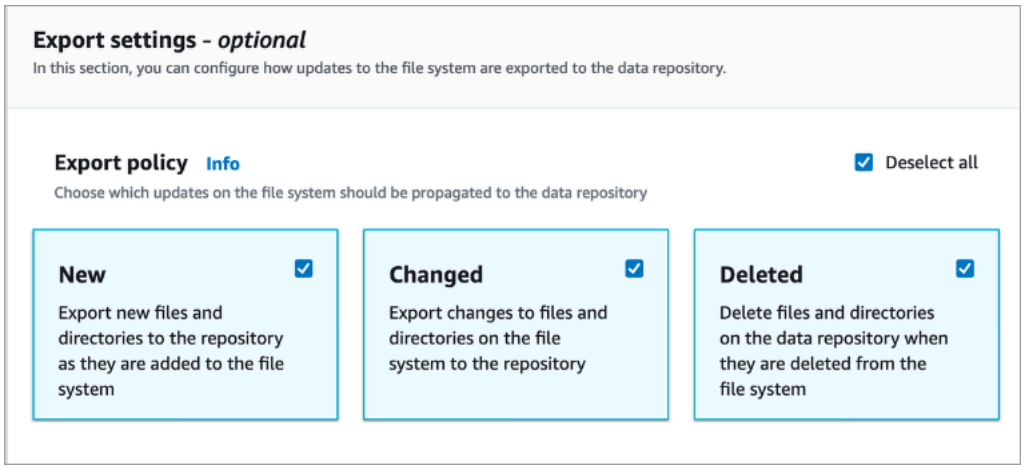


6. Legen Sie für Importeinstellungen — optional — eine Importrichtlinie fest, die festlegt, wie Ihre Datei- und Verzeichnislisten auf dem neuesten Stand gehalten werden, wenn Sie Objekte in Ihrem S3-Bucket hinzufügen, ändern oder löschen. Wählen Sie beispielsweise Neu aus, um Metadaten für neue Objekte,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

Weitere Informationen zu Importrichtlinien finden Sie unterAutomatisches Importieren von Updates aus Ihrem S3-Bucket.



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 unterExportieren Sie Updates automatisch in Ihren S3-Bucket.



8. Wählen Sie Create (Erstellen) aus.

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-Zuordnung 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 ConsoleAWS 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 aus. Für die Datenrepository-Zuordnung wird ein Bearbeitungsdialogfeld angezeigt.
6. Unter Importeinstellungen — optional können Sie Ihre Importrichtlinie aktualisieren. Weitere Informationen zu Importrichtlinien finden Sie unterAutomatisches Importieren von Updates aus Ihrem S3-Bucket.
7. Unter Exporteinstellungen — optional können Sie Ihre Exportrichtlinie aktualisieren. Weitere Informationen zu Exportrichtlinien finden Sie unterExportieren Sie Updates automatisch in Ihren S3-Bucket.
8. Wählen Sie Aktualisieren aus.

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.

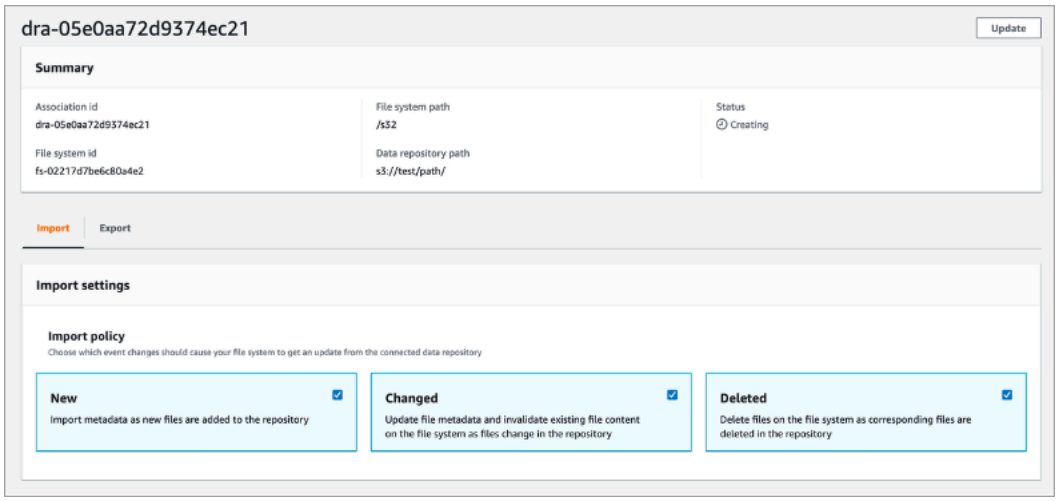
Details zur Datenrepository-Zuordnung anzeigen

Sie können die Details einer Datenrepository-Zuordnung mithilfe der FSx for Lustre-KonsoleAWS CLI, der und 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 Datenrepository.

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



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-Verknüpfung wird gerade 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-KonsoleAWS 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 Spiegelreflexkamera verknüpften ARN zu finden, suchen 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 importieren AWS-Region zu können.

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-ManagementkonsoleAWS 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 Datenrepositorys verwenden, wie unter beschriebenVerwenden von Datenrepository-Aufgaben zum Importieren von Änderungen.

> **Important**
>
> 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 davon 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 im selben. 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 die Importeinstellungen auch jederzeit aktualisieren, einschließlich der Importrichtlinie. 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 unterAutoImport und AutoExport 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 zurückzuversetzen, müssen Sie Ihre Datenrepository-Zuordnung aktualisieren. Sie können Ihre Datenrepository-Zuordnung mit dem update-data-repository-associationCLI-Befehl (oder der entsprechenden UpdateDataRepositoryAssociationAPI-Operation) aktualisieren. Der einzige Anforderungsparameter, den Sie benötigen, ist `AssociationID` der der 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 Synchronisation 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-Bucket`GetRequests`, `PutRequestsPostRequests`, 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

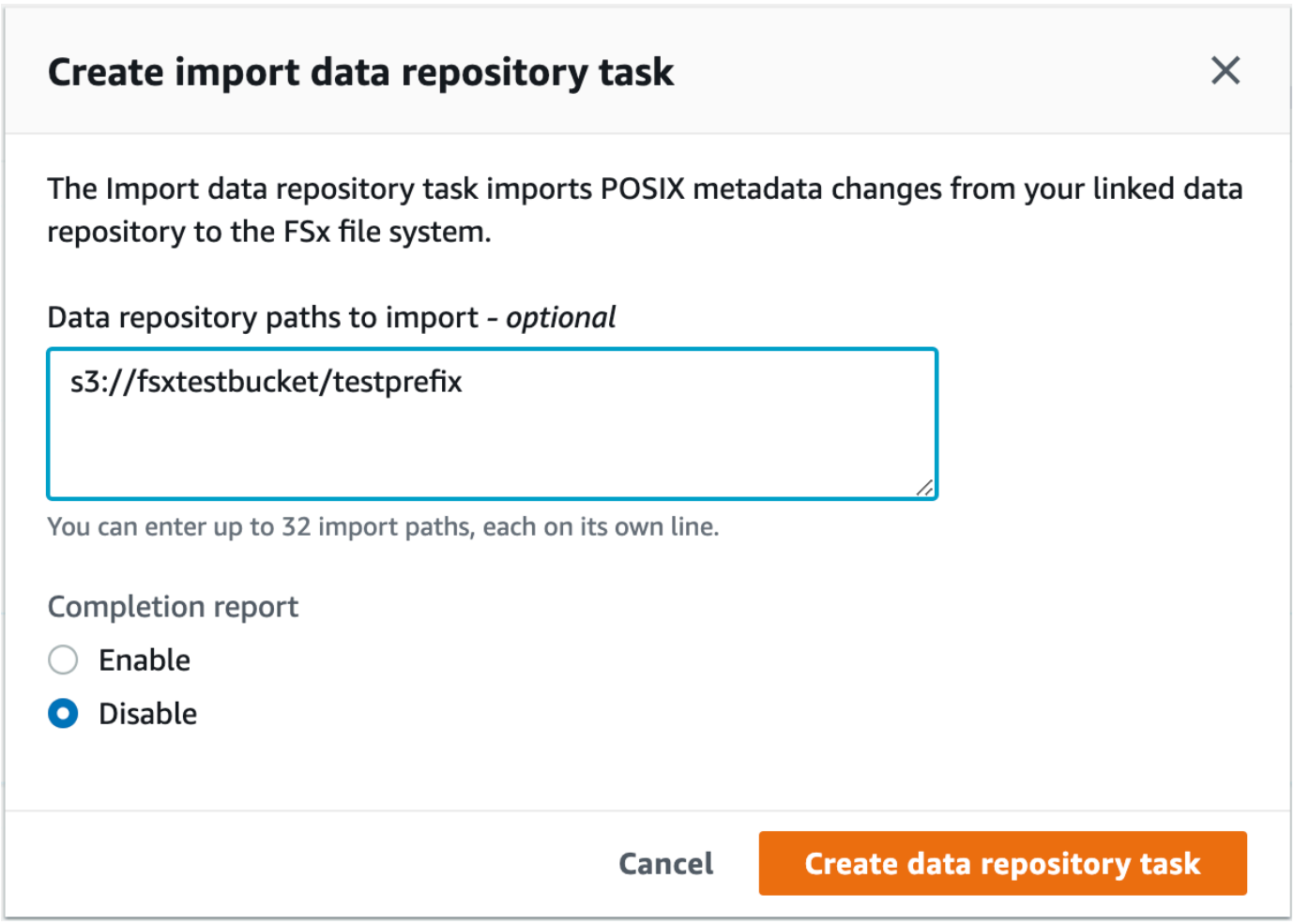
Verwenden von Datenrepository-Aufgaben zum Importieren von Änderungen

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.



6. (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.

7. (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.
8. Wählen Sie Create (Erstellen) aus.

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 unterZugreifen auf Daten-Repository-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 `NOOP` 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
```

Sie können Ihr gesamtes Dateisystem oder ein ganzes Verzeichnis innerhalb Ihres Dateisystems vorab laden, indem Sie die folgenden Befehle verwenden. (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 Verwalten 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 verknüpftes 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

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-ManagementkonsoleAWS 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-Datenrepository 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 beschriebenVerwenden 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 `AgeOfOldestQueuedMessage` 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 und AutoExport Metriken.

> **Important**
>
> Wenn Sie eine Datenrepository-Zuordnung oder ein Dateisystem mit aktiviertem automatischen Export löschen, sollten Sie zunächst sicherstellen, dass der Wert Null `AgeOfOldestQueuedMessage` ist, d. h., dass es keine Änderungen gibt, die noch nicht exportiert wurden. Wenn der Wert größer als Null `AgeOfOldestQueuedMessage` 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 `AgeOfOldestQueuedMessage` Sie, bis Null erreicht ist, bevor Sie Ihre Datenrepository-Zuordnung oder Ihr Dateisystem löschen.

Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen

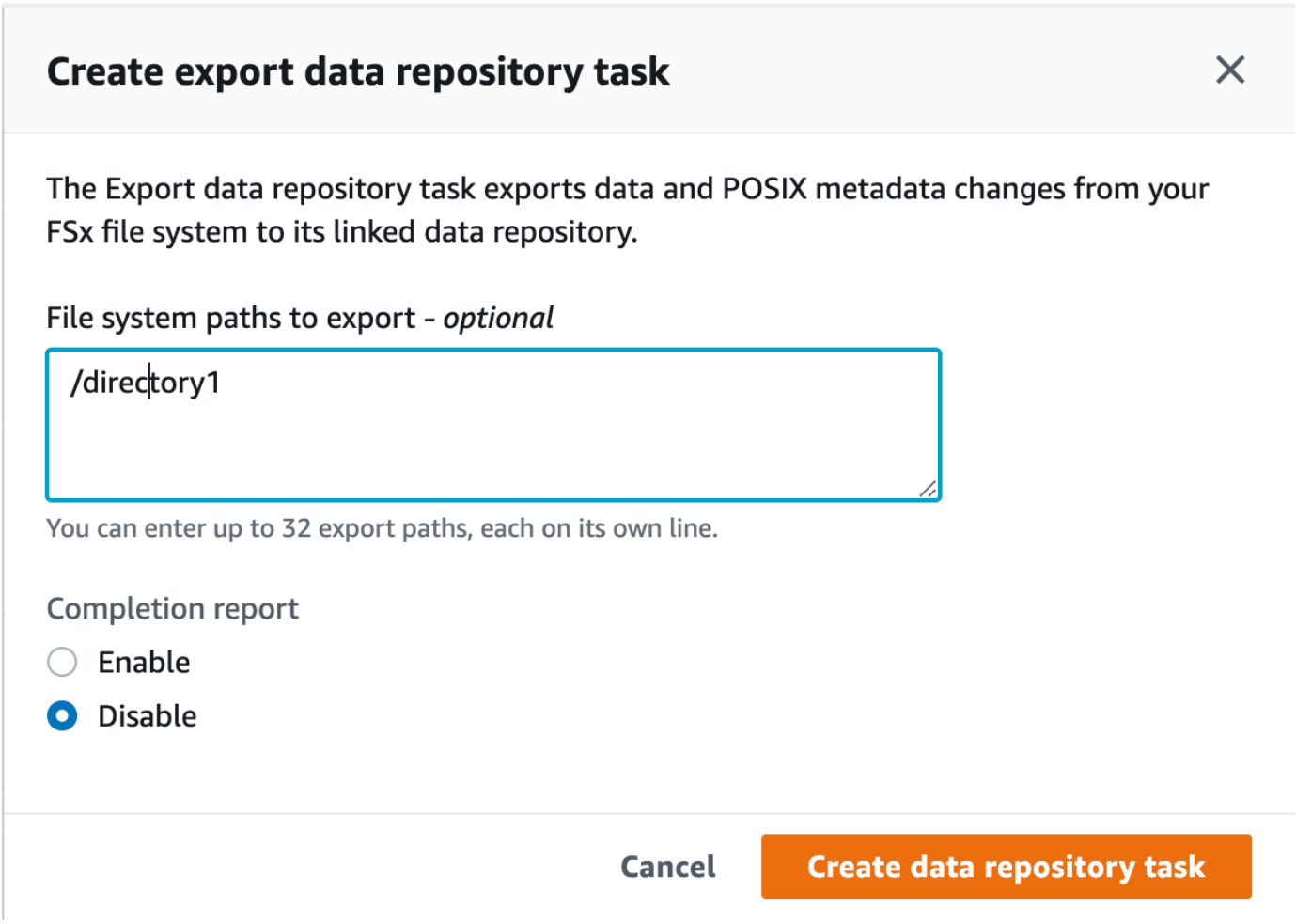
Die Aufgabe zum Exportieren von Datenrepositorien exportiert Dateien, die in Ihrem Dateisystem neu sind oder geändert wurden. Sie erstellt ein neues Objekt in S3 für jede neue Datei im Dateisystem. Für jede Datei, die im Dateisystem geändert wurde oder deren Metadaten geändert wurden, wird das entsprechende 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 Zieldatei 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 Datenrepository auf S3 verknüpft ist. Das Aufgabendialogfeld Exportdaten-Repository erstellen wird angezeigt.



6. (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 Einhängepunkt 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.

7. (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.
8. Wählen Sie Create (Erstellen) aus.

   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 unterZugreifen auf Daten-Repository-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.

Daten-Repository-Aufgaben

Durch die Verwendung von Import- und Exportaufgaben für Daten-Repositorys können Sie die Übertragung von Daten und Metadaten zwischen Ihrem FSx-for-Lustre-Dateisystem und jedem seiner dauerhaften Daten-Repositorys auf Amazon S3 verwalten.

Daten-Repository-Aufgaben optimieren Daten- und Metadatenübertragungen 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 seinem verknüpften Daten-Repository zu verfolgen. Sie tun dies auch, indem sie parallele Übertragungstechniken verwenden, um Daten mit Geschwindigkeiten von bis zu Hunderten von GB/s zu übertragen. Sie erstellen und zeigen Daten-Repository-Aufgaben mithilfe der Amazon-FSx-Konsole AWS CLI, der und der Amazon-FSx-API an.

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

Sie können eine Release-Daten-Repository-Aufgabe verwenden, um Dateisystemspeicher für neue Dateien freizugeben, indem Sie Dateien freigeben, die nach Amazon S3 exportiert wurden. Der Inhalt der freigegebenen Datei wird entfernt, aber die Metadaten der freigegebenen Datei verbleiben im Dateisystem. Benutzer und Anwendungen können weiterhin auf eine freigegebene Datei zugreifen, indem sie die Datei erneut lesen. Wenn der Benutzer oder die Anwendung die freigegebene Datei liest, ruft FSx for Lustre den Dateiinhalt transparent von Amazon S3 ab.

Arten von Daten-Repository-Aufgaben

Es gibt drei Arten von Daten-Repository-Aufgaben:

- Export ierenSie Daten-Repository-Aufgaben aus Ihrem Lustre-Dateisystem in einen verknüpften S3-Bucket.
- Import ierenSie Daten-Repository-Aufgaben aus einem verknüpften S3-Bucket in Ihr Lustre-Dateisystem.
- Freigabe von Daten-Repository-Aufgaben – Freigabe von Dateien, die aus Ihrem Lustre-Dateisystem in einen verknüpften S3-Bucket exportiert wurden.

Weitere Informationen finden Sie unter Erstellen einer Daten-Repository-Aufgabe.

Themen

- Fehlerbehebung bei Daten-Repository-Aufgabenfehlern

Den Status und die Details einer Aufgabe verstehen

Eine Daten-Repository-Aufgabe kann einen der folgenden Status haben:

- PENDING zeigt an, dass Amazon FSx die Aufgabe nicht gestartet hat.
- EXECUTING zeigt an, dass Amazon FSx die Aufgabe verarbeitet.
- FAILED zeigt an, dass Amazon FSx die Aufgabe nicht erfolgreich verarbeitet hat. Beispielsweise kann es Dateien geben, die die Aufgabe nicht verarbeiten konnte. Die Aufgabendetails enthalten weitere Informationen über den Fehler. Weitere Informationen zu fehlgeschlagenen Aufgaben finden Sie unter Fehlerbehebung bei Daten-Repository-Aufgabenfehlern.
- SUCCEEDED zeigt an, dass Amazon FSx die Aufgabe erfolgreich abgeschlossen hat.
- CANCELED zeigt an, dass die Aufgabe abgebrochen und nicht abgeschlossen wurde.
- CANCELING zeigt an, dass Amazon FSx gerade die Aufgabe abbricht.

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

- Der Aufgabentyp:
  - `EXPORT_TO_REPOSITORY` gibt eine Exportaufgabe an.
  - `IMPORT_METADATA_FROM_REPOSITORY` gibt eine Importaufgabe an.
  - `RELEASE_DATA_FROM_FILESYSTEM` gibt eine Release-Aufgabe an.
- Das Dateisystem, auf dem die Aufgabe ausgeführt wurde.
- Die Zeit der Aufgabenerstellung.
- Der Aufgabenstatus.
- Die Gesamtzahl der Dateien, die die Aufgabe verarbeitet hat.
- Die Gesamtzahl der Dateien, die die Aufgabe erfolgreich verarbeitet hat.
- Die Gesamtzahl der Dateien, die die Aufgabe nicht verarbeiten konnte. Dieser Wert ist größer als Null, wenn der Aufgabenstatus FEHLGESCHLAGEN lautet. Detaillierte Informationen zu fehlgeschlagenen Dateien finden Sie in einem Aufgabenabschlussbericht. Weitere Informationen finden Sie unter Arbeiten mit Aufgabenabschlussberichten.
- Die Uhrzeit, zu der die Aufgabe gestartet wurde.

- Der Zeitpunkt, zu dem der Aufgabenstatus zuletzt aktualisiert wurde. Der Aufgabenstatus wird alle 30 Sekunden aktualisiert.

Weitere Informationen zum Zugriff auf vorhandene Daten-Repository-Aufgaben finden Sie unter Zugreifen auf Daten-Repository-Aufgaben.

Verwenden von Daten-Repository-Aufgaben

Sie können Daten-Repository-Aufgaben mithilfe der Amazon-FSx-Konsole, der CLI oder der API erstellen, duplizieren, anzeigen und abbrechen.

Themen

- Erstellen einer Daten-Repository-Aufgabe
- Duplizieren einer Aufgabe
- Zugreifen auf Daten-Repository-Aufgaben
- Abbrechen einer Daten-Repository-Aufgabe

Erstellen einer Daten-Repository-Aufgabe

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

Sie können drei Arten von Daten-Repository-Aufgaben erstellen:

- Die Aufgabe Daten-Repository 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 Daten-Repository 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 Daten-Repository freigeben 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.

Duplizieren einer Aufgabe

Sie können eine vorhandene Daten-Repository-Aufgabe in der Amazon-FSx-Konsole duplizieren. Wenn Sie eine Aufgabe duplizieren, wird eine genaue Kopie der vorhandenen Aufgabe auf der Seite Importdaten-Repository-Aufgabe erstellen oder Exportdaten-Repository-Aufgabe erstellen angezeigt. Sie können nach Bedarf Änderungen an den Pfaden vornehmen, die exportiert oder importiert werden sollen, bevor Sie die neue Aufgabe erstellen und ausführen.

> **Note**
>
> Eine Anforderung zum Ausführen einer doppelten Aufgabe schlägt fehl, wenn bereits eine exakte Kopie dieser Aufgabe ausgeführt wird. Eine genaue Kopie einer bereits ausgeführten Aufgabe enthält denselben Dateisystempfad oder dieselben Pfade im Falle einer Exportaufgabe oder dieselben Daten-Repository-Pfade im Falle einer Importaufgabe.

Sie können eine Aufgabe aus der Aufgabendetailansicht, dem Bereich Data Repository-Aufgaben auf der Registerkarte Data Repository für das Dateisystem oder von der Seite DataRepository-Aufgaben duplizieren.

So duplizieren Sie eine vorhandene Aufgabe

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

Zugreifen auf Daten-Repository-Aufgaben

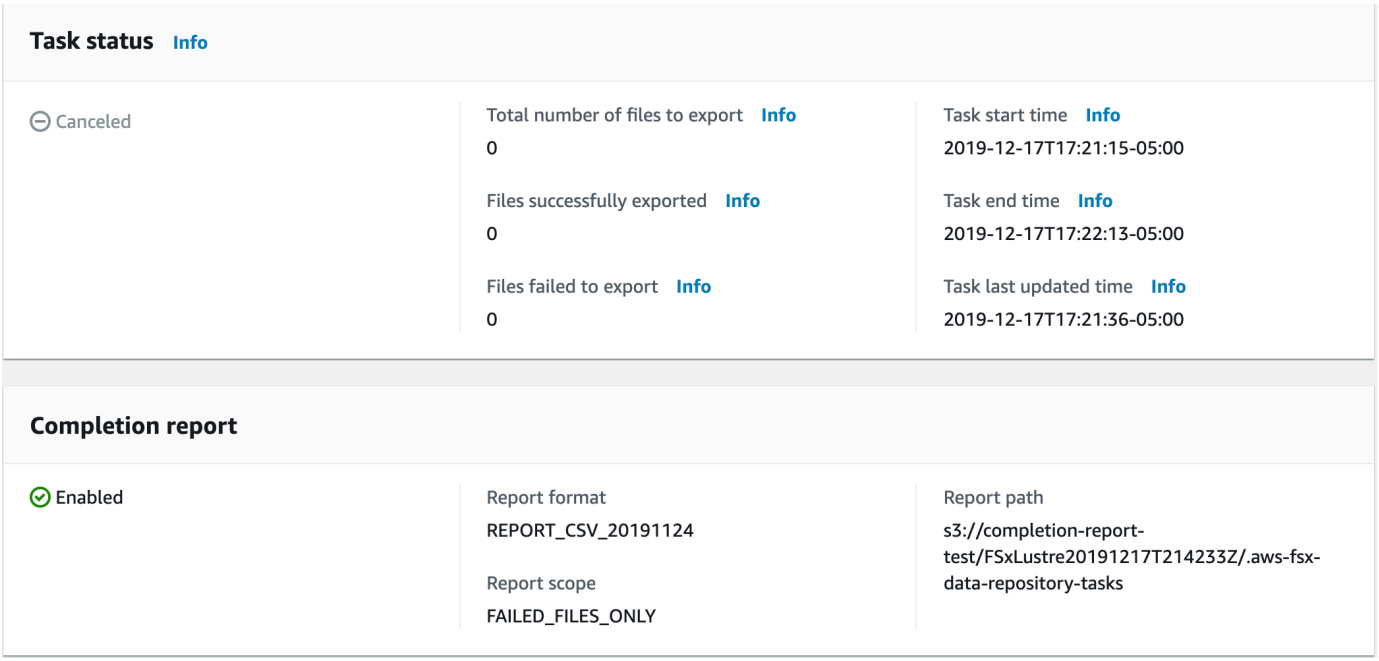
Nachdem Sie eine Daten-Repository-Aufgabe erstellt haben, können Sie über die Amazon-FSx-Konsole, die CLI und die API auf die Aufgabe und alle vorhandenen Aufgaben in Ihrem Konto zugreifen. Amazon FSx bietet die folgenden detaillierten Aufgabeninformationen:

- Alle vorhandenen Aufgaben.
- Alle Aufgaben für ein bestimmtes Dateisystem.
- Alle Aufgaben für eine bestimmte Daten-Repository-Zuordnung.
- Alle Aufgaben mit einem bestimmten Lebenszyklusstatus. Weitere Informationen zu den Statuswerten des Aufgabenlebenszyklus finden Sie unter Den Status und die Details einer Aufgabe verstehen.

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

So zeigen Sie Daten-Repository-Aufgaben und Aufgabendetails an (Konsole)

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Navigationsbereich Daten-Repository-Aufgaben (Lustre) aus. Die Seite Daten-Repository-Aufgaben wird angezeigt und zeigt vorhandene Aufgaben an.
3. Um die Details einer Aufgabe anzuzeigen, wählen Sie Aufgaben-ID oder Aufgabenname auf der Seite Daten-Repository-Aufgaben aus. Die Seite mit den Aufgabendetails wird angezeigt.



So rufen Sie Daten-Repository-Aufgaben und Aufgabendetails (CLI) ab

Mit dem Amazon-FSx`describe-data-repository-tasks`-CLI-Befehl können Sie alle Daten-Repository-Aufgaben und ihre Details in Ihrem Konto anzeigen. `DescribeDataRepositoryTasks` ist der entsprechende API-Befehl.

- Verwenden Sie den folgenden Befehl, um alle Daten-Repository-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"
```

```
        }
    ]
}
```

Anzeigen von Aufgaben nach Dateisystem

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

So zeigen Sie Aufgaben nach Dateisystem an (Konsole)

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

So rufen Sie Aufgaben nach Dateisystem (CLI) ab

- Verwenden Sie den folgenden Befehl, um alle Daten-Repository-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 Daten-Repository-Aufgabe

Sie können eine Daten-Repository-Aufgabe abbrechen, während sie sich entweder im Status PENDING oder EXECUTING befindet. Wenn Sie eine Aufgabe abbrechen, geschieht Folgendes:

- Amazon FSx verarbeitet keine Dateien, die sich in der zu verarbeitenden Warteschlange befinden.
- Amazon FSx verarbeitet weiterhin alle Dateien, die derzeit verarbeitet werden.
- Amazon FSx setzt keine Dateien zurück, die die Aufgabe bereits verarbeitet hat.

So brechen Sie eine Daten-Repository-Aufgabe ab (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 Daten-Repository-Aufgabe abbrechen möchten.
3. Öffnen Sie die Registerkarte Data Repository und scrollen Sie nach unten, um den Bereich Data-Repository-Aufgaben anzuzeigen.
4. Wählen Sie Aufgaben-ID oder Aufgabenname für die Aufgabe aus, die Sie abbrechen möchten.
5. Wählen Sie Aufgabe abbrechen, um die Aufgabe abzubrechen.
6. Geben Sie die Aufgaben-ID ein, um die Stornierungsanforderung zu bestätigen.

So stornieren Sie eine Daten-Repository-Aufgabe (CLI)

Verwenden Sie den Amazon-FSx`cancel-data-repository-task`-CLI-Befehl, um eine Aufgabe abzubrechen. `CancelDataRepositoryTask` ist der entsprechende API-Befehl.

- Verwenden Sie den folgenden Befehl, um eine Daten-Repository-Aufgabe abzubrechen.

```
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 Aufgabenabschlussberichten

Ein Aufgabenabschlussbericht enthält Details zu den Ergebnissen einer Export-, Import- oder Release-Daten-Repository-Aufgabe. Der Bericht enthält Ergebnisse für die von der Aufgabe verarbeiteten Dateien, die dem Umfang des Berichts entsprechen. Sie können angeben, ob ein Bericht für eine Aufgabe generiert werden soll, indem Sie den `-Enabled`Parameter verwenden.

Amazon FSx liefert den Bericht an das verknüpfte Daten-Repository des Dateisystems in Amazon S3 unter Verwendung des Pfads, den Sie beim Aktivieren des Berichts für eine Aufgabe angeben. Der Dateiname des Berichts gilt `report.csv` für Importaufgaben und `failures.csv` für Export- oder Release-Aufgaben.

Das Berichtsformat ist eine CSV-Datei (durch Kommas getrennte Werte), die drei Felder enthält: `FilePath`, `FileStatus`, und `ErrorCode`.

Berichte werden mit RFC-4180-format wie folgt kodiert:

- 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 mit einem zusätzlichen doppelten Anführungszeichen maskiert.

Im Folgenden finden Sie einige Beispiele für die Berichtskodierung:

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

Weitere Informationen zur RFC-4180-Kodierung finden Sie unter RFC-4180 – Gemeinsames Format und MIME-Typ für CSV-Dateien (Comma-Separated Values) auf der IETF-Website.

Im Folgenden finden Sie ein Beispiel für die Informationen in einem Aufgabenabschlussbericht, 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 Fehlerbehebung bei Daten-Repository-Aufgabenfehlern.

Fehlerbehebung bei Daten-Repository-Aufgabenfehlern

Sie können die Protokollierung in CloudWatch Logs aktivieren, um Informationen zu Fehlern zu protokollieren, die beim Importieren oder Exportieren von Dateien mithilfe von Daten-Repository-Aufgaben aufgetreten sind. Weitere Informationen zu CloudWatch Protokollen finden Sie unter Datenrepository-Ereignisprotokolle.

Wenn eine Daten-Repository-Aufgabe fehlschlägt, finden Sie die Anzahl der Dateien, die Amazon FSx nicht verarbeiten konnte, unter Dateien konnten nicht exportiert werden auf der Seite Aufgabenstatus 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 Daten-Repository-Aufgaben.

Für Daten-Repository-Aufgaben stellt Amazon FSx optional auch Informationen zu den spezifischen Dateien und Verzeichnissen bereit, die in einem Abschlussbericht fehlgeschlagen sind. Der Aufgabenabschlussbericht enthält die Datei oder den Verzeichnispfad auf dem fehlgeschlagenen Lustre-Dateisystem, seinen Status und den Grund für das Fehlschlagen. Weitere Informationen finden Sie unter Arbeiten mit Aufgabenabschlussberichten.

Eine Daten-Repository-Aufgabe kann aus mehreren Gründen fehlschlagen, einschließlich der im Folgenden aufgeführten.

Fehlercode	Erklärung
`FileSizeTooLarge`	Die maximale von Amazon S3 unterstützte Objektgröße beträgt 5 TiB .
`InternalError`	Im Amazon-FSx-Dateisystem ist ein Fehler für eine Import-, Export- oder Release-Aufgabe aufgetreten. Im Allgemeinen bedeutet dieser Fehlercode, dass sich das Amazon-FSx-Dateisystem, auf dem die fehlgeschlagene Aufgabe ausgeführt wurde, im Lebenszyk

Fehlercode	Erklärung
	lusstatus FEHLGESCHLAGEN befindet. In diesem Fall können die betroffenen Dateien aufgrund von Datenverlust möglicherweise nicht wiederhergestellt werden. Andernfalls können Sie hierarchische Speicherverwaltung sbefehle (HSM) 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.
`OperationNotPermitted`	Amazon FSx konnte die Datei nicht freigeben , da sie nicht in einen verknüpften S3-Bucket exportiert wurde. Sie müssen automatische Exporte oder Exporte von Daten-Repository-Aufgaben verwenden, um sicherzustellen, dass Ihre Dateien zuerst in Ihren verknüpften Amazon S3-Bucket exportiert werden.
`PathSizeTooLong`	Der Exportpfad ist zu lang. Die von S3 unterstüt zte maximale Objektschlüssellänge beträgt 1.024 Zeichen.
`ResourceBusy`	Amazon FSx konnte die Datei nicht exportieren oder freigeben, da auf sie von einem anderen Client im Dateisystem zugegriffen wurde. Sie können den erneut versuchen, DataRepos itoryTask nachdem Ihr Workflow mit dem Schreiben in die Datei fertig ist.

Fehlercode	Erklärung
`S3AccessDenied`	Der Zugriff auf Amazon S3 für eine Daten-Repository-Export- oder Importaufgabe wurde verweigert. Für Exportaufgaben muss das Amazon-FSx-Dateisystem über die Berechtigung zum Ausführen der `S3:PutObject` Operation zum Exportieren in ein verknüpftes Daten-Repository in S3 verfügen. Diese Berechtigung wird in der `AWSServiceRoleForFSxS3Access_` *`fs-0123456789abcdef0`* serviceverknüpften Rolle erteilt. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon FSx. Da für 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 `aws:SourceVpc` oder `aws:SourceVpce` IAM enthält. Für Importaufgaben muss das Amazon-FSx-Dateisystem über die Berechtigung zum Ausführen der `S3:GetObject` Operationen `S3:HeadObject` und zum Importieren aus einem verknüpften Daten-Repository auf S3 verfügen. Wenn Ihr S3-Bucket für Importaufgaben serverseitige Verschlüsselung mit vom Kunden verwalteten Schlüsseln verwendet, die in AWS Key Management Service (SSE-KMS) gespeichert sind, müssen Sie die Richtlinienkonfigurationen in befolgenArbeiten mit

Fehlercode	Erklärung
	serverseitig verschlüsselten Amazon S3 S3-Buckets. 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 Daten-Repository-Aufgaben S3-Metadaten ändern oder S3-Objekte überschreiben können, unabhängig davon, welches Konto sie hochgeladen hat. Wir empfehlen Ihnen, die Funktion S3 Object Ownership für Ihren S3-Bucket zu aktivieren. Mit dieser Funktion können Sie den Besitz neuer Objekte übernehmen, die andere in Ihren Bucket AWS-Konten hochladen, indem Sie Uploads zwingen, die `-/-acl bucket-owner-full-control` vordefinierte ACL bereitzustellen. Sie aktivieren S3 Object Ownership, indem Sie die Option Bucket-Eigentümer bevorzugt in Ihrem S3-Bucket auswählen. Weitere Informationen finden Sie unter Steuern des Eigentums an hochgeladenen Objekten mit S3 Object Ownership im Amazon S3-Benutzerhandbuch.
`S3Error`	Amazon FSx ist auf einen S3-related Fehler gestoßen, der nicht war`S3AccessDenied` .
`S3FileDeleted`	Amazon FSx konnte keine Hard Link-Datei exportieren, da die Quelldatei nicht im Daten-Repository vorhanden ist.

Fehlercode	Erklärung
`S3ObjectInUnsupportedTier`	Amazon FSx hat erfolgreich ein Nicht-Symlink-Objekt aus einer Speicherklasse S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive importiert. Die `FileStatus` wird `succeeded with warning` im Aufgabenabschlussbericht 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 `-hsm_restore` Befehl verwenden müssen, um das Objekt zu importieren.
`S3ObjectNotFound`	Amazon FSx konnte die Datei nicht importieren oder exportieren, da sie im Daten-Repository nicht vorhanden ist.
`S3ObjectPathNotPosixCompliant`	Das Amazon S3-Objekt ist vorhanden, kann aber nicht importiert werden, da es sich nicht um ein POSIX-konformes Objekt handelt. Informationen zu unterstützten POSIX-Met adaten finden Sie unter Unterstützung von POSIX-Metadaten für Daten-Repositorys.
`S3ObjectUpdateInProgressFro mFileRename`	Amazon FSx konnte die Datei nicht freigeben, da der automatische Export eine Umbenennu ng der Datei verarbeitet. Der automatis che Export-Umbenennungsprozess muss abgeschlossen sein, bevor die Datei freigegeb en werden kann.

Fehlercode	Erklärung
`S3SymlinkInUnsupportedTier`	Amazon FSx konnte ein Symlink-Objekt nicht importieren, da es sich in einer nicht unterstützten Amazon S3-Speicherklasse befindet, z. B. in einer Speicherklasse S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive. Die `FileStatus` wird `failed` im Aufgabenabschlussbericht enthalten sein.
`SourceObjectDeletedBeforeReleasing`	Amazon FSx konnte die Datei nicht aus dem Dateisystem freigeben, da die Datei aus dem Daten-Repository gelöscht wurde, bevor sie freigegeben 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 `atime`mem`time`, 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-Datenrepository exportiert wurden. Sie können Daten entweder mit der automatischen Exportfunktion, einer Aufgabe zum Exportieren eines Datenrepositorys oder mit HSM-Befehlen nach S3 exportieren. Um zu überprüfen, ob eine Datei in Ihr Daten-Repository 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 unter Verwendung von `sudo` ausführen.

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

Themen

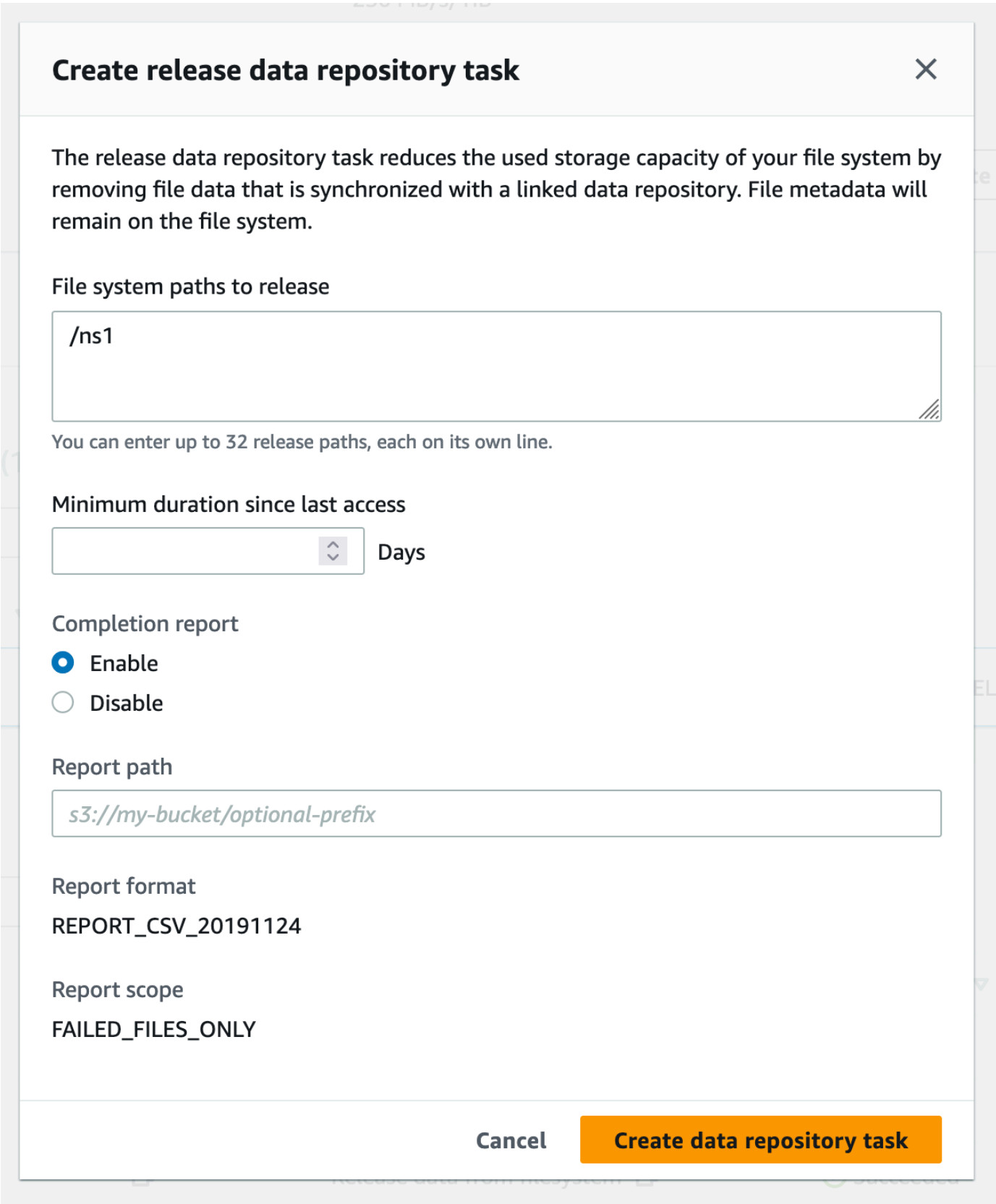
- Verwenden von Datenrepository-Aufgaben zur Freigabe von Dateien

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 Release-Aufgabe 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
/ns1
You can enter up to 32 release paths, each on its own line.
Minimum duration since last access
Days
Completion report
Enable
Disable
Report path
s3://my-bucket/optional-prefix
Report format
REPORT_CSV_20191124
Report scope
FAILED_FILES_ONLY
Cancel
Create data repository task

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 Einhängepunkt des Dateisystems beziehen. Wenn der Einhängepunkt 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 `atime`mem`time`, und berechnet`ctime`. 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 zur Übermittlung des Berichts anzugeben, geben Sie einen relativen Pfad im verknüpften S3-Datenrepository des Dateisystems als Berichtspfad ein.
9. Wählen Sie die Aufgabe „Datenrepository 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 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 veröffentlicht. 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 unterZugreifen auf Daten-Repository-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 aktivieren für CloudWatch Protokolle zur Protokollierung von Informationen über alle Fehler, die beim Import oder Export von Dateien mithilfe von Aufgaben zum automatischen Import, automatischen Export und zur Datenablage aufgetreten sind. Weitere Informationen finden Sie unter Protokollieren mit Amazon CloudWatch Logs.

> **Note**
>
> Wenn eine Datenrepository-Aufgabe fehlschlägt, schreibt Amazon FSx auch Fehlerinformationen in den Bericht zum Abschluss der Aufgabe. Weitere Informationen

zu Fehlerinformationen in Abschlussberichten finden Sie unterFehlerbehebung bei Daten-Repository-Aufgabenfehlern.

Automatische Import-, automatische Export- und Datenrepository-Aufgaben können aus verschiedenen Gründen fehlschlagen, einschließlich der unten aufgeführten. Informationen zum Anzeigen dieser Protokolle finden Sie unterAnzeigen von -Protokollen.

Ereignisse importieren

Fehlercode	Protokoebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ImportListObjectError`	ERROR	S3-Objekte konnten nicht im S3-Bucket aufgelistet werden*Bucket_me* mit Präfix*Präfix*.	Amazon FSx konnte S3-Objekte nicht im S3-Bucket auflisten. Dies kann passieren, wenn die S3-Bucket-Richtlinie Amazon FSx keine ausreichenden Berechtigungen gewährt.	–
`S3ImportUnsupportedTierWarning`	WARN	Das S3-Objekt mit dem Schlüssel konnte nicht importiert werden*Schlüsswert* im S3-Bucket *Bucket-Name* aufgrund	Amazon FSx konnte ein S3-Objekt nicht importieren, da es sich in einer Amazon S3-Speicherklasse befindet, die nicht unterstützt wird, wie	`S3ObjectInUnsupportedTier`

Fehlercode	Protokoebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
		eines S3-Objekts in einer nicht unterstützten Stufe*S3_Tier_Name* .	z. B. S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive.	
`S3ImportSymlinkInUnsupportedTierWarning`	WARN	Das S3-Objekt mit dem Schlüssel konnte nicht importiert werden*Schlüsselwert* im S3-Bucket *Bucket-Name* aufgrund eines S3-Symlink-Objekts in einer nicht unterstützten Stufe*S3_Tier_Name* .	Amazon FSx konnte ein Symlink-Objekt nicht importieren, da es sich in einer Amazon S3-Speicherklasse befindet, die nicht unterstützt wird, wie z. B. S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive.	`S3SymlinkInUnsupportedTier`

Fehlercode	Protokoebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ImportAccessDenied`	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht importiert werden*`Schlüsselwert`* im S3-Bucket *`Bucket-Name`* weil der Zugriff auf das S3-Objekt verweigert wurde.	Der Zugriff auf Amazon S3 wurde für eine Aufgabe zum Exportieren eines Datenrepositorys verweigert. Für Importaufgaben muss das Amazon FSx-Dateisystem über die erforderlichen Berechtigungen verfügen, um`s3:HeadObject` und`s3:GetObject` Operationen zum Importieren aus einem verknüpften Datenspeicher auf S3. Für Importaufgaben, wenn Ihr S3-Bucket serverseitige	`S3AccessDenied`

Fehlercode	Protokoebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
			Verschlüsselung mit vom Kunden verwalteten Schlüsseln verwendet, die in gespeichert sindAWS Key Management Service(SSE-KMS) müssen Sie die Richtlinienkonfigurationen in befolgenArbeiten mit serversei tig verschlüsselten Amazon S3 S3-Buckets.	

Fehlercode	Protokoebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ImportDeleteAccessDenied`	ERROR	Die lokale Datei für das S3-Objekt mit dem Schlüssel konnte nicht gelöscht werden*`Schlüsselwert`* im S3-Bucket *`Bucket-Name`* weil der Zugriff auf das S3-Objekt verweigert wurde.	Dem automatischen Import wurde der Zugriff auf ein S3-Objekt verweigert.	–

Fehlercode	Protokoebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ImportObjectPathNotPosixCompliant`	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht importiert werden*`Schlüsselwert`* im S3-Bucket *`Bucket-Name`* weil das S3-Objekt nicht POSIX-konform ist.	Das Amazon S3-Objekt ist vorhanden, kann aber nicht importiert werden, da es kein POSIX-kompatibles Objekt ist. Informationen zu unterstützten POSIX-Metadaten finden Sie unterUnterstützung von POSIX-Metadaten für Daten-Repositorys.	`S3ObjectPathNotPosixCompliant`

Fehlercode	Protokoebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ImportObjectTypeMismatch`	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht importiert werden*Schlüsselwert* im S3-Bucket *Bucket-Name* weil ein S3-Objekt mit demselben Namen bereits 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.	–

Fehlercode	Protokoebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ImportObjectDeleted`	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht importiert werden*Schlüsselwert* weil es nicht im S3-Bucket gefunden wurde*Bucket_Name* .	Amazon FSx konnte Dateimetadaten nicht importieren, da das entsprechende Objekt nicht im Daten-Repository existiert.	`S3FileDeleted`
`S3ImportBucketDoesNotExist`	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht importiert werden*Schlüsselwert* im S3-Bucket *Bucket-Name* da der Bucket nicht existiert.	Amazon FSx kann ein S3-Objekt nicht automatisch in das Dateisystem importieren, da der S3-Bucket nicht mehr existiert.	–

Fehlercode	Protokoebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ImportDeleteBucketDoesNotExist`	ERROR	Die lokale Datei für das S3-Objekt mit dem Schlüssel konnte nicht gelöscht werden*Schlüsselwert* im S3-Bucket *Bucket-Name* 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.	–
`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.	–

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`NoDiskSpace`	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht importiert werden*Schlüsselwert* im S3-Bucket *Bucket-Name* weil das Dateisystem voll ist.	Das Dateisystem hatte beim Erstellen der Datei oder des Verzeichnisses keinen Speicherplatz mehr auf den Metadatenservern.	–

Ereignisse exportieren

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ExportInternalError`	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht exportiert werden*Schlüsselwert* im S3-Bucket*Bucket-Name* aufgrund eines internen Fehlers.	Das Objekt wurde aufgrund eines internen Fehlers nicht exportiert.	`INTERNAL_ERROR`
`S3ExportAccessDenied`	ERROR	Die Datei konnte nicht exportiert werden, da der Zugriff auf das	Der Zugriff auf Amazon S3 wurde für eine Aufgabe zum	`S3AccessDenied`

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
		S3-Objekt mit dem Schlüssel verweigert wurde*Schlüsselwert* im S3-Bucket*Bucket-Name* .	Exportieren eines Datenrepositorys verweigert. Für Exportaufgaben muss das Amazon FSx-Dateisystem über die erforderlichen Berechtigungen verfügen, um`s3:PutObject` Vorgang zum Exportieren in ein verknüpftes Daten-Repository auf S3. Diese Erlaubnis wird erteilt in`AWSServiceRoleForFSxS3Access_`*fs-0123456789abcdef0* Rolle, die mit einem Dienst verknüpft ist. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon FSx.	

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
			Da für die Exportaufgabe Daten außerhalb der VPC eines Dateisystems fließen müssen, kann dieser Fehler auftreten , wenn das Ziel-Repo sitory über eine Bucket-Richtlinie verfügt, die eine der`aws:Sourc eVpc` oder`aws:Sc eVpce` Globale IAM-Bedin gungsschlüssel. Wenn Ihr S3-Bucket Objekte enthält, die von einem anderen hochgeladen wurdenAWS-Kontoals Ihr mit dem Dateisyst em verknüpft es S3-Bucket-Konto können Sie sicherste llen, dass Ihre Datenrepo sitory-Aufgaben	

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
			S3-Metadaten ändern oder S3-Objekte überschreiben können, unabhängig davon, welches Konto sie hochgeladen hat. Wir empfehlen, dass Sie die Funktion S3 Object Ownership für Ihren S3-Bucket aktivieren. Mit dieser Funktion können Sie die Verantwortung für neue Objekte übernehmen, die andereAWS-Kontenladen Sie es in Ihren Bucket hoch, indem Sie Uploads zwingen, Folgendes bereitzustellen`--acl bucket-owner-full-control` gescannrs ACL. Sie	

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
			aktivieren S3 Object Ownership , indem SieBevorzugter Bucket-BesitzerOption in Ihrem S3-Bucket. Weitere Informationen finden Sie unterSteuern des Eigentums an hochgeladenen Objekten mithilfe von S3 Object Ownershipin derAmazon S3-Benutzerhandbuch.	
`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 Objektschlüssellänge beträgt 1.024 Zeichen.	`PathSizeTooLong`

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ExportFileSizeTooLarge`	ERROR	Die Datei konnte nicht exportiert werden, da die Dateigröße die maximal unterstützte Größe von S3-Objekten überschreitet.	Die von Amazon S3 unterstützte maximale Objektgröße beträgt 5 TiB.	`FileSizeTooLarge`

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ExportKMSKeyNotFound`	ERROR	Die Datei für das S3-Objekt mit Schlüssel konnte nicht exportiert werden*`Schlüsselwert`* im S3-Bucket*`Bucket-Name`* weil der KMS-Schlüssel des Buckets nicht gefunden wurde.	Amazon FSx konnte die Datei nicht exportieren, weilAWS KMS keykonnte nicht gefunden werden. Achten Sie darauf, einen Schlüssel zu verwenden, der sich im selben befindetAWS-Region wie der S3-Bucket. Weitere Informationen zum Erstellen von KMS-Schlüsseln finden Sie unterSchlüssel erstellenin der AWS Key Management ServiceLeitfaden für Entwickler.	`N/A`

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	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`
`S3ExportLocalObjectReleaseWithoutS3Source`	WARN	Export übersprungen: Die lokale Datei befindet sich im Status Freigegeben und es handelt sich um ein verknüpftes S3-Objekt mit Schlüssel *`key_value`* wurde im Bucket nicht gefunden*`Bucket_me`* .	Amazon FSx konnte die Datei nicht exportieren, da sie sich im Dateisystem in einem freigegebenen Zustand befand.	–

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3ExportLocalObjectNotMatchDra`	WARN	Export übersprungen: Die lokale Datei gehört nicht zu einem mit einem Datenrepository verknüpften Dateisystempfad.	Amazon FSx konnte nicht exportieren, da das Objekt nicht zu einem Dateisystempfad gehört, der mit einem Daten-Repository verknüpft ist.	–
`InternalAutoExportError`	ERROR	Beim automatischen Export ist beim Export eines Dateisystemobjekts ein interner Fehler aufgetreten	Der Export ist aufgrund eines internen Fehlers (Autoexport oder Lustreebene) fehlgeschlagen.	–
`S3CompletionReportUploadFailure`	ERROR	Der Abschlussbericht für die Aufgabe im Datenrepository konnte nicht hochgeladen werden*Bucket_Name*	Amazon FSx konnte den Abschlussbericht nicht hochladen.	–

Fehlercode	Protokollebene	Nachricht protokollieren	Grundursache	Fehlercode im Abschlussbericht
`S3CompletionReportValidateFailure`	ERROR	Der Bericht über den Abschluss der Datenrepository-Aufgabe konnte nicht in den Bucket hochgeladen werden*bucket_name* weil der Pfad zum Abschlussbericht*report_path* gehört nicht zu einem Daten-Repository, 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.	–

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 derDateisystem erstellenAssistent, Sie legen die folgenden Eigenschaften der Datenrepository-Konfiguration im optionalen Feld festImportieren/Exportieren von DatenrepositorienFensterscheibe.

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

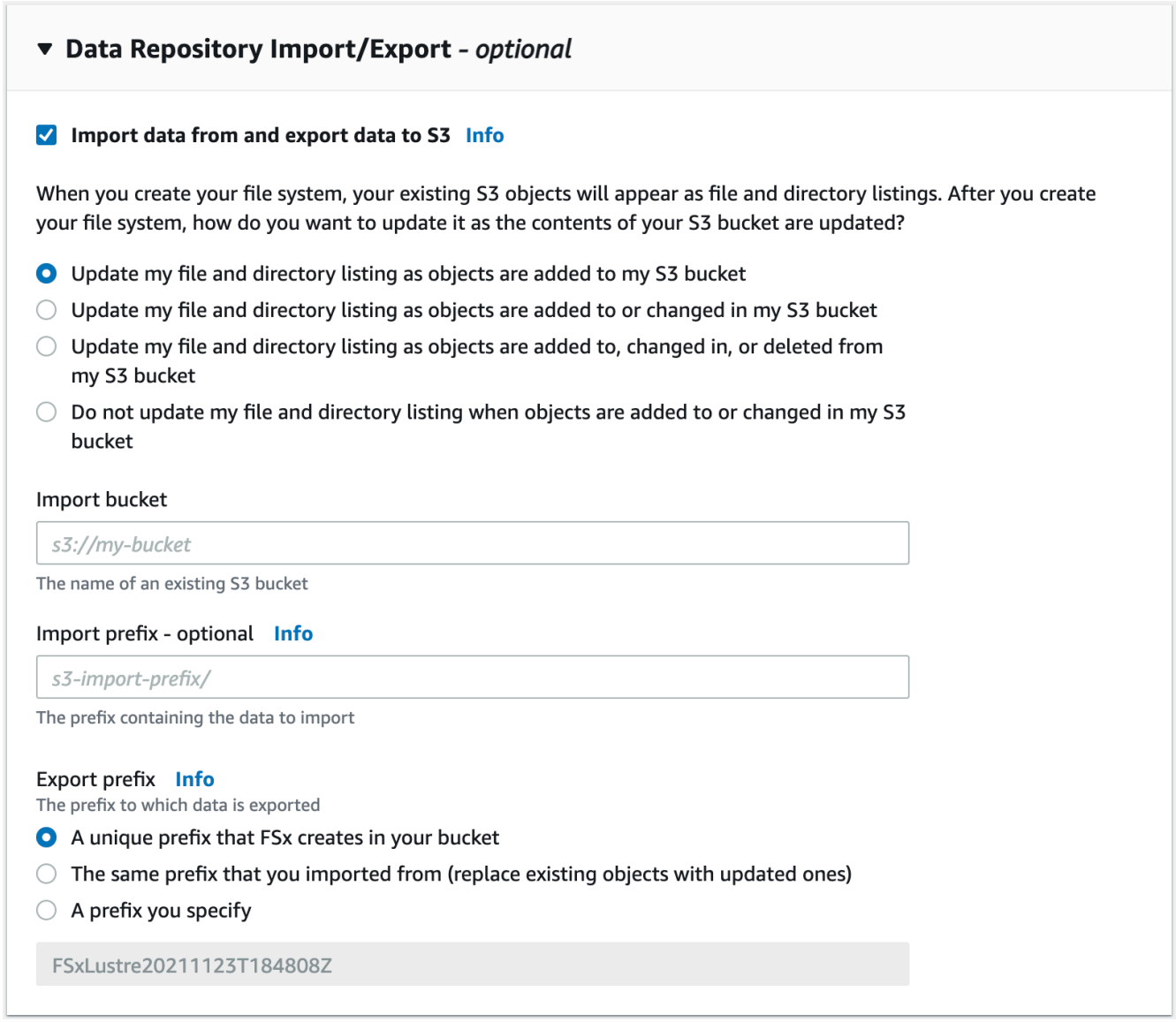
Mit dieser Methode können Sie bei der Angabe des Importpfads ein Importpräfix angeben, ohne dass sich dies auf eine 1:1 -Zuordnung für Exporte auswirkt.

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 desAWSManagement-Konsole undAWSBefehlszeilenschnittstelle (AWSCLI).

Console

1. Öffnen Sie die Amazon FSx-Konsole unterhttps://console.aws.amazon.com/fsx/.
2. Wählen Sie im DashboardDateisystem erstellen.
3. Wählen Sie für den DateisystemtypFSx für Lustre, und wählen Sie dannWeiter.
4. Geben Sie die erforderlichen Informationen für dieDateisystemdetailsundNetzwerk und SicherheitAbschnitte. Weitere Informationen finden Sie unter Erstellen Sie Ihr FSx for Lustre-Dateisystem.
5. Du benutzt dieImportieren/Exportieren von DatenrepositorienPanel zur Konfiguration eines verknüpften Datenrepositorys in Amazon S3. Wählen SieDaten aus S3 importieren und nach S3 exportierenzur Erweiterung derImportieren/Exportieren von Datenrepositorienschneiden Sie die Einstellungen des Datenrepositorys ab und konfigurieren Sie sie.



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 optionalesPräfix importierenwenn 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 verfügbarenPräfix exportierenOptionen:

   - 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 SieWeiter, 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 istlustre-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 lautetNONE, was sich vom Standardverhalten bei Verwendung der Konsole unterscheidet.

Verwenden Sie den Amazon FSx CLI-Befehl, um ein FSx for Lustre-Dateisystem zu erstellencreate-file-system, wie unten gezeigt. Die entsprechende API-Operation istCreateFileSystem.

```
$ 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

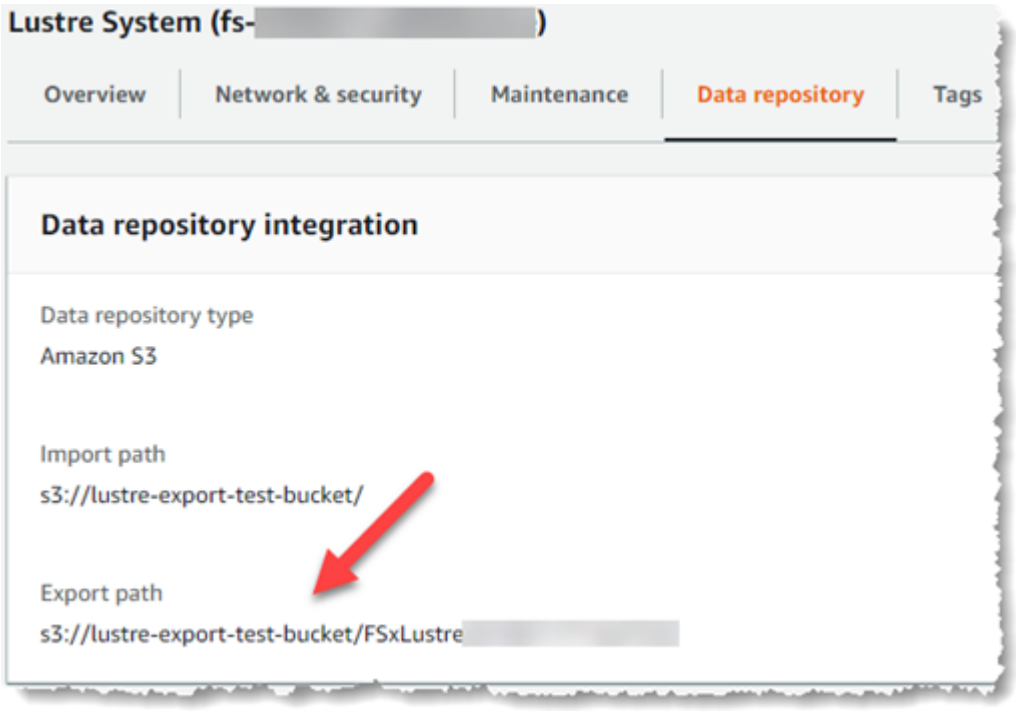
Sie können den Exportpfad eines Dateisystems mithilfe der FSx for Lustre-Konsole einsehen, derAWSCLI und die API.

Console

1. Öffnen Sie die Amazon FSx-Konsole unterhttps://console.aws.amazon.com/fsx/
2. Wählen SieName des DateisystemsoderDateisystem-IDfür das FSx for Lustre-Dateisystem, für das Sie den Exportpfad anzeigen möchten.

   Die Seite mit den Dateisystemdetails für dieses Dateisystem wird angezeigt.
3. Wähle denDatenspeicherTab.

   DerIntegration von DatenrepositorienEin Fenster 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-1111111"
    ],
    "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, derAWSBefehlszeilenschnittstelle und die Amazon FSx-API. In

der Amazon FSx-Konsole können Sie auf das Datenrepository zugreifenStatus des Lebenszyklusin derIntegration von DatenrepositorienBereich desDatenspeicherTab für das Dateisystem. Der`Lifecycle`Die 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, derAWSCLI und dieAWSAPI. (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.AWSRegion, 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 nicht`FSx`Konfiguration 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 derFSxDie Konfiguration der Ereignisbenachrichtigung im verknüpften S3-Bucket wurde gelöscht oder geändert.

Jede dieser Bedingungen führt dazu, dass der Lebenszyklusstatus des Datenrepositorys zuFalsch 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 Verknüpfen Sie Ihr Dateisystem mit einem S3-Bucket.

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

Console

1. Öffnen Sie die Amazon FSx-Konsole unterhttps://console.aws.amazon.com/fsx/.
2. Wählen Sie im DashboardDateisysteme.
3. Wählen Sie das Dateisystem aus, das Sie verwalten möchten, um die Dateisystemdetails anzuzeigen.
4. Wählen SieDatenspeicherum die Einstellungen des Datenrepositorys einzusehen.
   Sie können die Importeinstellungen ändern, wenn der Lebenszyklusstatus lautetVERFÜGBARoderFALSCH KONFIGURIERT. Weitere Informationen finden Sie unter Status des Lebenszyklus des Datenrepositorys.
5. Wählen SieAktionen, und wählen Sie dannImporteinstellungen aktualisierenum die anzuzeigenImporteinstellungen aktualisierenDialogfenster.
6. Wählen Sie die neue Einstellung aus und wählen Sie dannAktualisierenum 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"
            }
        }
    ]
}
```

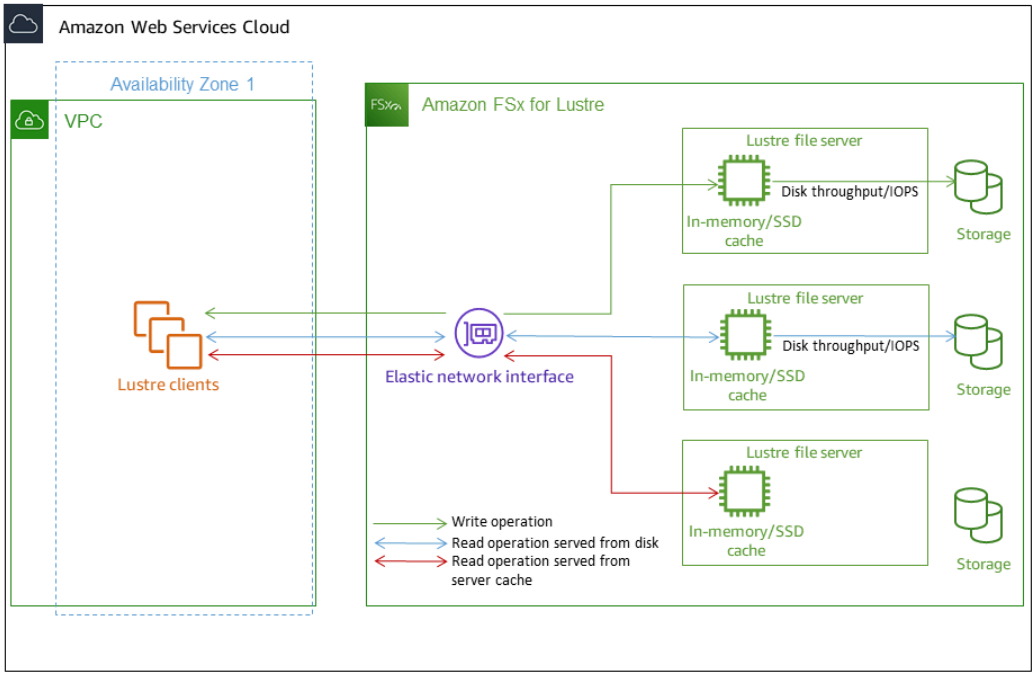
Leistung von Amazon FSx für Lustre

Amazon FSx for Lustre, das auf Lustre, dem beliebten Hochleistungsdateisystem, basiert, bietet Aufskalierungsleistung, die linear mit der Größe eines Dateisystems zunimmt. Lustre-Dateisysteme skalieren horizontal über mehrere Dateiserver und Datenträger hinweg. Diese Skalierung gibt jedem Client direkten Zugriff auf die auf jeder Festplatte gespeicherten Daten, um viele der Engpässe zu entfernen, die in herkömmlichen Dateisystemen vorhanden sind. Amazon FSx for Lustre baut auf der skalierbaren Architektur von Lustre auf, um ein hohes Leistungsniveau für eine große Anzahl von Clients zu unterstützen.

Themen

Funktionsweise von FSx-for-Lustre-Dateisystemen

Jedes FSx-für-Lustre-Dateisystem besteht aus den Dateiservern, mit denen die Clients kommunizieren, und einem Satz von Datenträgern, die an jeden Dateiserver angeschlossen sind, der Ihre Daten speichert. 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 Lese-Cache bereitgestellt werden, um die Leistung für die am häufigsten aufgerufenen Daten weiter zu verbessern. Wenn ein Client auf Daten zugreift, die im In-Memory- oder SSD-Cache gespeichert sind, muss der Dateiserver diese nicht von der Festplatte lesen, wodurch die Latenz reduziert und der Gesamtdurchsatz erhöht wird, den Sie erreichen können. Das folgende Diagramm veranschaulicht die Pfade eines Schreibvorgangs, eines Lesevorgangs, der von der Festplatte bereitgestellt wird, und eines Lesevorgangs, der von In-Memory- oder SSD-Cache bereitgestellt wird.



Wenn Sie Daten lesen, die im In-Memory- 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 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 HDD-Speicherkapazität des Dateisystems dimensioniert wird. Dies bietet Latenzen unter einer Millisekunde und höhere IOPS für häufig aufgerufene Dateien.

Aggregierte Dateisystemleistung

Der Durchsatz, den ein FSx for Lustre-Dateisystem unterstützt, ist proportional zu seiner Speicherkapazität. Dateisysteme von Amazon FSx für Lustre skalieren auf Hunderte von GBpss Durchsatz und Millionen von IOPS. Amazon FSx for Lustre unterstützt auch den gleichzeitigen Zugriff auf dieselbe Datei oder dasselbe Verzeichnis von Tausenden von Datenverarbeitungs-Instances. Dieser Zugriff ermöglicht ein schnelles Daten-Checkpointing vom Anwendungsspeicher zum Speicher, was eine gängige Technik bei High Performance Computing (HPC) ist. Sie können

die Speicher- und Durchsatzkapazität jederzeit nach Bedarf erhöhen, nachdem Sie das Dateisystem erstellt haben. Weitere Informationen finden Sie unter Verwalten der Speicherkapazität.

Dateisysteme von FSx für Lustre bieten einen Burst-Lesedurchsatz mithilfe eines Netzwerk-I/O-Guthabenmechanismus, um die Netzwerkbandbreite basierend auf der durchschnittlichen Bandbreitenauslastung zuzuweisen. Die Dateisysteme sammeln Guthaben an, wenn ihre Netzwerkbandbreitennutzung unter ihren Basisgrenzen liegt, und können diese Guthaben bei der Durchführung von Netzwerkdatenübertragungen verwenden.

Die folgenden Tabellen zeigen die Leistung, für die die FSx-for-Lustre-Bereitstellungsoptionen entwickelt wurden.

Dateisystemleistung für SSD-Speicheroptionen

Bereitstellungstyp	Netzwerkdurchsatz (MB/s/TiB bereitgestellter Speicher)		Netzwerk-IOPS (IOPS/TiB bereitgestellter Speicher)	Cache-Speicher (GiB RAM/TiB bereitgestellter Speicher)	Festplattenlatenzen pro Dateioperation (Millisekunden, P50)	Festplattendurchsatz (MBpsTiB Speicher oder SSD-Cache bereitgestellt)	
	Baseline	Burst				Baseline	Burst
SCRATCH_2	200	1300	Zehntausende Baseline Hunderttausende Burst	6.7	Metadaten: Unter-ms Daten: sub-ms	200 (lesen) 100 (Schreiben)	-
PERSISTENT-125	320	1300		3.4		125	500
PERSISTENT-250	640	1300		6.8		250	500
PERSISTENT-500	1300	-		13.7		500	-
PERSISTENT-1000	2600	-		27.3		1000	-

Dateisystemleistung für HDD-Speicheroptionen

Bereitstellungstyp	Netzwerkdurchsatz (MB/s/TiB Speicher oder SSD-Cache bereitgestellt)		Netzwerk-IOPS (IOPS/TiB bereitgestellter Speicher)	Cache-Speicher (GiB RAM/TiB bereitgestellter Speicher)	Festplattenlatenzen pro Dateioperation (Millisekunden, P50)	Festplattendurchsatz (MBpsTiB Speicher oder SSD-Cache bereitgestellt)	
	Baseline	Burst				Baseline	Burst
PERSISTENT-12							
HDD-Speicher	40	375*	Zehntausende Baseline Hunderttausende Burst	0.4 memory	Metadaten: Unter-ms Daten: einstellige ms	12	80 (lesen) 50 (Schreiben)
SSD-Lese-Cache	200	1,900		200-SSD-Cache	Daten: sub-ms	200	-
PERSISTENT-40							
HDD-Speicher	150	1,300*	Zehntausende Baseline Hunderttausende Burst	1.5	Metadaten: Unter-ms Daten: einstellige ms	40	250 (lesen) 150 (Schreiben)
SSD-Lese-Cache	750	6500		200 SSD cache	Daten: sub-ms	200	-

Dateisystemleistung für SSD-Speicheroptionen der vorherigen Generation

Bereitstellungstyp	Netzwerkdurchsatz (MB/s pro TiB bereitgestelltem Speicher)		Netzwerk-IOPS (IOPS pro TiB bereitgestelltem Speicher)	Cache-Speicher (GiB pro TiB bereitgestellter Speicher)	Festplattenlatenzen pro Dateioperation (Millisekunden, P50)	Festplattendurchsatz (MB/s pro TiB Speicher oder SSD-Cache bereitgestellt)	
	Baseline	Burst				Baseline	Burst
PERSISTENT-50	250	1,300*	Zehntausende Baseline Hunderttausende Burst	2.2 RAM	Metadaten: Unter-ms Daten: sub-ms	50	240
PERSISTENT-100	500	1,300*		4.4 RAM		100	240
PERSISTENT-200	750	1,300*		8.8 RAM		200	240

> **Note**
>
> *Persistente Dateisysteme im Folgenden AWS-Regionen bieten Netzwerk-Burst 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).

> **Note**
>
> Die Bereitstellungsoption FSx for Lustre SCRATCH_1 wurde entwickelt, um 200 MB/s/TiB zu unterstützen.

Beispiel: Aggregierter Basis- 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 Durchsatz pro TiB pro Speichereinheit bietet einen aggregierten Basis-Festplattendurchsatz 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 unter einer Millisekunde für Dateioperationen.

Layout des Dateisystemspeichers

Alle Dateidaten in Lustre werden auf Speicher-Volumes gespeichert, die als Objektspeicherziele (OSTs) bezeichnet werden. Alle Dateimetadaten (einschließlich Dateinamen, Zeitstempel, Berechtigungen und mehr) werden auf Speicher-Volumes gespeichert, die als Metadatenziele (MDTs) bezeichnet werden. Dateisysteme von Amazon FSx für Lustre bestehen aus einem einzigen MDT und mehreren OSTs. Jedes OST ist je nach Bereitstellungstyp des Dateisystems etwa 1 bis 2 TiB groß. Amazon FSx for Lustre verteilt Ihre Dateidaten auf die OSTs, aus denen Ihr Dateisystem besteht, um die Speicherkapazität mit Durchsatz und IOPS-Last auszugleichen.

Um die Speichernutzung der MDTs und OSTs anzuzeigen, 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
mountname-MDT0000_UUID      68.7G        5.4M       68.7G   0% /fsx[MDT:0]
mountname-OST0000_UUID       1.1T        4.5M        1.1T   0% /fsx[OST:0]
mountname-OST0001_UUID       1.1T        4.5M        1.1T   0% /fsx[OST:1]

filesystem_summary:          2.2T        9.0M        2.2T   0% /fsx
```

Entfernen von Daten in Ihrem Dateisystem

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

Das Entfernen bedeutet, dass Dateien in mehrere Blöcke unterteilt werden können, die dann in verschiedenen OSTs gespeichert werden. Wenn eine Datei auf mehrere OSTs verteilt ist, werden Lese- oder Schreibanforderungen an die Datei auf diese OSTs verteilt, wodurch der Gesamtdurchsatz oder die IOPS erhöht wird, die Ihre Anwendungen durch sie übertragen können.

Im Folgenden sind die Standardlayouts für Dateisysteme von Amazon FSx für Lustre 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 Datei, die in Amazon FSx for Lustre mit Standard-Linux-Tools erstellt wurde, auf einer einzigen Festplatte gespeichert wird.
- Für Dateisysteme, die nach dem 18. Dezember 2020 erstellt wurden, ist das Standardlayout ein progressives Dateilayout, in dem Dateien mit einer Größe von 1GiB 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 4-teiliges progressives Dateilayout, das in erläutert wirdProgressive Dateilayouts.
- Für alle Dateisysteme verwenden Dateien, die aus Amazon S3 importiert wurden, unabhängig von ihrem Erstellungsdatum nicht das Standardlayout, sondern das Layout im `ImportedFileChunkSize` Parameter des Dateisystems. S3-imported Dateien, die größer als sind`ImportedFileChunkSize`, werden auf mehreren OSTs mit einer Stripe-Anzahl von gespeichert`(FileSize / ImportedFileChunksize) + 1`. Der Standardwert von `ImportedFileChunkSize` ist 1GiB.

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 Anzahl der Stripes gibt an, wie viele OSTs die Datei mit einem Stripeshot versehen ist. Die Stripe-Größe gibt an, wie viele kontinuierliche Daten auf einem OST gespeichert werden. Der Stripe-Offset ist der Index des ersten OST, über das die Datei getripelt wird.

Ändern Ihrer Markierungskonfiguration

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 angegebenen 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 sie, um das Layout einer Datei anzugeben, bevor Sie sie erstellen. Sie können auch ein Layout für ein Verzeichnis definieren. Sobald dieses Layout in einem Verzeichnis festgelegt ist, wird es auf jede neue Datei angewendet, die diesem Verzeichnis hinzugefügt wird, aber nicht auf vorhandene Dateien. Jedes neue Unterverzeichnis, das Sie erstellen, erbt auch das neue Layout, das dann auf jede neue Datei oder jedes neue Verzeichnis angewendet wird, die bzw. das Sie in diesem Unterverzeichnis erstellen.

Verwenden Sie den `lfs migrate` Befehl , um das Layout einer vorhandenen Datei zu ändern. Dieser Befehl kopiert die Datei nach Bedarf, um ihren Inhalt entsprechend dem Layout zu verteilen,

das Sie im Befehl angeben. Beispielsweise ändern Dateien, die an angehängt oder vergrößert sind, die Anzahl der Stripes nicht, sodass Sie sie migrieren müssen, um das Dateilayout zu ändern. Alternativ können Sie eine neue Datei mit dem `lfs setstripe` Befehl erstellen, um ihr Layout anzugeben, den ursprünglichen Inhalt in die neue Datei kopieren und dann die neue Datei umbenennen, um die ursprüngliche Datei zu ersetzen.

Es kann Fälle geben, in denen die Standardlayoutkonfiguration für Ihren Workload nicht optimal ist. Beispielsweise kann ein Dateisystem mit Dutzenden von OSTs und einer großen Anzahl von Dateien mit mehreren Gigabyte eine höhere Leistung erzielen, indem die Dateien auf mehr als den Standardwert für die Anzahl von Stripes von fünf OSTs entfernt werden. Das Erstellen großer Dateien mit niedriger Stripe-Anzahl kann zu E/A-Leistungsengpässen führen und auch dazu führen, dass OSTs aufgefüllt werden. In diesem Fall können Sie ein Verzeichnis mit einer größeren Stripe-Anzahl für diese Dateien erstellen.

Das Einrichten eines Stripeset-Layouts für große Dateien (insbesondere Dateien, die größer als ein Gigabyte sind) ist aus den folgenden Gründen wichtig:

- Verbessert den Durchsatz, indem mehrere OSTs und die zugehörigen Server beim Lesen und Schreiben großer Dateien IOPS, Netzwerkbandbreite und CPU-Ressourcen beitragen können.
- Reduziert die Wahrscheinlichkeit, dass eine kleine Teilmenge von OSTs zu Hot Spots wird, die die allgemeine Workload-Leistung einschränken.
- Verhindert, dass eine einzelne große Datei ein OST füllt, was möglicherweise zu Fehlern bei vollem Datenträger führt.

Es gibt keine einzige optimale Layoutkonfiguration für alle Anwendungsfälle. Detaillierte Anleitungen zu Dateilayouts finden Sie unter Verwalten des Dateilayouts (Striping) und Freier Speicherplatz in der Dokumentation zu Lustre.org. Im Folgenden finden Sie allgemeine Richtlinien:

- Das Streifenlayout 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 eine Stripeset-Anzahl von fünf für Dateien mit einer Größe von mehr als 1GiB zu.
- Stripe count ist der Layoutparameter, den Sie für Systeme anpassen sollten, die große Dateien unterstützen. Die Stripe-Anzahl gibt die Anzahl der OST-Volumes an, die Blöcke einer Stripeset-Datei enthalten. Bei einer Stripe-Anzahl von 2 und einer Stripe-Größe von 1MiBschreibt Lustre beispielsweise alternative 1MiB-Blöcke einer Datei in jedes von zwei OSTs .

- Die effektive Stripe-Anzahl ist die geringere der tatsächlichen Anzahl von OST-Volumes und des von Ihnen angegebenen Stripe-Zählwerts. Sie können den speziellen Stripecount-Wert von verwenden, `-1` um anzugeben, dass Stripes auf allen OST-Volumes platziert werden sollen.
- Das Festlegen einer großen Stripe-Anzahl für kleine Dateien ist suboptimal, da Lustre für bestimmte Operationen einen Netzwerk-Roundtrip zu jedem OST im Layout erfordert, auch wenn die Datei zu klein ist, um Speicherplatz auf allen OST-Volumes zu belegen.
- Sie können ein progressives Dateilayout (PFL) einrichten, mit 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 Dateilayouts.
- Die Stripe-Größe beträgt standardmäßig 1MiB. Das Festlegen eines Stripe-Offsets kann unter besonderen Umständen benutzerfreundlich sein, aber im Allgemeinen empfiehlt es sich, ihn nicht anzugeben und den Standardwert zu verwenden.

Progressive Dateilayouts

Sie können eine progressive Dateilayout (PFL)-Konfiguration für ein Verzeichnis angeben, um verschiedene Stripe-Konfigurationen für kleine und große Dateien anzugeben, bevor Sie sie ausfüllen. Sie können beispielsweise einen PFL im 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
```

Dieser Befehl legt vier Layoutkomponenten fest:

- Die erste Komponente (`-E 100M -c 1`) gibt einen Stripe-Zählwert von 1 für Dateien mit einer Größe von bis zu 100MiB an.
- Die zweite Komponente (`-E 10G -c 8`) gibt eine Stripe-Anzahl von 8 für Dateien mit einer Größe von bis zu 10GiB an.
- Die dritte Komponente (`-E 100G -c 16`) gibt eine Stripe-Anzahl von 16 für Dateien mit einer Größe von bis zu 100GiB an.

- Die vierte Komponente (`-E -1 -c 32`) gibt eine Stripe-Anzahl von 32 für Dateien an, die größer als 100GiB.

> **Important**
>
> Das Anhängen von Daten an eine Datei, die mit einem PFL-Layout erstellt wurde, füllt alle ihre Layoutkomponenten aus. Wenn Sie beispielsweise mit dem oben gezeigten Befehl mit 4 Komponenten eine 1MiB-Datei erstellen und dann Daten am Ende hinzufügen, wird das Layout der Datei erweitert, sodass es eine Stripe-Anzahl von -1 hat, was alle OSTs im System bedeutet. Dies bedeutet nicht, dass Daten in jedes OST geschrieben werden, aber eine Operation wie das Lesen der Dateilänge sendet eine Anforderung parallel an jedes OST, wodurch eine erhebliche Netzwerklast zum Dateisystem hinzugefügt wird.
> Achten Sie daher darauf, die Anzahl der Stripes für kleine oder mittelgroße Dateien zu begrenzen, an die anschließend Daten angehängt werden können. Da Protokolldateien normalerweise durch das Anhängen neuer Datensätze wachsen, weist Amazon FSx for Lustre jeder Datei, die im Anhängemodus erstellt wurde, eine Standard-Stripe-Anzahl von 1 zu, unabhängig von der Standard-Stripe-Konfiguration, die durch das übergeordnete Verzeichnis angegeben wird.

Die PFL-Standardkonfiguration auf Amazon-FSx-für-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 einen sehr gleichzeitigen Zugriff auf mittlere und große Dateien haben, profitieren wahrscheinlich von einem Layout mit mehr Stripes in kleineren Größen und dem Entfernen über alle OSTs für die größten Dateien, wie im vierteiligen Beispiellayout gezeigt.

Überwachen von Leistung und Nutzung

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

Um Details zur aggregierten Dateisystemnutzung anzuzeigen, können Sie sich die Summenstatistik jeder Metrik ansehen. Beispielsweise meldet die Summe der `DataReadBytes` Statistik den

gesamten Lesedurchsatz, der von allen OSTs in einem Dateisystem angezeigt wird. In ähnlicher Weise meldet die Summe der `FreeDataStorageCapacity` Statistik die gesamte verfügbare Speicherkapazität für Dateidaten im Dateisystem.

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 für Lustre die folgenden Leistungstipps. Informationen zu Service-Limits finden Sie unter Kontingente.

- Durchschnittliche E/A-Größe – Da es sich bei Amazon FSx for Lustre um ein Netzwerkdateisystem handelt, durchläuft jeder Dateivorgang einen Umlauf zwischen dem Client und Amazon FSx for Lustre, was zu einem geringen Latenzaufwand führt. 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-Instance gepuffert, 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, gibt synchrone Anfragen an Amazon FSx for Lustre aus. Jede Operation durchläuft einen Umlauf zwischen dem Client und Amazon FSx for Lustre.

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

- Amazon EC2-Instances – Anwendungen, die eine große Anzahl von Lese- und Schreibvorgängen ausführen, benötigen wahrscheinlich mehr Arbeitsspeicher oder Rechenkapazität als Anwendungen, die dies nicht tun. Wählen Sie beim Starten Ihrer Amazon EC2-Instances für Ihre rechenintensive Workload Instance-Typen aus, die über die Menge dieser Ressourcen verfügen, die Ihre Anwendung benötigt. Die Leistungsmerkmale von Dateisystemen von Amazon FSx für Lustre hängen nicht von der Verwendung von Amazon-EBS-optimierten Instances ab.
- Empfohlene Client-Instance-Optimierung für optimale Leistung

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

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

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

   ```
   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 anzuwenden:

   ```
   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
   ```

   Nachdem der Client gemountet wurde, muss die folgende Optimierung angewendet 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` bekanntermaßen während des Neustarts nicht bestehen bleibt. Da diese Parameter clientseitig nicht dauerhaft festgelegt werden können, wird empfohlen, einen Boot-Cron-Auftrag zu implementieren, um die Konfiguration mit den empfohlenen Optimierungen festzulegen.

- Workload-Balance über OSTs hinweg – In einigen Fällen verursacht Ihr Workload nicht den Gesamtdurchsatz, den Ihr Dateisystem bereitstellen kann (200 MB/s pro TiB Speicher). In diesem Fall können Sie CloudWatch Metriken verwenden, um Fehler zu beheben, wenn die Leistung durch ein Ungleichgewicht der E/A-Muster Ihrer Workload beeinträchtigt wird. Um festzustellen, ob dies die Ursache ist, sehen Sie sich die CloudWatch Metrik Maximum für Amazon FSx for Lustre an.

  In einigen Fällen zeigt diese Statistik eine Last mit oder über 240 MBpss Durchsatz (die Durchsatzkapazität einer einzelnen 1,2 TiB Amazon FSx for Lustre-Festplatte). In solchen Fällen ist Ihr Workload nicht gleichmäßig auf Ihre Datenträger verteilt. In diesem Fall können Sie den `lfs`

`setstripe` Befehl verwenden, um das Entfernen von Dateien zu ändern, auf die Ihr Workload am häufigsten zugreift. Um eine optimale Leistung zu erzielen, sollten Sie Dateien mit hohen Durchsatzanforderungen über alle OSTs umgeben, hinweg aufteilen.

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

Angenommen, Ihr Workload verwendet ein 7,0-TiB-Dateisystem (das aus 6x 1,17-TiB-OSTs besteht) und muss einen hohen Durchsatz über 2,4-GiB-Dateien hinweg erreichen. In diesem Fall können Sie den `ImportedFileChunkSize` Wert auf setzen, `(2.4 GiB / 6 OSTs) = 400 MiB` sodass Ihre Dateien gleichmäßig auf die OSTs Ihres Dateisystems verteilt werden.

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 Datei`fstab` 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

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

Betriebssystem	Betriebssystemversion	Minimale Kernelversion	Maximale Kernelversion	Version des Dateisystems		
Ubuntu	22	6.2.0.1017.17~22,04	6.2.0. *	Nein	Ja	Ja
		5.15.0-1015-aws	5.15.0-1031-aws	Ja	Ja	Ja
	20	5.15.0-1015-aws	5,15,0 +	Ja	Ja	Ja
		5.4.0-1011-aws	5.13.0-1031-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/CentOS/Rocky Linux	9.3	Arm + x86	5,14,0-362,18,1	5,14,0-362,18,1	Nein	Ja	Ja
	9.0	Arm + x86	5,14,0-70,13,1	5,14,0-70,30,1	Nein	Ja	Ja
	8,9	Arm + x86	4,18,0-513*	4,18,0-513*	Ja	Ja	Ja

Betriebssystem	Betriebssystemversion	Architektur	Minimale Kernelversion	Maximale Kernelversion	Version des Dateisystems		
	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
	7.8	Arm	4,18,0-147*	4,18,0-147*	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 unterKompatibilität 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 weniger als zurückgibt`4.14.104-78.84.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 oder 9.3 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`5.14.0-362*`, müssen Sie die Repository-Konfiguration nicht ändern. Fahren Sie mit dem Verfahren So installieren Sie den Lustre-Client fort.
   - Wenn der Befehl zurückkehrt`5.14.0-70*`, 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 9.0 zu verweisen, *specific_RHEL_version* ersetzen `9.0` Sie den Befehl durch, wie im folgenden Beispiel.

   ```
   sudo sed -i 's#9#9.0#' /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 `7.8` den 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 unterInformationen 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 unterInformationen 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 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 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 unterInformationen 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 --gpgcheck-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 --gpgcheck-strict fsx-lustre-client.repo
     sudo sed -i 's#SLES-12#SP4#' /etc/zypp/repos.d/aws-fsx.repo
     sudo zypper refresh
     sudo zypper in lustre-client
     ```

   - 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 --gpgcheck-strict fsx-lustre-client.repo
     sudo sed -i 's#SP3#SP4#' /etc/zypp/repos.d/aws-fsx.repo
     sudo zypper ref
     sudo zypper up --force-resolution lustre-client-kmp-default
     ```

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 --gpgcheck-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-Instanz

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 Einhängepunkt.

   ```
   $ 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 es 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 DescribeFileSystemsAPI-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 über einen Docker-Container von Amazon Elastic Container Service (Amazon ECS) auf einer Amazon EC2 EC2-Instance auf Ihr FSx for Lustre-Dateisystem 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 es durch den Mount-Namen des Dateisystems.
- *mountpoint*Ersetzen Sie ihn durch den Einhängepunkt 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 Einhängepunkt 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 es 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` Fähigkeit 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	• 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 es 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 Das automatische Mounten schlägt fehl und die Instanz 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
file_system_dns_name `@tcp:/`	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
mountname	Der Mount-Name für das Dateisystem. Sie können diesen Namen von der Konsole oder programmgesteuert AWS CLI mithilfe des describe-

Feld	Beschreibung
	file-systems Befehls oder der AWS API oder des SDK mithilfe des DescribeFileSystems Vorgangs abrufen.
/fsx	Der Bereitstellungspunkt für das Amazon FSx-Dateisystem auf Ihrer EC2-Instance.
lustre	Der Typ des Dateisystems, Amazon FSx.
mount options	Einhängeoptionen für das Dateisystem, dargestellt als kommagetr ennte Liste der folgenden Optionen: • defaults— Dieser Wert weist das Betriebssystem an, die Standard-Einhängeoptionen zu verwenden. Sie können die Standard-Einhängeoptionen auflisten, nachdem das Dateisystem bereitgestellt wurde, indem Sie sich die Ausgabe des mount Befehls ansehen. • relatime— Diese Option verwaltet Daten atime (Inode-Zugriffszei ten), jedoch nicht für jeden Dateizugriff. Wenn diese Option aktiviert ist, atime werden Daten nur dann auf die Festplatte geschrieben, wenn die Datei seit der letzten Aktualisierung der atime Daten geändert wurde (mtime) oder wenn vor mehr als einer bestimmte n Zeit (standardmäßig ein Tag) zuletzt auf die Datei zugegriffen wurde. Wenn Sie Aktualisierungen der Inode-Zugriffszeit deaktivie ren möchten, verwenden Sie stattdessen die noatime Mount-Opt ion. • flock— hängt Ihr Dateisystem mit aktivierter Dateisperre ein. Wenn Sie nicht möchten, dass die Dateisperre aktiviert ist, verwenden Sie stattdessen die noflock Mount-Option. • _netdev— Der Wert teilt dem Betriebssystem mit, dass sich das Dateisystem auf einem Gerät befindet, das Netzwerkzugriff benötigt. Diese Option verhindert, dass die Instance das Dateisyst em mountet, bis das Netzwerk auf dem Client aktiviert wurde.

Feld	Beschreibung
`x-systemd.automount,x-systemd.requires=network.service`	Diese Optionen stellen sicher, dass der Auto Mounter nicht läuft, bis die Netzwerkverbindung online ist. **Note** Verwenden Sie für Ubuntu 22.04 die `x-systemd.requires=systemd-networkd-wait-online.service` Option anstelle der `x-systemd.requires=network.service` Option.
`0`	Ein Wert, der angibt, ob das Dateisystem von dump gesichert werden soll. Für Amazon FSx sollte dieser Wert sein. `0`
`0`	Ein Wert, der die Reihenfolge angibt, in der Dateisysteme beim Booten `fsck` überprüft werden. Für Amazon FSx-Dateisysteme sollte dieser Wert angeben, dass `0` sie beim Start nicht ausgeführt werden `fsck` sollen.

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 es 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 DescribeFileSystemsAPI-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 Einhängepunkt 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 Datenträgernutzungsstatistiken 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 nicht bereitgestellt wurde.

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 dazu finden Sie unter Spot-Instances im Amazon-EC2-Benutzerhandbuch für Linux-Instances.

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 Kündigungsmitteilungen 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 Kündigungsmitteilungen von Spot.
- Wenn es eine Kündigungsmitteilung 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 "${FSXPATH}"; then
        echo "Error unmouting '$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

Mit Amazon FSx for Lustre können Sie automatische tägliche Backups und vom Benutzer initiierte Backups persistenter Dateisysteme erstellen, die nicht mit einem dauerhaften Amazon S3-Daten-Repository verknüpft sind. Amazon-FSx-Backups sind file-system-consistent, sehr beständig und inkrementell. Um eine hohe Haltbarkeit zu gewährleisten, speichert Amazon FSx for Lustre Backups in Amazon Simple Storage Service (Amazon S3) mit einer Haltbarkeit von 99,999999999 % (99 %).

FSx-for-Lustre-Dateisystem-Backups sind blockbasierte, inkrementelle Backups, unabhängig davon, ob sie mit dem automatischen täglichen Backup oder der vom Benutzer initiierten Backup-Funktion generiert werden. Das bedeutet, dass Amazon FSx beim Erstellen einer Sicherung die Daten auf Ihrem Dateisystem mit Ihrer vorherigen Sicherung auf Blockebene vergleicht. Anschließend speichert

Amazon FSx eine Kopie aller Änderungen auf Blockebene im neuen Backup. Daten auf Blockebene, die unverändert bleiben, seit das vorherige Backup nicht im neuen Backup gespeichert wurde. Die Dauer des Backup-Vorgangs hängt davon ab, wie viele Daten sich seit der letzten Backup-Erstellung geändert haben, und ist unabhängig von der Speicherkapazität des Dateisystems. Die folgende Liste veranschaulicht die Backup-Zeiten unter verschiedenen Umständen:

- Die erste Sicherung eines völlig neuen Dateisystems mit sehr wenigen Daten dauert Minuten.
- Die erste Sicherung eines völlig neuen Dateisystems nach dem Laden von TBs an Daten dauert Stunden.
- Eine zweite Sicherung des Dateisystems mit TBs an Daten mit minimalen Änderungen an 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 ein Backup löschen, werden nur die für dieses Backup eindeutigen Daten entfernt. Jedes FSx-für-Lustre-Backup enthält alle Informationen, die zum Erstellen eines neuen Dateisystems aus dem Backup erforderlich sind, 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 unterstützen Ihre Anforderungen an die Aufbewahrung und Compliance von Backups. Das Arbeiten mit Backups von Amazon FSx für Lustre ist einfach, unabhängig davon, ob es sich um das Erstellen von Backups, das Kopieren eines Backups, das Wiederherstellen eines Dateisystems aus einem Backup oder das Löschen eines Backups handelt.

Backups werden auf Scratch-Dateisystemen nicht unterstützt, da diese Dateisysteme für die temporäre Speicherung und kürzere Verarbeitung von Daten konzipiert sind. Backups werden auf Dateisystemen, die mit einem Amazon S3-Bucket verknüpft sind, nicht unterstützt, da der S3-Bucket als primäres Daten-Repository dient und das Lustre-Dateisystem nicht unbedingt den vollständigen Datensatz zu einem bestimmten Zeitpunkt enthält.

Themen

- Verwenden von AWS Backup mit Amazon FSx
- Kopieren eines Backups
- Kopieren von Backups innerhalb derselben AWS-Konto
- Wiederherstellen von Sicherungen
- Löschen eines Backups

Backup-Unterstützung in FSx für Lustre

Backups werden nur auf persistenten FSx-für-Lustre-Dateisystemen unterstützt, die nicht mit einem Amazon S3-Daten-Repository verknüpft sind.

Amazon FSx unterstützt keine Backups auf Scratch-Dateisystemen, da Scratch-Dateisysteme für die temporäre Speicherung und kürzere Verarbeitung von Daten konzipiert sind. Amazon FSx unterstützt keine Backups auf Dateisystemen, die mit einem Amazon S3-Bucket verknüpft sind, da der S3-Bucket als primäres Daten-Repository dient und das Dateisystem nicht unbedingt den vollständigen Datensatz zu einem bestimmten Zeitpunkt enthält. Weitere Informationen finden Sie unter Optionen für die Bereitstellung des Dateisystems und Verwenden von Datenrepositorys.

Arbeiten mit automatischen täglichen Backups

Amazon FSx for Lustre kann eine automatische tägliche Sicherung Ihres Dateisystems erstellen. Diese automatischen täglichen Backups erfolgen während des täglichen Backup-Fensters, das beim Erstellen des Dateisystems eingerichtet wurde. Irgendwann während des täglichen Backup-Fensters kann die Speicher-I/O während der Initialisierung des Backup-Vorgangs kurzzeitig unterbrochen werden (in der Regel weniger als einige Sekunden). Wenn Sie Ihr tägliches Backup-Fenster wählen, empfehlen wir Ihnen, eine bequeme Uhrzeit auszuwählen. Diese Zeit liegt idealerweise außerhalb der normalen Betriebszeiten für die Anwendungen, die das Dateisystem verwenden.

Automatische tägliche Backups werden für einen bestimmten Zeitraum aufbewahrt, der als Aufbewahrungszeitraum bezeichnet wird. Sie können den Aufbewahrungszeitraum auf einen Wert zwischen 0 und 90 Tagen festlegen. Wenn Sie den Aufbewahrungszeitraum auf 0 (Null) Tage festlegen, werden automatische tägliche Backups deaktiviert. Der Standardaufbewahrungszeitraum für automatische tägliche Backups beträgt 0 Tage. Automatische tägliche Backups werden gelöscht, wenn das Dateisystem gelöscht wird.

> **Note**
>
> Wenn Sie den Aufbewahrungszeitraum auf 0 Tage festlegen, wird Ihr Dateisystem nie automatisch gesichert. Wir empfehlen dringend, automatische tägliche Backups für Dateisysteme zu verwenden, denen eine beliebige kritische Funktionalität zugeordnet ist.

Sie können die 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 über die Amazon-FSx-for-Lustre-Konsole, die API oder die AWS Command Line Interface (CLI) tun. Ihre vom Benutzer initiierten Backups von Amazon-FSx-Dateisystemen laufen nie ab und sind so lange verfügbar, wie Sie sie behalten möchten. Vom Benutzer initiierte Backups werden auch nach dem Löschen des gesicherten Dateisystems aufbewahrt. Sie können vom Benutzer initiierte Backups nur mithilfe der Amazon-FSx-for-Lustre-Konsole, API oder CLI löschen und sie werden niemals automatisch von Amazon FSx gelöscht. Weitere Informationen finden Sie unter Löschen eines Backups.

Erstellen von vom Benutzer initiierten Backups

Das folgende Verfahren führt Sie durch die Erstellung eines vom Benutzer initiierten Backups in der Amazon-FSx-Konsole für ein vorhandenes Dateisystem.

So erstellen Sie ein vom Benutzer initiiertes Dateisystem-Backup

1. Öffnen Sie die Konsole von Amazon FSx für Lustre unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Dashboard der Konsole 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 dürfen 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 all Ihrer Backups in der Konsole von Amazon FSx für Lustre, indem Sie in der linken Navigation Backups auswählen. Sie können nach dem Namen suchen, den Sie Ihrem Backup gegeben haben, und die Tabellenfilter zeigen nur übereinstimmende Ergebnisse an.

Wenn Sie wie in diesem Verfahren beschrieben ein vom Benutzer initiiertes Backup erstellen, hat es den Typ und den Status Wird erstelltUSER_INITIATED, während Amazon FSx das Backup erstellt. Der Status ändert sich in Übertragen, während das Backup an Amazon S3 übertragen wird, bis es vollständig verfügbar ist.

Verwenden von 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 die Erstellung vereinfachen soll. Kopieren, Wiederherstellung, und Löschen von Backups, bietet gleichzeitig verbesserte Berichte und Prüfungen. AWS Backup erleichtert die Entwicklung einer zentralen Backup-Strategie für die Rechtswissenschaft. regulatorische, und Professional Compliance. AWS Backup macht auch den Schutz Ihrer AWS Speicher-Volumes, -Datenbanken, - und -Dateisysteme erleichtern die Bereitstellung eines zentralen Orts, an dem Sie Folgendes tun können:

- Konfigurieren und Prüfen der zu sichernden AWS-Ressourcen.
- Automatisieren geplanter Sicherungen
- Festlegen von Aufbewahrungsrichtlinien
- Kopieren Sie Backups regions- AWS und AWSkontenübergreifend.
- Überwachen der letzten Sicherungs- und Wiederherstellungsaktivitäten

AWS Backup verwendet die integrierte Backup-Funktionalität von Amazon FSx . Von der AWS Backup Konsole erstellte Backups haben das gleiche Maß an Dateisystemkonsistenz und -leistung und dieselben Wiederherstellungsoptionen wie Backups, die über die Amazon-FSx-Konsole erstellt werden. Wenn Sie verwenden, AWS Backup um diese Backups zu verwalten, erhalten Sie zusätzliche Funktionen, z. B. unbegrenzte Aufbewahrungsoptionen und die Möglichkeit, geplante Backups so oft wie jede Stunde zu erstellen. Darüber hinaus AWS Backup behält Ihre unveränderlichen Backups auch nach dem Löschen des Quelldateisystems bei. Dies trägt zum Schutz vor versehentlichem oder böswilligem Löschen bei.

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 von AWS Backup in der Amazon-FSx-Konsole, CLI und API anzeigen und wiederherstellen. Von erstellte Backups AWS Backup haben den Backup-Typ `AWS_BACKUP`. Sie können die von erstellten Backups jedoch nicht AWS Backup in der Amazon-FSx-Konsole, CLI oder API löschen. Weitere Informationen zur Verwendung von AWS Backup zum Sichern 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 (regionsübergreifende Kopien) zu kopieren. Sie können regionsübergreifende Kopien nur innerhalb derselben AWS Partition erstellen. Sie können vom Benutzer initiierte Sicherungskopien mithilfe der Amazon-FSx-Konsole, AWS CLIder oder der API erstellen. Wenn Sie eine vom Benutzer initiierte Sicherungskopie erstellen, hat sie den Typ `USER_INITIATED`.

Sie können auch verwendenAWS Backup, um Backups über AWS Regionen und AWS Konten hinweg zu kopieren. AWS Backup ist ein vollständig verwalteter Backup-Management-Service, der eine zentrale Schnittstelle für richtlinienbasierte Backup-Pläne bietet. Mit der kontoübergreifenden Verwaltung können Sie automatisch Backup-Richtlinien verwenden, um Backup-Pläne auf die Konten in Ihrer Organisation anzuwenden.

Regionsübergreifende Backup-Kopien sind besonders nützlich für die regionsübergreifende Notfallwiederherstellung. Sie erstellen Backups und kopieren sie in eine andere AWS Region, sodass Sie im Notfall in der primären AWS Region 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 -AWSKontos (regionsübergreifend oder regionsübergreifend), indem Sie die Amazon-FSx-Konsole, AWS CLIoder die Amazon-FSx-for-Lustre-API verwenden. Sie können auch verwenden, AWS Backup um Sicherungskopien durchzuführen, entweder auf Abruf oder richtlinienbasiert.

Kontoübergreifende Backup-Kopien sind nützlich, um Ihre gesetzlichen Compliance-Anforderungen zu erfüllen und Backups auf ein isoliertes Konto zu kopieren. Sie bieten auch eine zusätzliche Datenschutzebene, um versehentliches oder böswilliges Löschen von Backups, den Verlust von Anmeldeinformationen oder die Kompromittierung von AWS KMS Schlüsseln zu verhindern. Kontoübergreifende Backups unterstützen Fan-In (Kopieren von Backups aus mehreren

Primärkonten in ein isoliertes Backup-Kopierkonto) und Fan-Out (Kopieren von Backups aus einem Primärkonto in mehrere isolierte Backup-Kopierkonten).

Sie können kontoübergreifende Backup-Kopien erstellen, indem Sie AWS Backup mit -AWS OrganizationsUnterstützung verwenden. Kontogrenzen für kontoübergreifende Kopien werden durch AWS Organizations Richtlinien definiert. Weitere Informationen zur Verwendung von AWS Backup zum Erstellen von kontoübergreifenden Sicherungskopien finden Sie unter Erstellen von Sicherungskopien über AWS-Konten hinweg im AWS Backup -Entwicklerhandbuch.

Einschränkungen bei Backup-Kopien

Die folgenden Einschränkungen gelten beim Kopieren von Backups:

- Regionsübergreifende Backup-Kopien werden nur zwischen zwei kommerziellen AWS-Regionen, zwischen den Regionen China (Peking) und China (Ningxia) und zwischen den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (USA-West) unterstützt, jedoch nicht über diese Regionen.
- Regionsübergreifende Backup-Kopien werden in Opt-in-Regionen nicht unterstützt.
- Sie können regionsinterne Backup-Kopien in jeder -AWSRegion erstellen.
- Das Quell-Backup muss den Status haben, `AVAILABLE` bevor Sie es kopieren können.
- Sie können eine Quellsicherung nicht löschen, wenn sie kopiert wird. Es kann eine kurze Verzögerung zwischen dem Zeitpunkt geben, an dem das Ziel-Backup verfügbar ist, und dem Zeitpunkt, an dem Sie das Quell-Backup löschen dürfen. Sie sollten diese Verzögerung berücksichtigen, wenn Sie erneut versuchen, ein Quell-Backup zu löschen.
- Sie können pro Konto bis zu fünf Backup-Kopieranforderungen an eine einzelne AWS Zielregion ausführen.

Berechtigungen für regionsübergreifende Backup-Kopien

Sie verwenden eine IAM-Richtlinienanweisung, um Berechtigungen zum Ausführen eines Sicherungskopiervorgangs zu erteilen. Um mit der AWS Quellregion zu kommunizieren, um eine regionsübergreifende Sicherungskopie anzufordern, muss der Anforderer (IAM-Rolle oder IAM-Benutzer) Zugriff auf die Quellsicherung und die AWS Quellregion haben.

Sie verwenden die -Richtlinie, um Berechtigungen für die -`CopyBackup`Aktion für den Backup-Kopiervorgang zu erteilen. Sie geben die Aktion im `Action` Feld der Richtlinie und 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 eine Sicherung in eine andere AWS-Region als die Quellsicherung kopieren, ist die erste Kopie eine vollständige Sicherungskopie. Nach der ersten Sicherungskopie sind alle nachfolgenden Sicherungskopien in dieselbe Zielregion innerhalb desselben AWS Kontos inkrementell, vorausgesetzt, Sie haben nicht alle zuvor kopierten Sicherungen in dieser Region gelöscht und denselben AWS KMS Schlüssel verwendet. Wenn beide Bedingungen nicht erfüllt sind, führt der Kopiervorgang zu einer vollständigen (nicht inkrementellen) Sicherungskopie.

Kopieren von Backups innerhalb derselben AWS-Konto

Sie können Backups von FSx-für-Lustre-Dateisystemen mit der AWS Management Console, CLI und API kopieren, wie in den folgenden Verfahren beschrieben.

So kopieren Sie ein Backup innerhalb desselben Kontos (regionsübergreifend oder regionsübergreifend) mithilfe der Konsole

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 die Sicherung kopiert werden soll. Das Ziel kann sich in einer anderen AWS Region (regionsübergreifende Kopie) oder innerhalb derselben AWS Region (regionsübergreifende Kopie) befinden.
- (Optional) Wählen Sie Tags kopieren aus, um Tags aus der Quellsicherung in die Zielsicherung zu kopieren. Wenn Sie in Schritt 6 Tags kopieren auswählen und auch Tags hinzufügen, werden alle Tags zusammengeführt.

5. Wählen Sie für Verschlüsselung den AWS KMSVerschlüsselungsschlüssel aus, um das kopierte Backup zu verschlüsseln.
6. Geben Sie für Tags – optional einen Schlüssel und einen Wert ein, um Tags für Ihre kopierte Sicherung 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 derselben AWS-Konto in die ausgewählte kopiertAWS-Region.

So kopieren Sie ein Backup innerhalb desselben Kontos (regionsübergreifend oder regionsübergreifend) mithilfe der CLI

- Verwenden Sie den `copy-backup` CLI-Befehl oder die CopyBackup API-Operation , um ein Backup innerhalb desselben AWS Kontos zu kopieren, entweder über eine -AWSRegion oder innerhalb einer -AWSRegion.

  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 zeigt die Beschreibung der kopierten Sicherung.

  Sie können Ihre Backups auf der Amazon-FSx-Konsole oder programmgesteuert mit dem `describe-backups` CLI-Befehl oder der DescribeBackups API-Operation anzeigen.

Wiederherstellen von Sicherungen

Sie können ein verfügbares Backup verwenden, um ein neues Dateisystem zu erstellen, wodurch effektiv ein point-in-time Snapshot eines anderen Dateisystems wiederhergestellt wird. Sie können ein Backup mithilfe der Konsole, AWS CLIoder eines der AWS -SDKs wiederherstellen. Das Wiederherstellen eines Backups in einem neuen Dateisystem dauert genauso lange wie das Erstellen eines neuen Dateisystems. Die aus dem Backup wiederhergestellten Daten werden fazy-geladen in das Dateisystem. 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 in einem Dateisystem wiederherstellen, das denselben Lustre-Versionstyp, Bereitstellungstyp, Durchsatz pro Speichereinheit, Speicherkapazität, Datenkomprimierungstyp und AWS Region wie das Original hat. Sie können die Speicherkapazität Ihres wiederhergestellten Dateisystems erhöhen, sobald es verfügbar ist. Weitere Informationen finden Sie unter Verwalten der Speicherkapazität.

So stellen Sie ein Dateisystem aus einem Backup wieder her

1. Öffnen Sie die Konsole von Amazon FSx für Lustre unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Dashboard der Konsole in der linken Navigationsleiste die Option 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 Dateisystem-Erstellungsassistent geöffnet. Dieser Assistent ist identisch mit dem standardmäßigen Assistenten zur Erstellung des Dateisystems, mit Ausnahme der Dateisystemkonfiguration (z. B. Bereitstellungstyp, Durchsatz pro Speichereinheit). Sie können jedoch die zugehörigen VPC- und Backup-Einstellungen ändern.
4. Schließen Sie den Assistenten wie beim Erstellen eines neuen Dateisystems ab.
5. Wählen Sie Review and create.
6. Überprüfen Sie die Einstellungen, die Sie für Ihr Dateisystem von Amazon FSx für Lustre ausgewählt haben, und wählen Sie dann Dateisystem erstellen aus.

Sie haben aus einem Backup wiederhergestellt und jetzt wird ein neues Dateisystem erstellt. Wenn sich der Status in ändert`AVAILABLE`, 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 ein Backup nur, wenn Sie sicher sind, dass Sie dieses Backup in Zukunft nicht mehr benötigen. Sie können keine Backups löschen, die von AWS Backup in der Amazon-FSx-Konsole, CLI oder API erstellt wurden.

So löschen Sie ein Backup

1. Öffnen Sie die Konsole von Amazon FSx für Lustre unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Dashboard der Konsole in der linken Navigation die Option Backups aus.
3. Wählen Sie das Backup, das Sie löschen möchten, aus der Tabelle Backups und 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 aktiviert ist, das Sie löschen möchten.
6. Wählen Sie Backups löschen aus.

Ihr Backup und alle enthaltenen Daten werden jetzt dauerhaft und nicht wiederherstellbar 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 einschränken, die ein Benutzer, eine Gruppe oder ein Projekt verbrauchen kann. 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 erzwingt Kontingente und verhindert, dass Benutzer, die sie überschritten haben, in den Speicherplatz schreiben. Wenn Benutzer ihre Kontingente überschreiten, müssen sie genügend Dateien löschen, um die Kontingentlimits zu erreichen, damit sie erneut in das Dateisystem schreiben können.

Themen

Durchsetzung von Kontingenten

Die Durchsetzung von Benutzer-, Gruppen- und Projektkontingenten wird auf allen Dateisystemen von FSx für Lustre automatisch aktiviert. Sie können die Kontingenterzwingung nicht deaktivieren.

Arten von Kontingenten

Systemadministratoren mit Root-Benutzer-Anmeldeinformationen des - AWS Kontos können die folgenden Kontingenttypen 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 auf Lustre-Version 2.15 auf FSx-für-Lustre-Dateisystemen unterstützt.

- Ein Blockkontingent begrenzt den Speicherplatz, den ein Benutzer, eine Gruppe oder ein Projekt verbrauchen 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 Knoten 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. Sie wird auch durch beide Kontingente begrenzt. Wenn eines der Kontingente erreicht ist, 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 mit dem `sudo` Befehl die Durchsetzung des Kontingents.

Kontingentlimits und Übergangsfristen

Amazon FSx erzwingt Benutzer-, Gruppen- und Projektkontingente als hartes Limit oder als weiches Limit mit einer konfigurierbaren Übergangsfrist.

Das harte Limit ist das absolute Limit. Wenn Benutzer ihr hartes Limit überschreiten, schlägt eine Block- oder Inode-Zuweisung mit einer Meldung fehl, dass das Festplattenkontingent überschritten wurde. Benutzer, die ihr hartes Kontingentlimit erreicht haben, müssen genügend Dateien oder Verzeichnisse löschen, um das Kontingentlimit zu erreichen, bevor sie erneut in das Dateisystem schreiben können. Wenn eine Übergangsfrist festgelegt ist, können Benutzer das weiche Limit innerhalb der Übergangsfrist überschreiten, wenn es unter dem harten Limit liegt.

Für weiche Limits konfigurieren Sie eine Übergangsfrist in Sekunden. Das weiche Limit muss kleiner als das harte Limit sein.

Sie können verschiedene Übergangszeiträume für Inode- und Blockkontingente festlegen. Sie können auch unterschiedliche Übergangsfristen für ein Benutzerkontingent, ein Gruppenkontingent und ein Projektkontingent festlegen. Wenn Benutzer-, Gruppen- und Projektkontingente unterschiedliche Übergangsfristen haben, wird das weiche Limit nach Ablauf der Übergangsfrist eines dieser Kontingente in ein hartes Limit umgewandelt.

Wenn Benutzer ein weiches Limit überschreiten, ermöglicht Amazon FSx ihnen, ihr Kontingent so lange weiter zu überschreiten, bis die Übergangsfrist abgelaufen ist oder bis das harte Limit erreicht ist. Nach Ablauf der Übergangsfrist wird das weiche Limit in ein hartes Limit konvertiert, und Benutzer werden von allen weiteren Schreibvorgängen blockiert, bis ihre Speichernutzung unter das definierte Blockkontingent oder die Kontingentgrenzen für Inodes zurückkehrt. Benutzer erhalten keine Benachrichtigung oder Warnung, wenn die Übergangsfrist beginnt.

Festlegen und Anzeigen von Kontingenten

Sie legen Speicherkontingente mithilfe von Lustre-`lfs`Dateisystembefehlen in Ihrem Linux-Terminal fest. Der `lfs setquota` Befehl legt Kontingentlimits fest und der `lfs quota` Befehl zeigt Kontingentinformationen an.

Weitere Informationen zu Lustre-Kontingentbefehlen finden Sie im Lustre-Betriebshandbuch auf der Lustre-Dokumentationswebsite.

Festlegen 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.
- `-b` legt ein Blockkontingent mit einem Soft Limit fest. `-B` legt ein Blockkontingent mit einem Hard Limit fest. Sowohl *`block_softlimit`* als auch *`block_hardlimit`* werden in Kilobyte ausgedrückt und der Mindestwert beträgt 1024 KB.
- `-i` legt ein Inode-Kontingent mit einem Soft-Limit fest. `-I` legt ein Inode-Kontingent mit einem Hard-Limit fest. Sowohl *`inode_softlimit`* als auch *`inode_hardlimit`* werden in der Anzahl der Inodes ausgedrückt, und der Mindestwert beträgt 1024 Inodes.
- *`mount_point`* ist das Verzeichnis, in dem das Dateisystem gemountet wurde.

Beispiel für ein Benutzerkontingent: Der folgende Befehl legt ein Limit von 5 000 KB für Soft Blocks, ein Hard-Block-Limit von 8 000 KB, ein Soft-Inode-Limit von 2 000 und ein Hard-Inode-Limit-Kontingent von 3 000 für `user1` auf dem Dateisystem fest, das in gemountet ist`/mnt/fsx`.

```
sudo lfs setquota -u user1 -b 5000 -B 8000 -i 2000 -I 3000 /mnt/fsx
```

Beispiel für ein Gruppenkontingent: Der folgende Befehl legt ein hartes Blocklimit von 100.000 KB für die Gruppe mit dem Namen `group1` auf dem Dateisystem fest, das in gemountet ist`/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 dem Projekt die gewünschten Dateien und Verzeichnisse 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. Der folgende Befehl legt ein Limit von 307.200 KB für Soft Blocks, ein Hard Block-Limit von 309.200 KB, ein Limit von 10.000 Soft Inodes und ein Limit von 11.000 Hard Inodes für das Projekt `250` auf dem Dateisystem fest, das in gemountet ist`/mnt/fsx`.

```
sudo lfs setquota -p 250 -b 307200 -B 309200 -i 10000 -I 11000 /mnt/fsx
```

Festlegen von Kulanzzeiträumen

Die standardmäßige Übergangsfrist beträgt eine Woche. Sie können die standardmäßige Übergangsfrist 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 eine Übergangsfrist 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. block*_grace* und *inode_grace* werden in ganzen Sekunden oder im `XXwXXdXXhXXmXXs` Format ausgedrückt.
- *mount_point* ist das Verzeichnis, in dem das Dateisystem gemountet wurde.

Der folgende Befehl legt Übergangsfristen von 1 000 Sekunden für Benutzerblockkontingente und 1 Woche und 4 Tage für Benutzerknotenkontingente fest.

```
sudo lfs setquota -t -u -b 1000 -i 1w4d /mnt/fsx
```

Anzeigen von Kontingenten

Der `quota` Befehl zeigt Informationen zu Benutzerkontingenten, Gruppenkontingenten, Projektkontingenten und Übergangszeiträumen an.

Anzeigen des Kontingentbefehls	Angezeigte Kontingentinformationen
`lfs quota /`*mount_point*	Allgemeine Kontingentinformationen (Festplattennutzung und -limits) für den Benutzer, der den Befehl ausführt, und die Primärgruppe des Benutzers.
`lfs quota -u` *username* `/`*mount_point*	Allgemeine Kontingentinformationen für einen bestimmten Benutzer. Benutzer mit Root-Benutzer-Anmeldeinformationen des - AWS Kontos können diesen Befehl für jeden Benutzer ausführen, Nicht-Root-Benutzer können diesen Befehl jedoch nicht ausführen, um Kontingen

Anzeigen des Kontingentbefehls	Angezeigte Kontingentinformationen
	tinformationen über andere Benutzer abzurufen.
`lfs quota -u username -v /mount_point`	Allgemeine Kontingentinformationen für einen bestimmten Benutzer und detaillierte Kontingentstatistiken für jedes Objektspeicherziel (OST) und Metadatenziel (MDT). Benutzer mit Root-Benutzer-Anmeldeinformationen des - AWS Kontos können diesen Befehl für jeden Benutzer ausführen, Nicht-Root-Benutzer können diesen Befehl jedoch nicht ausführen, um Kontingentinformationen über andere Benutzer abzurufen.
`lfs quota -g groupname /mount_point`	Allgemeine Kontingentinformationen für eine bestimmte Gruppe.
`lfs quota -p projectid /mount_point`	Allgemeine Kontingentinformationen für ein bestimmtes Projekt.
`lfs quota -t -u /mount_point`	Sperren und Inode-Kulanzzeiten für Benutzerkontingente.
`lfs quota -t -g /mount_point`	Sperren und Inode-Kulanzzeiten für Gruppenkontingente.

Anzeigen des Kontingentbefehls	Angezeigte Kontingentinformationen
`lfs quota -t -p /mount_point`	Sperren und Inode-Kulanzzeiten für Projektkontingente.

Kontingente und mit Amazon S3 verknüpfte Buckets

Sie können Ihr FSx-for-Lustre-Dateisystem mit einem Amazon S3-Daten-Repository verknüpfen. Weitere Informationen finden Sie unter Verknüpfen Sie Ihr Dateisystem mit einem S3-Bucket.

Sie können optional einen bestimmten Ordner oder ein bestimmtes Präfix innerhalb eines verknüpften S3-Buckets als Importpfad zu Ihrem Dateisystem auswählen. Wenn ein Ordner in Amazon S3 angegeben und aus S3 in Ihr Dateisystem importiert wird, werden nur die Daten aus diesem Ordner auf das Kontingent angewendet. Die Daten des gesamten Buckets werden nicht auf die Kontingentlimits angerechnet.

Dateimetadaten in einem verknüpften S3-Bucket werden in einen Ordner importiert, dessen Struktur mit dem importierten Ordner aus Amazon S3 übereinstimmt. Diese Dateien werden auf die Inode-Kontingente der Benutzer und Gruppen angerechnet, die Eigentümer der Dateien sind.

Wenn ein Benutzer eine `hsm_restore` Datei oder Lazy lädt, wird die vollständige Größe der Datei auf das Blockkontingent angerechnet, das dem Eigentümer der Datei zugeordnet ist. Wenn Benutzer A beispielsweise Lazy eine Datei lädt, die Benutzer B gehört, wird die Speicher- und 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 Blockkontingenten des Benutzers oder der Gruppe freigegeben, dem/der die Datei gehört.

Da HSM-Wiederherstellungen und Lazy Loading mit Root-Zugriff durchgeführt werden, umgehen sie die Durchsetzung von Kontingenten. Sobald Daten importiert wurden, werden sie dem Benutzer oder der Gruppe auf der Grundlage der in S3 festgelegten Eigentümerschaft angerechnet, was dazu führen kann, dass Benutzer oder Gruppen ihre Blocklimits überschreiten. In diesem Fall müssen sie Dateien freigeben, um erneut in das Dateisystem schreiben zu können.

Ebenso erstellen Dateisysteme mit aktiviertem automatischen Import automatisch neue Inodes für Objekte, die zu S3 hinzugefügt werden. Diese neuen Knoten werden mit Root-Zugriff und Umgehung

der Kontingenterzwingung während ihrer Erstellung erstellt. Diese neuen Knoten werden den Benutzern und Gruppen angerechnet, je nachdem, wem das Objekt in S3 gehört. Wenn diese Benutzer und Gruppen ihre Inode-Kontingente basierend auf automatischen Importaktivitäten überschreiten, müssen sie Dateien löschen, um zusätzliche Kapazität freizugeben und ihre Kontingentlimits zu unterschreiten.

Kontingente und Wiederherstellen 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.

Verwalten der Speicherkapazität

Sie können die Speicherkapazität erhöhen, die auf Ihrem FSx-for-Lustre-Dateisystem konfiguriert ist, wenn Sie zusätzlichen Speicher und Durchsatz benötigen. Da der Durchsatz eines FSx for Lustre-Dateisystems linear mit der Speicherkapazität skaliert wird, erhalten Sie auch eine vergleichbare Erhöhung 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 Netzwerkdateiserver hinzu und skaliert Ihren Metadatenserver. Bei der Skalierung der Speicherkapazität ist das Dateisystem möglicherweise einige Minuten lang nicht verfügbar. Dateioperationen, die von Clients ausgegeben werden, während das Dateisystem nicht verfügbar ist, werden transparent 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 gesetzt`AVAILABLE`.

Amazon FSx führt dann einen Speicheroptimierungsprozess durch, der Daten transparent über die vorhandenen und neu hinzugefügten Dateiserver verteilt. Der Neuausgleich erfolgt im Hintergrund ohne Auswirkungen auf die Verfügbarkeit des Dateisystems. Während des Neuausgleichs kann es zu einer verringerten Dateisystemleistung kommen, wenn Ressourcen für die Datenverschiebung verbraucht werden. Bei den meisten Dateisystemen dauert die Speicheroptimierung einige Stunden bis zu einigen Tagen. Sie können während der Optimierungsphase auf Ihr Dateisystem zugreifen und es verwenden.

Sie können den Fortschritt der Speicheroptimierung jederzeit mithilfe der Amazon-FSx-Konsole, der CLI und der API verfolgen. Weitere Informationen finden Sie unter Überwachung des Anstiegs der Speicherkapazität.

Themen

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.
- Erhöhungsinkremente – Wenn Sie die Speicherkapazität erhöhen, verwenden Sie die im Dialogfeld Speicherkapazität erhöhen aufgeführten Inkremente.
- Zeit zwischen den Erhöhungen – Sie können keine weiteren Erhöhungen der Speicherkapazität in einem Dateisystem vornehmen, bis 6 Stunden nach der letzten Erhöhung oder bis der Speicheroptimierungsprozess abgeschlossen ist, je nachdem, welcher Zeitraum länger ist.
- Durchsatzkapazität – Sie erhöhen die Durchsatzkapazität automatisch, 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 HDD-Speicherkapazität dimensioniert 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 Verwalten der Durchsatzkapazität.

- Bereitstellungstyp – Sie können die Speicherkapazität aller Bereitstellungstypen erhöhen, mit Ausnahme von Scratch-1-Dateisystemen. 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 des freien Speichers zu überwachen, der im Dateisystem verfügbar ist. Sie können einen Amazon CloudWatch-Alarm für diese Metrik erstellen und benachrichtigt werden, wenn sie unter einen bestimmten Schwellenwert fällt. Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch.

Sie können - CloudWatch Metriken verwenden, um die kontinuierliche Durchsatznutzung Ihres Dateisystems zu überwachen. Wenn Sie feststellen, dass Ihr Dateisystem eine höhere Durchsatzkapazität benötigt, können Sie anhand der Metrikinformationen entscheiden, wie stark Sie die Speicherkapazität erhöhen möchten. Weitere Informationen zum Ermitteln des aktuellen Durchsatzes Ihres Dateisystems 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 für Lustre.

Sie können die Speicherkapazität und den Gesamtdurchsatz Ihres Dateisystems auch im Bereich Zusammenfassung der Seite mit den Dateisystemdetails anzeigen.

So werden gleichzeitige Speicherskalierungs- und Backup-Anforderungen verarbeitet

Sie können eine Sicherung kurz vor Beginn oder während der Ausführung eines Workflows zur Speicherskalierung anfordern. Die Reihenfolge, in der Amazon FSx die beiden Anfragen verarbeitet, lautet wie folgt:

- Wenn ein Workflow zur Speicherskalierung ausgeführt wird (der Status der Speicherskalierung ist `IN_PROGRESS` und der Dateisystemstatus ist `UPDATING`) und Sie eine Sicherung anfordern, wird die Sicherungsanforderung in die Warteschlange gestellt. Die Backup-Aufgabe wird gestartet, wenn sich die Speicherskalierung in der Speicheroptimierungsphase befindet (Speicherskalierungsstatus ist `UPDATED_OPTIMIZING` und Dateisystemstatus ist `AVAILABLE`).
- Wenn das Backup läuft (der Backup-Status ist `CREATING`) und Sie eine Speicherskalierung anfordern, wird die Speicherskalierungsanforderung in die Warteschlange gestellt. Der Workflow

zur Speicherskalierung wird gestartet, wenn Amazon FSx das Backup an Amazon S3 überträgt (der Backup-Status ist `TRANSFERRING`).

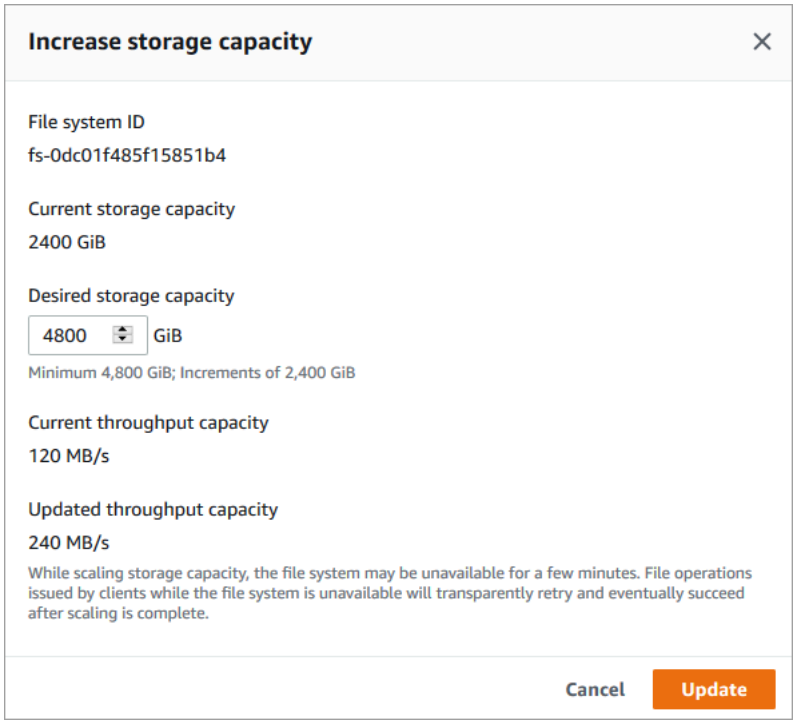
Wenn eine Speicherskalierungsanforderung aussteht und eine Sicherungsanforderung für das Dateisystem ebenfalls aussteht, hat die Sicherungsaufgabe Vorrang. Die Speicherskalierungsaufgabe wird erst gestartet, wenn die Sicherungsaufgabe abgeschlossen ist.

Wie erhöht man die Speicherkapazität

Sie können die Speicherkapazität eines Dateisystems mithilfe der Amazon-FSx-KonsoleAWS CLI, der oder der Amazon-FSx-API erhöhen.

So erhöhen Sie die Speicherkapazität für ein Dateisystem (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 Speicherkapazität erhöhen möchten.
3. Wählen Sie für Aktionen die Option Speicherkapazität aktualisieren aus. Oder wählen Sie im Bereich Zusammenfassung neben der Speicherkapazität des Dateisystems die Option Aktualisieren aus, um das Dialogfeld Speicherkapazität erhöhen anzuzeigen.



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 in Vielfachen von 2400 GiB angegeben werden.
   - Für ein persistentes HDD-Dateisystem muss dieser Wert in Vielfachen von 6 000 GiB für 12 MB/s/TiB-Dateisysteme und in Vielfachen von 1 800 GiB für 40 MB/s/TiB-Dateisysteme angegeben werden.

   > **Note**
   >
   > Sie können die Speicherkapazität von Scratch-1-Dateisystemen nicht erhöhen.

5. Wählen Sie Aktualisieren, um die Aktualisierung der Speicherkapazität zu initiieren.
6. Sie können den Aktualisierungsfortschritt auf der Detailseite des Dateisystems auf der Registerkarte Updates überwachen.

So erhöhen Sie die Speicherkapazität für ein Dateisystem (CLI)

1. Verwenden Sie den AWS CLI Befehl , um die Speicherkapazität für ein FSx-for-Lustre-Dateisystem zu erhöhenupdate-file-system. Legen Sie die folgenden Parameter fest:

   Setzen Sie `--file-system-id` auf die ID des Dateisystems, das Sie aktualisieren.

   Auf `--storage-capacity` einen ganzzahligen Wert festlegen, der der Menge der Speicherkapazitätserhöhung in GiB entspricht. Für ein persistentes SSD- oder Scratch-2-Dateisystem muss dieser Wert in Vielfachen von 2400 angegeben werden. Für ein persistentes HDD-Dateisystem muss dieser Wert in Vielfachen von 6 000 für 12 MB/s/TiB-Dateisysteme und in Vielfachen von 1 800 für 40 MB/s/TiB-Dateisysteme liegen. Der neue Zielwert muss größer sein als die aktuelle Speicherkapazität des Dateisystems.

   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 der Aktualisierung mit dem AWS CLI Befehl überwachendescribe-file-systems. Suchen Sie `administrative-actions` in der Ausgabe nach .

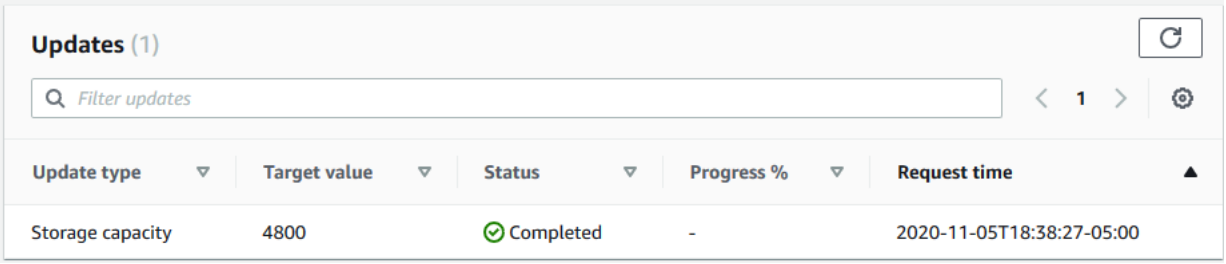
   Weitere Informationen finden Sie unter AdministrativeAction.

Überwachung des Anstiegs der Speicherkapazität

Sie können den Fortschritt einer Erhöhung der Speicherkapazität mithilfe der Amazon-FSx-Konsole, der API oder der überwachenAWS CLI.

Überwachen von Erhöhungen in der Konsole

Auf der Registerkarte Updates auf der Seite mit den Dateisystemdetails können Sie die 10 letzten Updates für jeden Aktualisierungstyp anzeigen.



Sie können die folgenden Informationen anzeigen:

Aktualisierungstyp

Unterstützte Typen sind Speicherkapazität und Speicheroptimierung.

Zielwert

Der gewünschte Wert, auf den die Speicherkapazität des Dateisystems aktualisiert werden soll.

Status

Der aktuelle Status der Speicherkapazitätsaktualisierungen. Die möglichen Werte lauten wie folgt:

- Ausstehend – Amazon FSx hat die Aktualisierungsanforderung erhalten, aber noch nicht mit der Verarbeitung begonnen.
- In Bearbeitung – Amazon FSx verarbeitet die Aktualisierungsanforderung.
- Aktualisiert; Optimieren – Amazon FSx hat die Speicherkapazität des Dateisystems erhöht. Der Prozess der Speicheroptimierung gleicht jetzt Daten über die Dateiserver aus.

- Abgeschlossen – Die Erhöhung der Speicherkapazität wurde erfolgreich abgeschlossen.
- Fehlgeschlagen – Die Erhöhung der Speicherkapazität ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Details dazu anzuzeigen, warum die Speicheraktualisierung fehlgeschlagen ist.

Fortschritt in %

Zeigt den Fortschritt des Speicheroptimierungsprozesses als abgeschlossen an.

Anforderungszeit

Der Zeitpunkt, zu dem Amazon FSx die Aktualisierungsaktionsanforderung erhalten hat.

Überwachen von Erhöhungen mit der AWS CLI und API

Sie können Anforderungen zur Erhöhung der Speicherkapazität des Dateisystems mit dem describe-file-systems AWS CLI Befehl und der DescribeFileSystems API-Aktion 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 - `FILE_SYSTEM_UPDATE` und eine -`STORAGE_OPTIMIZATION`Aktion.

Das folgende Beispiel zeigt einen Auszug aus der Antwort eines describe-file-systems CLI-Befehls. Das Dateisystem hat eine Speicherkapazität von 4 800 GB und es gibt eine ausstehende administrative Maßnahme, um die Speicherkapazität auf 9 600 GB zu erhöhen.

```
{
    "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 zuerst die `FILE_SYSTEM_UPDATE` Aktion und fügt dem Dateisystem neue Dateiserver hinzu. Wenn der neue Speicher für das Dateisystem verfügbar ist, ändert sich der `FILE_SYSTEM_UPDATE` Status in `UPDATED_OPTIMIZING`. Die Speicherkapazität zeigt den neuen größeren Wert, und Amazon FSx beginnt mit der Verarbeitung der `STORAGE_OPTIMIZATION` administrativen Aktion. Dies wird im folgenden Auszug der Antwort eines describe-file-systems CLI-Befehls 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 gezeigt.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 4800,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 9600
                }
            ]
```

Verwalten der Durchsatzkapazität

Jedes FSx-für-Lustre-Dateisystem verfügt über eine Durchsatzkapazität, die beim Erstellen des Dateisystems konfiguriert wird. Der Durchsatz eines FSx for Lustre-Dateisystems 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. Eine höhere Durchsatzkapazität bietet auch höhere IOPS (I/O Operations Per Second) und mehr Speicher für das Zwischenspeichern von Daten auf dem Dateiserver. Weitere Informationen finden Sie unter Leistung von Amazon FSx für Lustre.

Sie können die Durchsatzstufe eines persistenten SSD-basierten Dateisystems ändern, indem Sie den Wert des Durchsatzes des Dateisystems pro Speichereinheit erhöhen oder verringern. Gültige Werte hängen wie folgt vom Bereitstellungstyp des Dateisystems ab:

- Für SSD-basierte Bereitstellungstypen von Persistent_1 sind die gültigen Werte 50, 100 und 200 MB/s/TiB .
- Für SSD-basierte Bereitstellungstypen von Persistent_2 lauten die gültigen Werte 125, 250, 500 und 1 000 MB/s/TiB .

Sie können den aktuellen Wert des Durchsatzes des Dateisystems pro Speichereinheit wie folgt anzeigen:

- Verwenden der Konsole – Im Bereich Zusammenfassung der 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 im Hintergrund ändern, schaltet Amazon FSx die Dateiserver des Dateisystems aus. Ihr Dateisystem ist während der Skalierung der Durchsatzkapazität einige Minuten lang nicht verfügbar. Ihnen wird die neue Menge an Durchsatzkapazität in Rechnung gestellt, sobald sie für Ihr Dateisystem verfügbar ist.

Themen

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 im Dialogfeld Durchsatzstufe aktualisieren aufgeführten Inkremente.
- Zeit zwischen den Erhöhungen – Sie können keine weiteren Änderungen der Durchsatzkapazität in einem Dateisystem vornehmen, bis 6 Stunden nach der letzten Anforderung oder bis der Prozess zur Durchsatzoptimierung abgeschlossen ist, je nachdem, welcher Zeitraum länger ist.
- Bereitstellungstyp – Sie können nur die Durchsatzkapazität persistenter SSD-basierter Bereitstellungstypen aktualisieren.

Wann sollte die Durchsatzkapazität geändert werden?

Amazon FSx lässt sich in Amazon integrieren CloudWatch, sodass Sie die kontinuierliche Durchsatznutzung Ihres Dateisystems überwachen können. Die Leistung (Durchsatz und IOPS), die Sie durch Ihr Dateisystem steuern können, hängt zusätzlich zur Durchsatzkapazität, Speicherkapazität und Speichertyp Ihres Dateisystems von den Eigenschaften Ihres spezifischen Workloads ab. Weitere Informationen zum Ermitteln des aktuellen Durchsatzes Ihres Dateisystems finden Sie unter So verwenden Sie Amazon FSx for Lustre-Metriken. Weitere Informationen zu - CloudWatch Metriken finden Sie unter Überwachung mit Amazon CloudWatch.

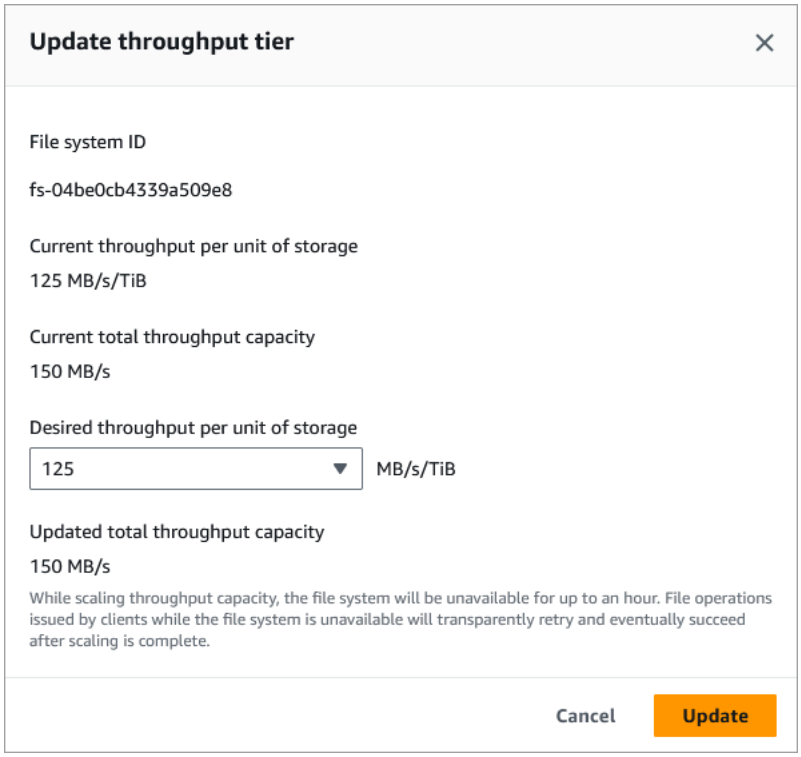
So ändern Sie die Durchsatzkapazität

Sie können die Durchsatzkapazität eines Dateisystems mithilfe der Amazon-FSx-Konsole, der AWS Command Line Interface (AWS CLI) oder der Amazon-FSx-API ändern.

So ändern Sie die Durchsatzkapazität eines Dateisystems (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-für-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 dem Durchsatz des Dateisystems pro Speichereinheit 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.



5. Wählen Sie Aktualisieren, um die Aktualisierung der Durchsatzkapazität zu initiieren.

> **Note**
>
> Bei Ihrem Dateisystem kann es während der Aktualisierung zu einer sehr kurzen Zeit der Nichtverfügbarkeit kommen.

So ändern Sie die Durchsatzkapazität (CLI) eines Dateisystems

- Um die Durchsatzkapazität eines Dateisystems zu ändern, verwenden Sie den update-file-system CLI-Befehl (oder die entsprechende UpdateFileSystem API-Operation). Legen Sie die folgenden Parameter fest:

  - Setzen Sie `--file-system-id` auf die ID des Dateisystems, das Sie aktualisieren.
  - Setzen Sie `--lustre-configuration PerUnitStorageThroughput` auf den Wert `50`, `100`, oder `200` MB/s/TiB für Persistent_1 SSD-Dateisysteme oder auf den Wert `125`, `250`, `500`oder `1000` MB/s/TiB für Persistent_2 SSD-Dateisysteme.

  Dieser Befehl gibt an, dass die Durchsatzkapazität für das Dateisystem auf 1000 MB/s/TiB festgelegt werden soll.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration PerUnitStorageThroughput=1000
```

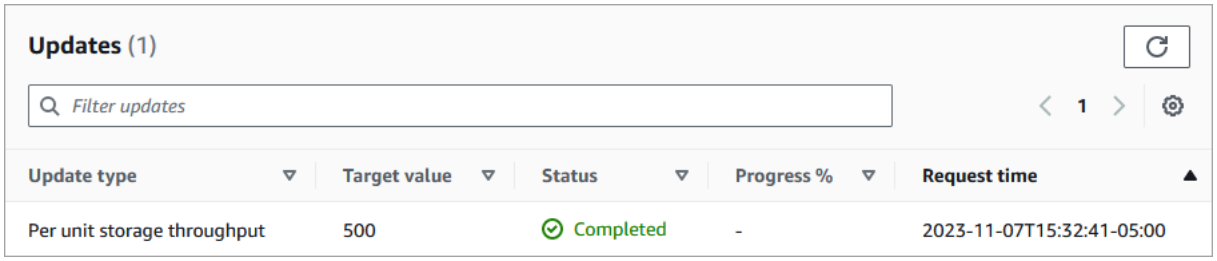
Überwachen von Änderungen der Durchsatzkapazität

Sie können den Fortschritt einer Änderung der Durchsatzkapazität mithilfe der Amazon-FSx-Konsole, der API und der überwachenAWS CLI.

Überwachen 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 letzten Aktualisierungsaktionen für jeden Aktualisierungsaktionstyp anzeigen.



  Für Aktionen zur Aktualisierung der Durchsatzkapazität können Sie die folgenden Informationen anzeigen.

  Aktualisierungstyp

  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 der Aktualisierung. Für Aktualisierungen der Durchsatzkapazität sind die möglichen Werte wie folgt:

  - Ausstehend – Amazon FSx hat die Aktualisierungsanforderung erhalten, hat aber nicht mit der Verarbeitung begonnen.

- In Bearbeitung – Amazon FSx verarbeitet die Aktualisierungsanforderung.
- Aktualisiert; Optimieren – Amazon FSx hat die Netzwerk-I/O-, CPU- und Speicherressourcen des Dateisystems aktualisiert. Das neue Disk-I/O-Leistungsniveau ist für Schreibvorgänge verfügbar. Ihre Lesevorgänge sehen die Festplatten-I/O-Leistung zwischen der vorherigen Ebene und der neuen Ebene, bis sich Ihr Dateisystem nicht mehr in diesem Status befindet.
- Abgeschlossen – Die Aktualisierung der Durchsatzkapazität wurde erfolgreich abgeschlossen.
- Fehlgeschlagen – Die Aktualisierung der Durchsatzkapazität ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Details dazu anzuzeigen, warum die Durchsatzaktualisierung fehlgeschlagen ist.

Anforderungszeit

Der Zeitpunkt, zu dem Amazon FSx die Aktualisierungsanforderung erhalten hat.

Überwachen von Dateisystemaktualisierungen (CLI)

- Sie können Anforderungen zur Änderung der Durchsatzkapazität des Dateisystems mit dem describe-file-systems -CLI-Befehl und der DescribeFileSystems-API-Aktion anzeigen und überwachen. Das `AdministrativeActions`Array listet die 10 letzten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die Durchsatzkapazität eines Dateisystems ändern, wird eine `FILE_SYSTEM_UPDATE` administrative Aktion generiert.

  Das folgende Beispiel zeigt den Antwortauszug 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.

Bei der Datenkomprimierung wird der LZ4-Algorithmus verwendet, 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 ausgewogenes Verhältnis zwischen Kompressionsgeschwindigkeit 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 Speichern übertragen wird. Wenn Sie nicht bereits komprimierte Dateiformate verwenden, werden Sie bei der Datenkomprimierung eine Erhöhung der Gesamtdurchsatzkapazität des Dateisystems feststellen. Erhöhungen der Durchsatzkapazität im Zusammenhang mit der Datenkomprimierung werden begrenzt, nachdem Sie Ihre Frontend-Netzwerkschnittstellenkarten überlastet haben.

Wenn es sich bei Ihrem Dateisystem beispielsweise um einen PERSISTENT-50-SSD-Bereitstellungstyp handelt, liegt Ihr Netzwerkdurchsatz bei einem Basiswert von 250 MB/s pro TiB Speicher. Ihr Festplattendurchsatz hat einen Basiswert von 50 MB/s pro TiB. Bei der Datenkomprimierung könnte Ihr Festplattendurchsatz von 50 MB/s pro TiB auf maximal 250 MB/s pro TiB steigen, was der grundlegenden Netzwerkdurchsatzgrenze entspricht. Weitere Informationen zu

Netzwerk- und Festplattendurchsatzlimits finden Sie in den Leistungstabellen für das Dateisystem unterAggregierte Dateisystemleistung. Weitere Informationen zur Datenkomprimierungsleistung finden Sie im Beitrag Weniger ausgeben und gleichzeitig die Leistung erhöhen mit Amazon FSx for Lustre im AWSStorage-Blog.

Themen

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 erstellen.AWS CLI

So aktivieren Sie die Datenkomprimierung beim Erstellen eines Dateisystems (Konsole)

1. Öffnen Sie die Amazon FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, dasErstellen Sie Ihr FSx for Lustre-Dateisystem im Abschnitt Erste Schritte beschrieben wird.
3. Wählen Sie im Abschnitt Dateisystemdetails als Datenkomprimierungstyp die Option LZ4 aus.
4. Füllen Sie den Assistenten wie beim Erstellen eines neuen Dateisystems aus.
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 im Folgenden 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 Komprimierung zuvor geschriebener Dateien.

So aktualisieren Sie die Datenkomprimierung auf einem vorhandenen Dateisystem (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 Datenkomprimierung verwalten möchten.
3. Wählen Sie für Aktionen den Komprimierungstyp „Datenkomprimierung aktualisieren“.
4. Wählen Sie im Dialogfeld Datenkomprimierungstyp aktualisieren die Option LZ4, um die Datenkomprimierung zu aktivieren, oder wählen Sie KEINE, um sie zu deaktivieren.
5. Wählen Sie Update (Aktualisieren).
6. Sie können den Aktualisierungsfortschritt auf der Dateisystem-Detailseite auf der Registerkarte Updates überwachen.

So aktualisieren Sie die Datenkomprimierung in einem vorhandenen Dateisystem (CLI)

Verwenden Sie denAWS CLI Befehl, um die Datenkomprimierungskonfiguration für ein vorhandenes FSx for Lustre-Dateisystem zu aktualisieren update-file-system. Legen Sie die folgenden Parameter fest:

- Auf`--file-system-id` die ID des Dateisystems setzen, das Sie aktualisieren.
- Stellen Sie`--lustre-configuration DataCompressionType` dieseNONE Option ein, um die DatenkomprimierungLZ4 zu deaktivieren oder die Datenkomprimierung mit dem LZ4-Algorithmus zu aktivieren.

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 Sicherung

Sie können ein verfügbares Backup verwenden, um ein neues Amazon FSx for Lustre-Dateisystem zu erstellen. Wenn Sie ein neues Dateisystem aus einer Sicherung erstellen, müssen Sie das nicht angeben`DataCompressionType`. Die Einstellung wird anhand der`DataCompressionType` Backup-Einstellung angewendet. Wenn Sie`DataCompressionType` beim Erstellen aus einer Sicherung den angeben, muss der Wert mit den`DataCompressionType` Einstellungen des Backups übereinstimmen.

Um die Einstellungen für ein Backup anzuzeigen, wählen Sie es auf der Registerkarte Backups der Amazon FSx-Konsole aus. Einzelheiten des Backups werden auf der Übersichtsseite des Backups aufgeführt. Sie können den `describe-backups`AWS CLIBefehl auch ausführen (die entsprechende API-Aktion ist `DescribeBackups`).

Komprimierung zuvor geschriebener Dateien

Dateien sind unkomprimiert, wenn sie erstellt wurden, als die Datenkomprimierung im Amazon FSx for Lustre-Dateisystem deaktiviert wurde. 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 wurde, um vorhandene Dateien zu komprimieren. Ein Beispiel finden Sie unter FSXL-Komprimierung, die verfügbar ist 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.

CloudWatch Metriken verwenden

Sie können Amazon CloudWatch Logs-Metriken verwenden, um Ihre Dateisystemnutzung einzusehen. Die`LogicalDiskUsage` Metrik zeigt die gesamte logische Festplattenauslastung (ohne Komprimierung) und die`PhysicalDiskUsage` Metrik zeigt die gesamte physische Festplattenauslastung (mit Komprimierung). Diese beiden Metriken sind nur verfügbar, wenn in Ihrem Dateisystem die Datenkomprimierung aktiviert ist oder diese zuvor aktiviert war.

Sie können die Kompressionsrate Ihres Dateisystems ermitteln, indem Sie den Wert`Sum` der`LogicalDiskUsage` Statistik durch den Wert`Sum` der`PhysicalDiskUsage` Statistik dividieren. Hinweise zur Verwendung von metrischer Mathematik zur Berechnung dieses Verhältnisses finden Sie unterMetrische Mathematik: Datenkomprimierungsrate.

Weitere Informationen zur Überwachung der Leistung Ihres Dateisystems finden Sie unterÜberwachung 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

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 und 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 gezeigt. Um Root Squash beim Erstellen eines Dateisystems (Konsole) zu aktivieren Sie können den `RootSquash` Parameter auch mit der API AWS CLI oder verwenden, um die UID- und GID-Werte bereitzustellen, wie unter gezeigt. So aktivieren Sie Root Squash beim Erstellen eines Dateisystems (CLI)

Optional können Sie auch eine Liste mit NIDs von Clients angeben, für die Root-Squash nicht gilt. Eine Client-NID ist eine Lustre-Netzwerkkennung, 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 unterRoot Squash verwalten.

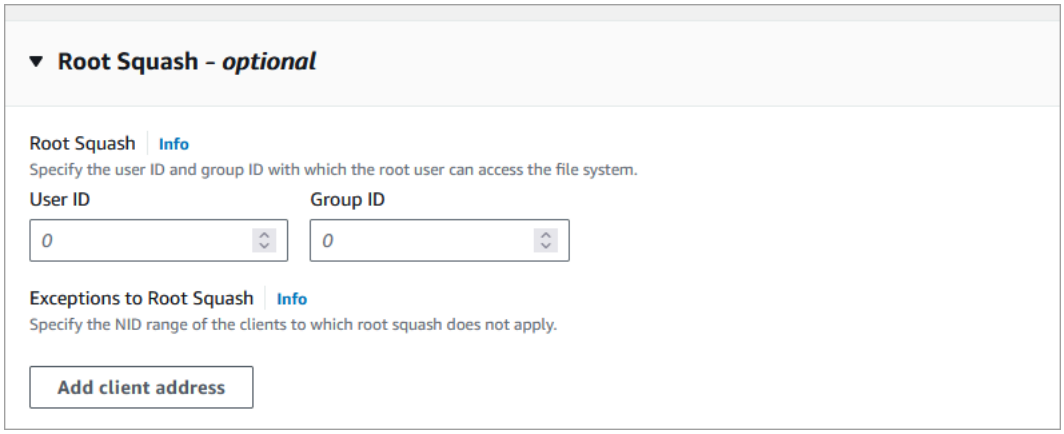
> **Note**
>
> Root Squash wird für Backups und Wiederherstellungen nicht unterstützt. Um Backups und Wiederherstellungen verwenden zu können, müssen Sie Root Squash deaktivieren, indem Sie den `RootSquash` Parameter auf `0:0` und den `NoSquashNids` Parameter auf `[]` mit der AWS CLI oder API setzen oder indem Sie im Dialogfeld Root Squash-Einstellungen aktualisieren in der Amazon FSx-Konsole die Option 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 unterWie funktioniert Root Squash.
   3. Wiederholen Sie den Vorgang nach Bedarf, um weitere Client-IP-Adressen hinzuzufügen.

6. Führen Sie den Assistenten genauso aus, wie Sie es beim Erstellen eines neuen Dateisystems tun.
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-Netzwerkkennungen (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.

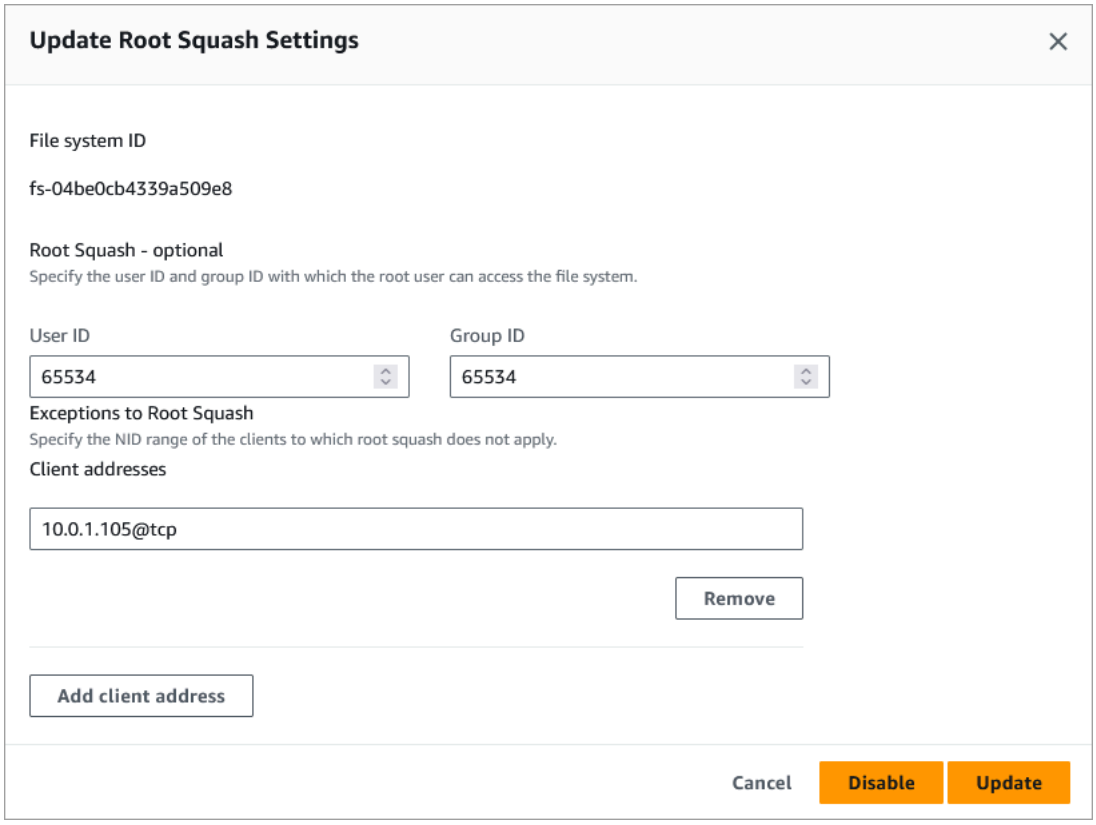
```
{

    "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.



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 aus.

> **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-Netzwerkkennungen (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-systemsoder der API-Operation anzeigen. DescribeFileSystems

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 Dateisyst em.
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: • Das Dateisystem ist ausgefallen und Amazon FSx kann es nicht wiederherstellen. • Beim Erstellen eines neuen Dateisystems konnte Amazon FSx das Dateisystem nicht erstellen.

Markieren Ihrer Amazon ECX-Ressourcen mit Tags

Um Sie bei der Verwaltung Ihrer Dateisysteme und anderer Amazon FSx for Lustre Lustre-Ressourcen zu unterstützen, können Sie jeder Ressource eigene Metadaten in Form von Tags zuweisen. Mit Tags (Markierungen) 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)

Ein Tag (Markierung) ist eine Markierung, die Sie einer AWS-Ressource zuordnen. Jeder Tag (Markierung) besteht aus einem Schlüssel und einem optionalen Wert, beides können Sie bestimmen.

Mit Tags (Markierungen) können Sie Ihre AWS-Ressourcen auf unterschiedliche Weise kategorisieren (z. B. nach Zweck, Eigentümer oder Umgebung). Sie können zum Beispiel eine Reihe von Tags für die Amazon FSX for Lustre-Dateisysteme in Ihrem Konto definieren, um die Eigentümer der einzelnen Instances und die Stack-Ebene nachzuverfolgen.

Wir empfehlen die Verwendung von Tag (Markierung)-Schlüsseln, die die Anforderungen der jeweiligen Ressourcentypen erfüllen. Eine Anzahl einheitlicher Tag (Markierung)-Schlüssel vereinfacht das Verwalten der Ressourcen. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags (Markierungen) filtern und danach suchen.

Tags (Markierungen) haben keine semantische Bedeutung für Amazon ECX und werden ausschließlich als Zeichenfolgen 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,AWS CLI oder eineAWS SDK verwenden, verwenden Sie die`TagResource` API-Aktion, 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 Lustre-Ressourcen markieren, die in Ihrem Konto bestehen. Wenn Sie die Amazon FSX-Konsole verwenden, können Sie auf der Registerkarte Tags auf dem entsprechenden Ressourcenbildschirm Tags auf Ressourcen anwenden. Wenn Sie Ressourcen erstellen, können Sie den Name-Schlüssel mit einem Wert anwenden, und Sie können Tags Ihrer Wahl anwenden, wenn Sie ein neues Dateisystem erstellen. Die Konsole strukturiert Ressourcen gemäß dem Name -Tags Name. Allerdings hat das Tag keine semantische Bedeutung für den Amazon FSx for Lustre-Service.

Sie können Tag-basierte Berechtigungen auf Ressourcenebene in Ihren IAM-Richtlinien auf die Amazon FSX for LustreAPI-Aktionen anwenden, die das Tagging bei der Erstellung unterstützen, um eine granulare Kontrolle über die Benutzer und Gruppen zu implementieren, die Ressourcen bei der Erstellung mit Tags versehen 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 ebenfalls Berechtigungen auf Ressourcenebene auf die `-TagResource` und`UntagResource` -Amazon FSx for Lustre-API-Aktionen in den IAM-Richtlinien anwenden, um die Tag-Schlüssel und -Werte zu steuern, die für Ihre bestehenden Ressourcen festgelegt sind.

Weitere Informationen zum Markieren von Ressourcen für die Fakturierung finden Sie unter Verwendung von Tags (Markierungen) zur Kostenzuordnung im Benutzerhandbuch für AWS Billing.

Tag (Markierung)-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
- Folgende Zeichen für Amazon FSx for Lustre Lustre-Tags sind: Buchstaben, Zahlen und Leerzeichen, die in UTF-8 darstellbar sind, und die folgenden Sonderzeichen: + - =. _:/@
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Das Präfix `aws:` ist zur Verwendung in AWS 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 Ressourcen nicht allein auf Grundlage ihrer Tags löschen. Um ein Dateisystem zu löschen, das Sie mit einem Tag-Schlüssel markiert haben`DeleteMe`, müssen Sie die`DeleteFileSystem` Aktion mit dem DateisystemRessourcenbezeichner verwenden, z. B. fs-1234567890abcdef0.

Wenn Sie öffentliche oder gemeinsam genutzte Ressourcen markieren, sind die von IhnenAWS-Konto zugewiesenenAWS-Konto Tags nur für Sie verfügbar. Für die Tag basierte Zugriffskontrolle auf freigegebene RessourcenAWS-Konto muss jede Ressource ihren eigenen Satz von Tags zuweisen, um den Zugriff auf die Ressource zu kontrollieren.

Berechtigungen

Weitere Informationen zu den Berechtigungen, die erforderlich sind, um Amazon FSx-Ressourcen bei der Erstellung zu taggen,Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung finden Sie unter. Weitere Informationen zur Verwendung von Tags zur Beschränkung des Zugriffs auf Amazon FSx-Ressourcen in IAM-Richtlinien finden Sie unterVerwenden von mithilfe von von von von von von von von von von von von von von von von von FSx von mit.

Wartungszeitraum ändern: Amazon FSx for Lustre Wartungszeitraum ändern

Amazon FSx for Lustre führt routinemäßiges Software-Patching für die von ihm verwaltete Lustre-Software durch. Das Wartungsfenster bietet Ihnen die Möglichkeit, zu kontrollieren, an welchem Tag und zu welcher Uhrzeit die Softwarepatches 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. Das Wartungsfenster wählen Sie bei der Erstellung des Dateisystems. Wenn Sie keine Zeitpräferenz haben, wird ein 30-minütiges Standardfenster zugewiesen.

Mit FSx for Lustre können Sie Ihr Wartungsfenster nach Bedarf an Ihre Arbeitslast und Betriebsanforderungen anpassen. Sie können Ihr Wartungsfenster beliebig oft verschieben, sofern mindestens 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 ConsoleAWS CLI, dieAWS API oder eines derAWS SDKs verwenden, um das Wartungsfenster für Ihre Dateisysteme zu ändern.

So bearbeiten Sie den Wartungszeitraum ändern möchten

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 den Wartungszeitraum ändern möchten. Die Seite mit den Dateisystemdetails wird angezeigt.
4. Wählen Sie den Tab Wartung. Das Einstellungsfenster des Wartungsfensters wird angezeigt.
5. Wählen Sie Bearbeiten und geben Sie den neuen Tag und die neue Uhrzeit ein, zu der das Wartungsfenster beginnen soll.
6. Wählen Sie Save (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-systemCLI-Befehl ändern. Führen Sie den folgenden Befehl aus und ersetzen Sie die Dateisystem-ID durch die ID für Ihr Dateisystem sowie das Datum und die Uhrzeit, an denen Sie das Fenster beginnen 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 AgeOfOldestQueuedMessageMetrik Null ist (wenn Sie den automatischen Export verwenden), oder Sie können eine Aufgabe zum Exportieren eines Datenrepositorys 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 DeleteFileSystemAPI-Vorgang oder den delete-file-systemCLI-Befehl.

Migrieren zu Amazon FSx for Lustre unter Verwendung von AWS DataSync

Sie können AWS DataSync es verwenden, um Daten zwischen FSx for Lustre-Dateisystemen zu übertragen. DataSyncist ein Service für die Datenübertragung, der das Verschieben und Replizieren von Daten zwischen selbstverwalteten Speichersystemen und AWS Speicherdiensten über das Internet vereinfacht, automatisiert und beschleunigt. AWS Direct Connect DataSynckann Ihre Dateisystemdaten und Metadaten wie Eigentum, Zeitstempel und Zugriffsberechtigungen übertragen.

So migrieren Sie vorhandene Dateien zu FSx for Lustre mit AWS DataSync

Sie können FSx for Lustre-Dateisysteme verwendenDataSync, um einmalige Datenmigrationen durchzuführen, Daten für verteilte Workloads regelmäßig zu erfassen und die Replikation für Datenschutz und Wiederherstellung zu planen. Informationen zu bestimmten Übertragungsszenarien finden Sie unter Wo kann ich meine Daten übertragen? im AWS DataSyncBenutzerhandbuch.

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 DataSync im AWS DataSyncBenutzerhandbuch unter Anforderungen für.

- Sie haben ein FSx Ziel-Dateisystem für Lustre-Dateisystem erstellt. Weitere Informationen finden Sie unter Erstellen Sie Ihr FSx for Lustre-Dateisystem.
- Das Quell- und das Zieldateisystem sind in derselben Virtual Private Cloud (VPC) miteinander verbunden. Das Quelldateisystem kann sich vor Ort oder in einer anderen Amazon VPC befinden, oder AWS-KontoAWS-Region, aber es muss sich in einem Netzwerk befinden, das mit dem des Zieldateisystems über Amazon VPC Peering, Transit Gateway, oder verbunden ist. AWS Direct Connect AWS VPN Weitere Informationen finden Sie unter Was ist VPC Peering? im Amazon VPC Peering Guide.

> **Note**
>
> DataSynckann nur von oder AWS-Konten zu FSx for Lustre übertragen werden, wenn der andere Übertragungsort Amazon S3 ist.

Grundlegende Schritte für die Migration von Dateien mit DataSync

Das Verschieben von Dateien von einer Quelle an ein Ziel mit DataSync umfasst die folgenden grundlegenden Schritte:

- Laden Sie einen Agenten herunter, stellen Sie ihn in Ihrer Umgebung bereit und aktivieren Sie ihn (bei einer Übertragung zwischen diesen nicht erforderlichAWS-Services).
- Erstellen Sie einen Quell- und einen Zielspeicherort.
- Erstellen Sie eine Aufgabe.
- Führen Sie die Aufgabe aus, um Dateien von der Quelle zum Ziel zu übertragen.

Weitere Informationen finden Sie unter 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 DataSyncBenutzerhandbuch.
- Stellen Sie Ihren Agenten auf Amazon EC2 bereit

Überwachung von Amazon FSx for Lustre

Sie können die folgenden automatisierten Tools zur Überwachung von Amazon FSx for Lustre verwenden und auftretende Probleme melden:

- -Überwachung mit Amazon CloudWatch — CloudWatch erfasst und verarbeitet Sie Rohdaten von Amazon FSx for Lustre in lesbare Metriken, bei denen es sich nahezu um Echtzeitdaten handelt. Sie können einen CloudWatch -Alarm erstellen, der eine Amazon SNS SNS-Nachricht sendet, sobald sich der Status des Alarms ändert.
- Überwachung mit Lustre-Logging — 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 Sie CloudTrail Protokolldateien in Echtzeit, indem Sie sie an die CloudWatch Logs senden, schreiben Sie Anwendungen zur Protokollverarbeitung in Java und vergewissern Sie sich, dass nach der Lieferung bis keine Änderungen an den Protokolldaten vorgenommen wurden CloudTrail.

Themen

Überwachung mit Amazon CloudWatch

Sie können Ihre Dateisysteme mit Amazon CloudWatch überwachen. Dabei werden Rohdaten von Amazon FSx for Lustre gesammelt und in lesbare Metriken verarbeitet, bei denen es sich nahezu um Echtzeitdaten handelt. Diese -Statistiken werden für einen Zeitraum von 15 Monaten vorgehalten, damit Sie auf Verlaufsinformationen zugreifen besser feststellen können, wie die Webanwendung oder der Service ausgeführt wird. Standardmäßig werden die Metrikdaten von Amazon FSx for Lustre-Metrikdaten in Abständen von 1 Minute automatisch CloudWatch an gesendet. Weitere Informationen finden Sie CloudWatch unter Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

CloudWatch Metriken werden als unformatierte Bytes gemeldet. Bytes werden nicht auf eine Dezimalzahl oder ein binäres Vielfaches der Einheit gerundet.

Dateismet

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`Sum` Statistik verwenden. Beachten Sie, dass die Dateiserver hinter Ihren FSx for Lustre-Dateisystemen auf mehrere Festplatten verteilt sind.

Metrik	Beschreibung
`DataReadBytes`	Die Anzahl der Byte für Dateisystem-Lesevorgänge. Die`Sum` -Statistik enthält die Gesamtzahl der Byte, die während des Zeitraums mit Lesevorgängen verknüpft ist. Die`Minimum` Statistik ist die Mindestanzahl von Byte, die Leseoperationen auf einer einzelnen Festplatte zugeordnet sind. Die`Maximum` Statistik gibt die maximale Anzahl von Bytes an, die Leseoperationen auf der Festplatte zugeordne t sind. Die`Average` Statistik ist die durchschnittliche Anzahl von Byte, die Lesevorgängen pro Festplatte zugeordnet sind. Die`SampleCount` Statistik gibt die Anzahl der Festplatten an. Zum Berechnen des durchschnittlichen Durchsatzes (Byte pro Sekunde) für einen Zeitraum dividieren Sie die`Sum` -Statistik durch die Anzahl der Sekunden im Zeitraum. Einheiten: • Byte für `Sum`, `Minimum`, `Maximum` und `Average`. • Anzahl für `SampleCount` . Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCou nt`
`DataWriteBytes`	Die Anzahl der Byte für Dateisystem-Schreibvorgänge. Die `Sum`-Statistik ist die Gesamtzahl von Byte, die mit den Schreibop erationen verknüpft sind. Die`Minimum` Statistik ist die Mindestanzahl von Byte, die Schreibvorgängen auf einer einzelnen Festplatte zugeordne t sind. Die`Maximum` Statistik gibt die maximale Anzahl von Bytes an,

Metrik	Beschreibung
	die Schreibvorgängen auf der Festplatte zugeordnet sind. Die`Average` Statistik gibt die durchschnittliche Anzahl von Bytes an, die Schreibvo rgängen pro Festplatte zugeordnet sind. Die`SampleCount` Statistik gibt die Anzahl der Festplatten an. Zum Berechnen des durchschnittlichen Durchsatzes (Byte pro Sekunde) für einen Zeitraum dividieren Sie die`Sum` -Statistik durch die Anzahl der Sekunden im Zeitraum. Einheiten: • Byte für `Sum`, `Minimum`, `Maximum` und `Average`. • Anzahl für `SampleCount` . Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCou nt`

Metrik	Beschreibung
DataReadOperations	Die Anzahl der Lesevorgänge. DieSum -Statistik enthält die Gesamtzahl der Lesevorgänge. DieMinimum Statistik gibt die Mindestanzahl von Lesevorgängen auf einer einzelnen Festplatte an. DieMaximum Statistik gibt die maximale Anzahl von Lesevorgängen auf der Festplatte an. DieAverage -Statistik enthält die durchschnittliche Anzahl von Lesevorgängen pro Festplatte. DieSampleCount Statistik gibt die Anzahl der Festplatten an. Zum Berechnen der durchschnittlichen Anzahl von Leseoperationen (Operationen pro Sekunde) für einen Zeitraum dividieren Sie dieSum -Statistik durch die Anzahl der Sekunden im Zeitraum. Einheiten: • Byte für Sum, Minimum, Maximum und Average. • Anzahl für SampleCount . Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCount

Metrik	Beschreibung
`DataWrite Operations`	Die Anzahl der Schreiboperationen. Die`Sum` -Statistik enthält die Gesamtzahl der Schreibvorgänge. 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 enthält die durchschnittliche Anzahl von Schreibvorgänge pro Festplatte. Die`SampleCount` Statistik gibt die Anzahl der Festplatten an. Zum Berechnen der durchschnittlichen Anzahl von Schreiboperationen (Operationen pro Sekunde) für einen Zeitraum dividieren Sie die`Sum` -Statistik durch die Anzahl der Sekunden im Zeitraum. Einheiten: • Byte für `Sum`, `Minimum`, `Maximum` und `Average`. • Anzahl für `SampleCount` . Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Metrik	Beschreibung
`MetadataOperations`	Die Anzahl der Metadatenvorgänge. Die`Sum` Statistik ist die Anzahl der Metadatenoperationen. Die`Minimum` Statistik ist die Mindestanzahl von Metadatenoperationen pro Festplatte. Die`Maximum` Statistik gibt die maximale Anzahl von Metadatenoperationen pro Festplatte an. Die`Average` Statistik ist die durchschnittliche Anzahl von Metadatenoperationen pro Festplatte. Die`SampleCount` Statistik gibt die Anzahl der Festplatten an. Zum Berechnen der durchschnittlichen Anzahl von Metadatenoperationen (Operationen pro Sekunde) für einen Zeitraum dividieren Sie die`Sum` -Statistik durch die Anzahl der Sekunden im Zeitraum. Einheiten: • Zähle für`Sum`,`Minimum`,`Maximum`,`Average`, und`SampleCount` . Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Metrik	Beschreibung
`FreeDataStorageCapacity`	Die Menge der verfügbaren Speicherkapazität. Die`Sum` Statistik ist die Gesamtzahl der im Dateisystem verfügbaren Byte. Die`Minimum` Statistik gibt die Gesamtzahl der Byte an, die auf der vollen Festplatte verfügbar sind. Die`Maximum` Statistik ist die Gesamtzahl der auf der Festplatte verfügbaren Byte mit dem größten verfügbaren Speicherplatz. Die`Average` Statistik gibt die durchschnittliche Anzahl der pro Festplatte verfügbaren Byte an. Die`SampleCount` Statistik gibt die Anzahl der Festplatten an. Einheiten: • Bytes für`Sum`,`Minimum`,`Maximum`. • Anzahl für `SampleCount` . Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`
`LogicalDiskUsage`	Die Menge der gespeicherten logischen Daten (unkomprimiert). Die`Sum` Statistik ist die Gesamtzahl der im Dateisystem gespeicherten logischen Byte. Die`Minimum` Statistik ist die kleinste Anzahl logischer Byte, 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 ist die durchschnittliche Anzahl der pro Festplatte gespeicherten logischen Byte. Die`SampleCount` Statistik gibt die Anzahl der Festplatten an. Einheiten: • Bytes für`Sum`,`Minimum`,`Maximum`. • Anzahl für `SampleCount` . Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Metrik	Beschreibung
PhysicalDiskUsage	Die Menge des Speichers, der physisch von Dateisystemdaten belegt wird (komprimiert). DieSum Statistik gibt die Gesamtzahl der Byte an, die auf Festplatten im Dateisystem belegt sind. DieMinimum Statistik gibt die Gesamtzahl der Bytes an, die auf der leersten Festplatte belegt sind. DieMaximum Statistik gibt die Gesamtzahl der Bytes an, die auf der vollständigsten Festplatte belegt sind. DieAverage Statistik gibt die durchschnittliche Anzahl der pro Festplatte belegten Byte an. DieSampleCount Statistik gibt die Anzahl der Festplatten an. Einheiten: • Bytes fürSum,Minimum,Maximum. • Anzahl für SampleCount . Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCount

AutoImport und AutoExport Metriken

FSx for Lustre veröffentlicht die folgendenAutoImport (automatischer Import) undAutoExport (automatischer Export) Metriken imFSx Namespace in CloudWatch. Diese Metriken verwenden Dimensionen, um detailliertere Messungen Ihrer Daten zu ermöglichen. AlleAutoImport undAutoExport Metriken haben diePublisher DimensionenFileSystemId und.

Metrik	Beschreibung
AgeOfOldestQueuedMessage Dimension: AutoExport	Das Alter der ältesten Nachricht in Sekunden, die darauf wartet, exportiert zu werden. DieAverage Statistik ist das Durchschnittsalter der ältesten Nachricht, die darauf wartet, exportiert zu werden. DieMaximum Statistik gibt die maximale Anzahl von Sekunden an, die eine Nachricht in der Exportwarteschlange verbracht hat. DieMinimum Statistik gibt die Mindestan

Metrik	Beschreibung
	zahl von Sekunden an, die eine Nachricht in der Exportwarteschlange verbracht hat. Ein Wert gleich 0 deutet darauf hin, dass keine Nachricht en darauf warten, exportiert zu werden. Einheiten: Sekunden Gültige Statistiken: `Average`, `Minimum`, `Maximum`
`RepositoryRenameOperations` Dimension: `AutoExport`	Die Anzahl der Umbenennungen, die das Dateisystem als Reaktion auf eine größere Verzeichnisumbenennung verarbeitet. Die`Sum` Statistik gibt die Gesamtzahl der Umbenennungsvorgänge an, die aus einer Verzeichnisumbenennung resultieren. Die`Average` Statistik ist die durchschnittliche Anzahl von Umbenennungsvorgängen für das Dateisystem. Die`Maximum` Statistik gibt die maximale Anzahl von Umbenennungsvorgängen an, die mit einer Verzeichnisumbenen nung im Dateisystem verbunden sind. Die`Minimum` Statistik gibt die Mindestanzahl von Umbenennungen an, die einer Verzeichnisumbenen nung im Dateisystem zugeordnet sind. Einheiten: Anzahl Gültige Statistiken:`Sum`,`Minimum`,`Maximum`,`Average`
`AgeOfOldestQueuedMessage` Dimension: `AutoImport`	Das Alter der ältesten Nachricht in Sekunden, die darauf wartet, importiert zu werden. Die`Average` Statistik ist das Durchschnittsalter der ältesten Nachricht , die darauf wartet, importiert zu werden. Die`Maximum` Statistik gibt die maximale Anzahl von Sekunden an, die eine Nachricht in der Importwarteschlange verbracht hat. Die`Minimum` Statistik gibt an, wie viele Sekunden eine Nachricht mindestens in der Importwarteschlange verbracht hat. Ein Wert gleich 0 deutet darauf hin, dass keine Nachricht en darauf warten, importiert zu werden. Einheiten: Sekunden Gültige Statistiken: `Average`, `Minimum`, `Maximum`

Amazon FSx for Lustre-Abmessungen

Die Metriken von Amazon FSx for Lustre-Metriken verwenden den`FSx` Namespace und stellen Sie Metriken für die Dimension bereit`FileSystemId`. Die ID eines Dateisystems kann mit dem`describe-file-systems`AWS CLI Befehl ermittelt werden und hat die Form *`fs-01234567890123456`*.

Eine zusätzliche Dimension,`Publisher`, ist in CloudWatch undAWS CLI für die`AutoImport` und`AutoImport` -Metriken verfügbar, um anzugeben, 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 häufige Verwendungszwecke für die Metriken. Es handelt sich dabei um Vorschläge für den Einstieg und nicht um eine umfassende Liste.

Wie ermittle ich...	Relevante Metriken (Dimension | Metrik)
Der Durchsatz meines Dateisystems?	SUMME (DataReadBytes + DataWriteBytes) /Zeitraum (in Sekunden)
Die IOPS meines Dateisystems?	Gesamt-IOPS = SUMME (DataReadOperations DataWriteOperations + MetadataOperations) /Zeitraum (in Sekunden)
Die Datenkomp rimierungsrate meines Dateisystems?	SUMME (LogicalDiskUsage)/SUMME (PhysicalDiskUsage)
Wenn Updates für mein Dateisystem mit meinem S3-Bucket synchronisiert wurden?	AutoExport | AgeOfOldestQueuedMessage
Wenn Updates für meinen S3-Bucket mit meinem Dateisyst	AutoImport | AgeOfOldestQueuedMessage

Wie ermittle ich...	Relevante Metriken (Dimension | Metrik)
em synchronisiert wurden?	

Metrische Mathematik: Datenkomprimierungsrate

Mithilfe von Metrikberechnungen können Sie mehrere CloudWatch Metriken abfragen und mathematische Ausdrücke verwenden, um neue Zeitreihen basierend auf diesen Metriken zu erstellen. Sie können die resultierenden Zeitreihen in der CloudWatch -Konsole visualisieren und zu Dashboards hinzufügen. Weitere Informationen zur metrischen Mathematik finden Sie unter Verwenden metrischer Mathematik im CloudWatch Amazon-Benutzerhandbuch.

Dieser metrikberechnete 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 lautet: Summe von`LogicalDiskUsage` ÷ Summe von`PhysicalDiskUsage`

Daraus ergeben sich folgende CloudWatch Metrikinformationen.

ID	Verwendbare Metrik	Statistik	Intervall
m1	`LogicalDiskUsage`	Summe	1 Minute
m2	`PhysicalDiskUsage`	Summe	1 Minute

ID und Ausdruck Ihrer Metrikberechnung lauten wie folgt.

ID	Expression
e1	`m1/m2`

e1ist das Datenkomprimierungsverhältnis.

Zugriff auf CloudWatch Metriken

Sie können sich die Metriken von Amazon FSx for Lustre CloudWatch auf viele Arten anzeigen lassen. 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 Sie Sie Sie mit der 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 Dimensionen zu filtern, wählen Sie FileSystemId.

So greifen Sie auf Metriken aus dem AWS CLI zu:

- 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 CloudWatch Amazon-API-Referenz.

Erstellen von CloudWatch Alarmen zur Überwachung von Amazon FSx for Lustre

Sie können einen CloudWatch -Alarm erstellen, der eine Amazon SNS SNS-Nachricht sendet, sobald 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.

Alarme rufen nur Aktionen für nachhaltige Statusänderungen auf. CloudWatch -Alarme rufen keine Aktionen auf, nur weil sie einen bestimmten Status aufweisen. Der Status muss geändert und für eine bestimmte Anzahl an Zeiträumen aufrechterhalten worden sein.

Im folgenden Verfahren wird beschrieben, wie Sie Alarme für Amazon FSx for Lustre erstellen.

So richten Sie Sie mit der CloudWatch -Konsole Alarme ein

1. Melden Sie sich bei der anAWS Management Console und öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie Create Alarm (Alarm erstellen) aus. Dadurch wird der Assistent zum Erstellen von Alarmen gestartet.
3. Wählen Sie FSx Metriken und durchblättern Sie die Amazon FSx for Lustre-Metriken, bis Sie die Metrik finden, für die Sie einen Alarm setzen möchten. Um in diesem Dialogfeld nur die Amazon FSx for Lustre-Metriken anzuzeigen, suchen Sie nach der Dateisystem-ID Ihres Dateisystems. Wählen Sie die Metrik, auf der ein Alarm erstellt werden soll, und wählen Sie Weiter.
4. Wählen Sie im Abschnitt Bedingungen die Bedingungen aus, die Sie für den Alarm wünschen, und klicken Sie auf Weiter.

   > **Note**
   >
   > Metriken dürfen während der Dateisystemwartung nicht veröffentlicht werden. Um unnötige und irreführende Änderungen der Alarmbedingungen zu verhindern und Ihre Alarme so zu konfigurieren, dass sie gegen fehlende Datenpunkte resistent sind, finden Sie im CloudWatch Amazon-Benutzerhandbuch unter Konfiguration, wie CloudWatch Alarme mit fehlenden Daten umgehen.

5. Wenn Ihnen eine E-Mail-Nachricht senden CloudWatch soll, wenn der Alarmstatus erreicht ist, wählen Sie im Feld Wann immer dieser Alarm ausgegeben wird: die Option Status lautet ALARM aus. 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 für future Alarme in dem Feld.

   > **Note**
   >
   > Wenn Sie Thema erstellen verwenden, um ein neues Amazon SNS SNS-Thema zu erstellen, vergewissern Sie sich, dass die E-Mail Adressen überprüft werden, 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. Zeigen Sie eine Vorschau des Alarms an, den Sie im Bereich Alarmvorschau erstellen möchten. Wenn es wie erwartet erscheint, wählen Sie Alarm erstellen.

So richten Sie mit der einen Alarm ei AWS CLI

- Rufen Sie die folgende Seite auf `put-metric-alarm`. Weitere Informationen finden Sie in der AWS CLI-Befehlsreferenz.

So richten Sie mit der CloudWatch -API einen Alarm ein

- Rufen Sie die folgende Seite auf `PutMetricAlarm`. Weitere Informationen finden Sie unter Amazon CloudWatch API-Referenz.

Protokollieren mit Amazon CloudWatch Logs

FSx for Lustre unterstützt die Protokollierung von Fehler- und Warnereignissen für Daten-Repositorys, die Ihrem Dateisystem zugeordnet sind, in Amazon CloudWatch Logs.

> **Note**
>
> Die Protokollierung mit Amazon CloudWatch Logs ist nur auf Dateisystemen von Amazon FSx für Lustre verfügbar, die am 30. November 2021 nach 15 Uhr PST erstellt wurden.

Themen

Übersicht über die Protokollierung

Wenn Sie Daten-Repositorys mit Ihrem FSx for Lustre-Dateisystem verknüpft haben, können Sie die Protokollierung von Daten-Repository-Ereignissen in Amazon CloudWatch Logs aktivieren. Fehler- und Warnereignisse können von den folgenden Daten-Repository-Operationen protokolliert werden:

- Automatischer Export
- Daten-Repository-Aufgaben

Weitere Informationen zu diesen Operationen und zur Verknüpfung mit Daten-Repositorys 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**
>
> Wir empfehlen dringend, Protokolle für Dateisysteme zu aktivieren, denen eine beliebige kritische Funktionalität zugeordnet ist.

Protokollziele

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 einen Protokollstream für Ihr Dateisystem innerhalb dieser Protokollgruppe. CloudWatch Mit Logs können Sie Audit-Ereignisprotokolle in der Amazon CloudWatch-Konsole speichern, anzeigen und durchsuchen, Abfragen für die Protokolle mit CloudWatch Logs Insights ausführen und Alarme oder Lambda-Funktionen auslösen CloudWatch.

Sie wählen das Protokollziel aus, wenn Sie Ihr FSx for Lustre-Dateisystem erstellen, oder danach, indem Sie es aktualisieren. Weitere Informationen finden Sie unter Verwalten der Protokollierung.

Standardmäßig erstellt und verwendet Amazon FSx eine Standard- CloudWatch Protokollgruppe in Ihrem Konto als Ereignisprotokollziel. Wenn Sie eine benutzerdefinierte CloudWatch Logs-Protokollgruppe als Ereignisprotokollziel verwenden möchten, sind hier die Anforderungen für den Namen und den Speicherort des Ereignisprotokollziels aufgeführt:

- Der Name der CloudWatch Protokollgruppe muss mit dem `/aws/fsx/` Präfix beginnen.
- Wenn Sie beim Erstellen oder Aktualisieren eines Dateisystems in der Konsole keine CloudWatch Protokollgruppe haben, kann Amazon FSx for Lustre einen Standardprotokollstream in der CloudWatch `/aws/fsx/lustre`Protokollgruppe erstellen und verwenden. Der Protokollstream wird im Format erstellt `datarepo_`*`file_system_id`* (z. B. `datarepo_fs-0123456789abcdef0`).
- Wenn Sie die Standardprotokollgruppe nicht verwenden möchten, können Sie mit der Konfigurations-Benutzeroberfläche eine CloudWatch Protokollprotokollgruppe erstellen, wenn Sie Ihr Dateisystem in der Konsole erstellen oder aktualisieren.
- Die CloudWatch Protokollgruppe muss sich in derselben AWS Partition AWS-Region, und AWS-Konto wie Ihr Dateisystem von Amazon FSx für Lustre befinden.

Sie können das Ereignisprotokollziel jederzeit ändern. Wenn Sie dies tun, werden neue Ereignisprotokolle nur an das neue Ziel gesendet.

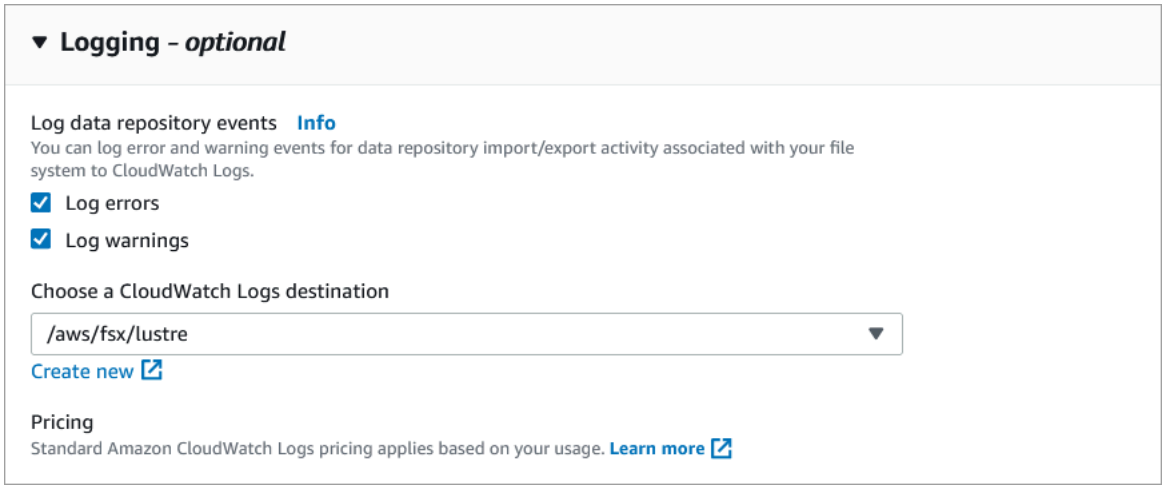
Verwalten der Protokollierung

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 über die Amazon-FSx-Konsole erstellen. Die Protokollierung ist jedoch standardmäßig deaktiviert, wenn Sie ein Dateisystem mit der AWS CLI oder Amazon-FSx-API erstellen.

Auf 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 AWS CLI oder der Amazon-FSx-API ausführen.

So aktivieren Sie die Protokollierung beim Erstellen eines Dateisystems (Konsole)

1. Öffnen Sie die Amazon-FSx-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie den Anweisungen zum Erstellen eines neuen Dateisystems, das unter Erstellen Sie Ihr FSx for Lustre-Dateisystem im Abschnitt Erste Schritte beschrieben wird.
3. Öffnen Sie den Abschnitt Protokollierung – optional. Die Protokollierung ist standardmäßig aktiviert.



4. Fahren Sie mit dem nächsten Abschnitt des Dateisystem-Erstellungsassistenten 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 mit der -CreateFileSystemOperation, 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.

So ändern Sie die Protokollierungskonfiguration (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 aus.
5. Ändern Sie im Dialogfeld Protokollierungskonfiguration aktualisieren die gewünschten Einstellungen.

a. Wählen Sie Protokollfehler, um nur Fehlerereignisse zu protokollieren, oder Protokollwarnungen, um nur Warnereignisse zu protokollieren, oder beides. Die Protokollierung ist deaktiviert, wenn Sie keine Auswahl treffen.

b. Wählen Sie ein vorhandenes CloudWatch Protokollziel aus oder erstellen Sie ein neues Protokollziel.

6. Wählen Sie Speichern.

So ändern Sie die Protokollierungskonfiguration (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 anzeigen, nachdem Amazon FSx mit der Ausgabe begonnen hat. Sie können die Protokolle wie folgt anzeigen:

- Sie können Protokolle anzeigen, indem Sie die Amazon- CloudWatch Konsole aufrufen und die Protokollgruppe und den Protokollstream auswählen, an die Ihre Ereignisprotokolle gesendet werden. Weitere Informationen finden Sie unter Anzeigen von Protokolldaten, die an - CloudWatch Protokolle gesendet wurden im Amazon- CloudWatch Logs-Benutzerhandbuch.
- Sie können CloudWatch Logs Insights verwenden, um interaktiv Ihre Protokolldaten zu durchsuchen 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.

Weitere Informationen zu den Fehlerursachen finden Sie unter Datenrepository-Ereignisprotokolle.

Protokollieren von FSx for Lustre Lustre-API-Aufrufen mitAWS CloudTrail

Amazon FSx for Lustre ist integriert inAWS CloudTraileinen -Service, der die Aktionen eines Benutzers, einer Rolle oder einesAWS-Service in Amazon FSx for Lustre. CloudTrail erfasst alle API-Aufrufe für Amazon FSx for Lustre als Ereignisse. Zu erfassten Aufrufen gehören Aufrufe von der Amazon FSx for Lustre Lustre-Konsole und Codeaufrufe an Amazon FSx for Lustre Lustre-API-Operationen.

Wenn Sie einen Trail erstellen, aktivieren Sie die kontinuierliche Bereitstellung von CloudTrail Ereignisse in einem Amazon S3 S3-Bucket, einschließlich Ereignissen für Amazon FSx for Lustre. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse in der CloudTrail -Konsole inEreignisverlauf desaus. Mit den von CloudTrail erfassten Informationen können Sie ermitteln, welche Anforderung 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 zu CloudTrail finden Sie im AWS CloudTrail-Benutzerhandbuch.

Informationen zu Amazon FSx for Lustre Lustre-Informationen in CloudTrail

CloudTrail wird beim Erstellen Ihres AWS-Kontos für Sie aktiviert. Erfolgen API-Aktivitäten in Amazon FSx for Lustre, werden diese als CloudTrail Event zusammen mit anderenAWS-Service-Ereignisse inEreignisverlauf desaus. Sie können die neusten Ereignisse in Ihr AWS-Konto downloaden und dort suchen und anzeigen. Weitere Informationen finden Sie unterAnzeigen von -Ereignissen mit CloudTrail Ereignisverlauf desaus.

Für eine kontinuierliche Aufzeichnung von Ereignissen in IhremAWSErstellen Sie einen Trail, einschließlich Ereignissen für Amazon FSx for Lustre. EINWanderwegaktiviert CloudTrail um Protokolldateien an einen Amazon S3 S3-Bucket bereitzustellen. Wenn Sie einen Trail in der Konsole anlegen, gilt dieser für alle AWS-Regionen. Der Trail protokolliert Ereignisse aus allen AWS-Regionen in der AWS-Partition und stellt die Protokolldateien in dem Amazon-S3-Bucket bereit, den Sie angeben. Darüber hinaus können Sie andereAWS-Services zur weiteren Analyse und Umsetzung der in erfassten Ereignisdaten CloudTrail protokolliert. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail-Benutzerhandbuch:

- Übersicht zum Erstellen eines Trails
- Von CloudTrail unterstützte Dienste und Integrationen

- Konfigurieren von Amazon-SNS-Benachrichtigungen für CloudTrail
- Empfangen CloudTrail Protokolldateien aus mehreren RegionenundEmpfangen von CloudTrail-Protokolldateien aus mehreren Konten

Alle Amazon FSx for LustreAPI-Aufrufewerden von CloudTrail protokolliert. Zum Beispiel werden durch Aufrufe`CreateFileSystem`und`TagResource`Operationen generieren Einträge im CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Anhand der Identitätsinformationen zur Benutzeridentität können Sie Folgendes bestimmen:

- Ob die Anfrage mit Stammbenutzer- oder AWS Identity and Access Management (IAM)-Anmeldeinformationen ausgeführt wurde.
- Ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer ausgeführt wurde.
- Ob die Anforderung aus einem anderen AWS-Service gesendet wurde

Weitere Informationen finden Sie unter CloudTrail-userIdentity-Element im AWS CloudTrail-CloudTrail-Benutzerhandbuch.

Verstehen von Amazon FSx for Lustre Lustre-Protokolldateieinträgen

EINWanderwegist eine Konfiguration, durch die Ereignisse als Protokolldateien an den von Ihnen angegebenen Amazon-S3-Bucket übermittelt werden. CloudTrail -Protokolldateien können einen oder mehrere Einträge enthalten. Importieren in &S3;Veranstaltungstellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält unter anderem Informationen über die angeforderte Aktion, das Datum und die Uhrzeit der Aktion sowie über die Anforderungsparameter. CloudTrail -Protokolleinträge sind kein geordnetes Stacktrace der öffentlichen API-Aufrufe und erscheinen daher nicht in einer bestimmten Reihenfolge.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die`TagResource`-Operation, wenn ein Tag für das 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, wenn ein Tag für das Dateisystem von der Konsole aus 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

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 Sicherheitsservices 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

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

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. Bei diesem KMS-Schlüssel kann es sich um einen der beiden folgenden Typen handeln:

- 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: GenerateDataKeyWithoutPlaintext — (Erforderlich) Gibt einen mit einem KMS-Schlüssel verschlüsselten Datenverschlüsselungsschlüssel zurück. Diese Berechtigung ist in der Standardschlüsselrichtlinie unter kms: GenerateDataKey * enthalten.
- kms: CreateGrant — (Erforderlich) Fügt einem Schlüssel einen Zuschuss 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 Schlüsselaliase 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 für Linux-Instances.

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)	✓	✓	✓

AWS-Region	Scratch_2	Persistent_1	Persistent_2
USA Ost (Nord-Virginia)	✓	✓	✓
USA West (Oregon)	✓	✓	✓
USA West (Nordkalifornien) *	✓	✓	
USA West (Los Angeles)	✓	✓	
AWS GovCloud (US-Ost) *	✓	✓	
AWS GovCloud (US-West)	✓	✓	
Kanada (Zentral) *	✓	✓	✓
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) *	✓	✓	✓
Israel (Tel Aviv) *		✓	

AWS-Region	Scratch_2	Persistent_1	Persistent_2
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 für die 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.

Identity and Access Management für Amazon FSx for Lustre

AWS Identity and Access Management (IAM) ist ein AWS-Service, mit dem Administratoren den Zugriff auf AWS-Ressourcen sicher steuern können. IAM-Administratoren steuern, wer für die Nutzung von Amazon-FSx-Ressourcen authentifiziert (angemeldet) und autorisiert (im Besitz von Berechtigungen) werden kann. IAM ist ein AWS-Service, den Sie ohne zusätzliche Kosten verwenden können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, unterscheidet sich je nach Ihrer Arbeit in Amazon FSx .

Service-Benutzer – Wenn Sie den Amazon-FSx-Service zur Ausführung von Aufgaben verwenden, stellt Ihnen Ihr Administrator die Anmeldeinformationen und Berechtigungen bereit, die Sie benötigen.

Wenn Sie für Ihre Arbeit weitere Amazon-FSx-Funktionen ausführen, benötigen Sie möglicherweise zusätzliche Berechtigungen. Wenn Sie die Featuresweise der Zugriffskontrolle nachvollziehen, wissen Sie bereits, welche Berechtigungen Sie von Ihrem Administrator anzufordern müssen. Wenn Sie nicht auf ein Feature in Amazon FSx zugreifen können, finden Sie weitere Informationen unter Fehlerbehebung für Identität und Zugriff auf Amazon FSx for Lustre.

Service-Administrator – Wenn Sie in Ihrem Unternehmen für Amazon-FSx-Ressourcen verantwortlich sind, haben Sie wahrscheinlich vollständigen Zugriff auf Amazon FSx . Ihre Aufgabe besteht darin, zu bestimmen, auf welche Amazon-FSx-Funktionen und -Ressourcen Ihre Service-Benutzer 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 dazu, wie Ihr Unternehmen IAM mit Amazon FSx verwenden kann, finden Sie unter Funktionsweise von Amazon FSx for Lustre mit IAM.

IAM-Administrator – Wenn Sie als IAM-Administrator fungieren, sollten Sie Einzelheiten dazu kennen, wie Sie Richtlinien zur Verwaltung des Zugriffs auf Amazon FSx verfassen können. 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, wie Sie sich mit Ihren Anmeldeinformationen bei AWS anmelden. Die Authentifizierung (Anmeldung bei AWS) muss als Root-Benutzer des AWS-Kontos, als IAM-Benutzer oder durch Übernahme einer IAM-Rolle erfolgen.

Sie können sich bei AWS als Verbundidentität mit Anmeldeinformationen anmelden, die über eine Identitätsquelle bereitgestellt werden. Benutzer von AWS IAM Identity Center (IAM Identity Center), die Single-Sign-on-Authentifizierung Ihres Unternehmens und Anmeldeinformationen für Google oder Facebook sind Beispiele für Verbundidentitäten. Wenn Sie sich als Verbundidentität anmelden, hat der Administrator vorher mithilfe von IAM-Rollen einen Identitätsverbund eingerichtet. Wenn Sie auf AWS mithilfe des Verbunds zugreifen, übernehmen Sie indirekt eine Rolle.

Je nachdem, welcher Benutzertyp Sie sind, können Sie sich bei der AWS Management Console oder beim AWS-Zugriffsportal anmelden. Weitere Informationen zum Anmelden bei AWS finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch von AWS-Anmeldung.

Bei programmgesteuertem Zugriff auf AWS bietet AWS ein Software Development Kit (SDK) und eine Command Line Interface (CLI, Befehlszeilenschnittstelle) zum kryptographischen Signieren Ihrer Anfragen mit Ihren Anmeldeinformationen. Wenn Sie keine AWS-Tools verwenden, müssen

Sie Anforderungen selbst signieren. Weitere Informationen zur Verwendung der empfohlenen Methode zum eigenen Signieren von Anforderungen finden Sie unter Signieren von AWS-API-Anforderungen im IAM-Benutzerhandbuch.

Unabhängig von der verwendeten Authentifizierungsmethode müssen Sie möglicherweise zusätzliche Sicherheitsinformationen angeben. AWS empfiehlt beispielsweise die Verwendung von Multi-Faktor Authentifizierung (MFA), um die Sicherheit Ihres Kontos zu verbessern. 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 AWS-Konto neu erstellen, beginnen Sie mit einer Anmeldeidentität, die vollständigen Zugriff auf alle AWS-Services und Ressourcen des Kontos hat. Diese Identität wird als AWS-Konto-Root-Benutzer bezeichnet. Für den Zugriff auf den Root-Benutzer müssen Sie sich mit der E-Mail-Adresse und dem Passwort anmelden, die zur Erstellung des Kontos verwendet wurden. 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 empfiehlt es sich, menschliche Benutzer, einschließlich Benutzer, die Administratorzugriff benötigen, aufzufordern, den Verbund mit einem Identitätsanbieter zu verwenden, um auf AWS-Services mit temporären Anmeldeinformationen zuzugreifen.

Eine Verbundidentität ist ein Benutzer aus dem Benutzerverzeichnis Ihres Unternehmens, ein Web Identity Provider, AWS Directory Service, das Identity-Center-Verzeichnis oder jeder Benutzer, der mit Anmeldeinformationen, die über eine Identitätsquelle bereitgestellt werden, auf AWS-Services zugreift. Wenn Verbundidentitäten auf AWS-Konten zugreifen, 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 im IAM Identity Center erstellen oder Sie können eine Verbindung mit einer Gruppe von Benutzern und Gruppen in Ihrer eigenen Identitätsquelle herstellen und synchronisieren, um sie in allen AWS-Konten und 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 in Ihrem AWS-Konto mit bestimmten Berechtigungen für eine einzelne Person oder eine einzelne Anwendung. 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 in Ihrem AWS-Konto mit spezifischen Berechtigungen. Sie ist einem IAM-Benutzer vergleichbar, ist aber nicht mit einer bestimmten Person verknüpft. Sie können vorübergehend eine IAM-Rolle in der AWS Management Console übernehmen, indem Sie Rollen wechseln. Sie können eine Rolle annehmen, 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. In einigen AWS-Services können Sie jedoch eine Richtlinie direkt an eine Ressource anfügen (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 Features 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 Servicerolle oder mit einer serviceverknüpften Rolle tun.
  - Forward access sessions (FAS) – Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. In diesem Fall müssen Sie über Berechtigungen zum Ausführen beider Aktionen verfügen. Einzelheiten zu den Richtlinien für FAS-Anfragen finden Sie unter Zugriffssitzungen weiterleiten.
  - Servicerolle: Eine Servicerolle ist eine IAM-Rolle, die ein Service übernimmt, 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.

  - Serviceverknüpfte Rolle: Eine serviceverknüpfte Rolle ist ein Typ von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. Ein IAM-Administrator kann die Berechtigungen für serviceverbundene Rollen anzeigen, aber nicht bearbeiten.
- Anwendungen in Amazon EC2: Sie können eine IAM-Rolle verwenden, um temporäre Anmeldeinformationen für Anwendungen zu verwalten, die auf einer EC2-Instance ausgeführt werden und AWS CLI- oder AWS-API-Anforderungen durchführen. Das ist eher zu empfehlen, als Zugriffsschlüssel innerhalb der EC2-Instance zu speichern. Erstellen Sie ein Instance-Profil, das an die Instance angefügt ist, um eine AWS-Rolle einer EC2-Instance zuzuweisen und die Rolle für sämtliche Anwendungen der Instance bereitzustellen. 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

Für die Zugriffssteuerung in AWS erstellen Sie Richtlinien und weisen diese den AWS-Identitäten oder -Ressourcen zu. Eine Richtlinie ist ein Objekt in AWS, das, wenn es einer Identität oder Ressource zugeordnet wird, deren Berechtigungen definiert. AWS wertet diese Richtlinien aus, wenn ein Prinzipal (Benutzer, Root-Benutzer oder Rollensitzung) eine Anforderung stellt. Berechtigungen in den Richtlinien bestimmen, ob die Anforderung zugelassen oder abgelehnt wird. Die meisten Richtlinien werden in 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 festlegen, wer zum Zugriff auf was berechtigt ist. 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 Benutzerinformationen über die AWS Management Console, die AWS CLI oder die 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 AWS-Konto anfügen können. Verwaltete Richtlinien umfassen von AWS verwaltete und von 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. Prinzipale können Konten, Benutzer, Rollen, Verbundbenutzer oder AWS-Services umfassen.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können verwaltete AWS-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, AWS WAF und Amazon VPC sind Beispiele für Dienste, die ACLs unterstützen. 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 häufig verwendete 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-Kontrollrichtlinien (SCPs) – SCPs sind JSON-Richtlinien, die die maximalen Berechtigungen für eine Organisation oder Organisationseinheit (OE) in AWS Organizations angeben. AWS Organizations ist ein Dienst für die Gruppierung und zentrale Verwaltung mehrerer AWS-Konten Ihres Unternehmens. Wenn Sie innerhalb einer Organisation alle Features aktivieren, können Sie Service-Kontrollrichtlinien (SCPs) auf alle oder einzelne Ihrer Konten anwenden. SCPs schränken Berechtigungen für Entitäten in Mitgliedskonten einschließlich des jeweiligen Root-Benutzer des AWS-Kontos ein. 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 dazu, wie AWS die Zulässigkeit einer Anforderung ermittelt, wenn mehrere Richtlinientypen beteiligt sind, finden Sie unter Logik für die Richtlinienauswertung im IAM-Benutzerhandbuch.

Funktionsweise von Amazon FSx for Lustre mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon FSx zu verwalten, erfahren Sie, welche IAM-Funktionen Sie mit Amazon FSx verwenden können.

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
Forward Access Sessions (FAS)	Ja
Servicerollen	Nein
Serviceverknüpfte Rollen	Ja

Einen Überblick über das Zusammenwirken von Amazon FSx und anderen -AWSServices mit den meisten IAM-Funktionen finden Sie unter -AWSServices, die mit IAM funktionieren im IAM-Benutzerhandbuch.

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 Amazon-FSx-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Lustre.

Ressourcenbasierte Richtlinien in Amazon FSx

Unterstützt ressourcenbasierte Richtlinien	Nein

Richtlinienaktionen für Amazon FSx

Unterstützt Richtlinienaktionen	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. 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 die zugehörige AWS-API-Operation. Es gibt einige Ausnahmen, z. B. Aktionen, die nur mit Genehmigung durchgeführt werden können und für die es keine passende API-Operation 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-Autorisierungs-Referenz.

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 Amazon-FSx-Richtlinien 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 festlegen, wer zum Zugriff auf was berechtigt ist. 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-Autorisierungs-Referenz. Informationen zu den Aktionen, mit denen Sie den ARN einzelner Ressourcen angeben können, finden Sie unter Von Amazon FSx for Lustre definierte Aktionen.

Beispiele für identitätsbasierte Amazon-FSx-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Lustre.

Richtlinienbedingungsschlüssel für Amazon FSx

Unterstützt servicespezifische Richtlini enbedingungsschlüssel	Ja

Administratoren können mithilfe von AWS-JSON-Richtlinien festlegen, wer zum Zugriff auf was berechtigt ist. 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 Bedingungsschlüssel angeben, wertet AWS die Bedingung mittels 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 Bedingungsschlüssel und servicespezifische Bedingungsschlüssel. Eine Liste aller globalen AWS-Bedingungsschlüssel finden Sie unter Globale AWS-Bedingungskontextschlüssel im IAM-Benutzerhandbuch.

Eine Liste der Amazon-FSx-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon FSx for Lustre in der Service-Autorisierungs-Referenz. Informationen dazu, mit welchen Aktionen und Ressourcen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon FSx for Lustre definierte Aktionen.

Beispiele für identitätsbasierte Amazon-FSx-Richtlinien finden Sie unter Beispiele für identitätsbasierte Richtlinien für Amazon FSx for Lustre.

Zugriffssteuerungslisten (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 AWS werden diese Attribute als Tags bezeichnet. Sie können Tags an IAM-Entitäten (Benutzer oder Rollen) und mehrere AWS-Ressourcen anfügen. 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 Bedingungselement 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 Markieren von Amazon-FSx-Ressourcen finden Sie unter Markieren Ihrer Amazon ECX-Ressourcen mit Tags.

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 von von FSx von mit.

Verwenden temporärer Anmeldeinformationen mit Amazon FSx

Unterstützt temporäre Anmeldeinformationen	Ja

Einige AWS-Services Featureieren nicht, wenn Sie sich mit temporären Anmeldeinformationen anmelden. Weitere Informationen, unter anderem darüber, welche AWS-Services mit temporären Anmeldeinformationen arbeiten, finden Sie unter AWS-Services, die mit IAM arbeiten im IAM-Benutzerhandbuch.

Sie verwenden temporäre Anmeldeinformationen, wenn Sie sich mit einer anderen Methode als einem Benutzernamen und einem Passwort bei der AWS Management Console anmelden. Wenn Sie beispielsweise über den Single Sign-On (SSO)-Link Ihres Unternehmens auf AWS zugreifen, erstellt dieser Prozess automatisch temporäre Anmeldeinformationen. 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.

Sie können mithilfe der AWS CLI- oder AWS-API manuell temporäre Anmeldeinformationen erstellen. Sie können dann diese temporären Anmeldeinformationen verwenden, um auf AWS zuzugreifen. AWS empfiehlt, dass Sie temporäre Anmeldeinformationen dynamisch generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Sicherheitsanmeldeinformationen in IAM.

Weiterleiten von Zugriffssitzungen für Amazon FSx

Unterstützt Forward Access Sessions (FAS)	Ja

Wenn Sie einen IAM-Benutzer oder eine IAM-Rolle zum Ausführen von Aktionen in AWS verwenden, gelten Sie als Prinzipal. Bei einigen Services könnte es Aktionen geben, die dann eine andere Aktion in einem anderen Service auslösen. FAS verwendet die Berechtigungen des Prinzipals, der einen AWS-Service aufruft, in Kombination mit der Anforderung an den AWS-Service, Anforderungen an nachgelagerte Services zu stellen. FAS-Anfragen werden nur dann gestellt, wenn ein Service eine Anfrage erhält, die eine Interaktion mit anderen AWS-Services oder -Ressourcen erfordert. 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 könnte die Amazon-FSx-Funktionalität beeinträchtigen. Bearbeiten Sie Servicerollen nur, wenn Amazon FSx dazu Anleitungen gibt.

Serviceverknüpfte Rollen für Amazon FSx

Unterstützt serviceverknüpfte Rollen	Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einem AWS-Service verknüpft ist. Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Serviceverknüpfte Rollen werden in Ihrem AWS-Konto angezeigt und gehören zum Service. 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

Benutzer und Rollen besitzen standardmäßig keine Berechtigungen zum Erstellen oder Ändern von Amazon-FSx-Ressourcen. Sie können auch keine Aufgaben über die AWS Management Console, die AWS Command Line Interface (AWS CLI) oder die 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 Aktionen und Ressourcentypen, die von Amazon FSx definiert werden, einschließlich des Formats der ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FSx for Lustre in der Service-Autorisierungs-Referenz.

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 sie löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Befolgen Sie beim Erstellen oder Bearbeiten identitätsbasierter Richtlinien die folgenden Anleitungen und Empfehlungen:

- Erste Schritte mit AWS-verwaltete Richtlinien und Umstellung auf Berechtigungen mit den geringsten Berechtigungen:Um Ihren Benutzern und Workloads Berechtigungen zu gewähren, verwenden Sie die AWS-verwaltete Richtlinien die Berechtigungen für viele allgemeine Anwendungsfälle gewähren. Sie sind in Ihrem AWS-Konto verfügbar. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete AWS-Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter AWS-verwaltete Richtlinien oder AWS-verwaltete Richtlinien für Auftragsfunktionen 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 Service-Aktionen zu gewähren, wenn diese durch ein bestimmtes AWS-Service, wie beispielsweise AWS CloudFormation, verwendet werden. 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 Richtlinienvalidierung zum IAM Access Analyzer im IAM-Benutzerhandbuch.

- Bedarf einer Multi-Faktor-Authentifizierung (MFA):Wenn Sie ein Szenario haben, das IAM-Benutzer oder Root-Benutzer in Ihrem AWS-Konto erfordert, 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, müssen Sie über einen Mindestsatz von Berechtigungen verfügen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den Amazon-FSx-Ressourcen in Ihrem aufzulisten und anzuzeigenAWS-Konto. 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.

Für Benutzer, die nur Aufrufe an die AWS CLI oder AWS-API durchführen, müssen Sie keine Mindestberechtigungen in der Konsole erteilen. 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 von Amazon FSx verwaltete Service-Richtlinien in sehenAWS Von 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 enthält Berechtigungen für die Ausführung dieser Aktion auf der Konsole oder für die programmgesteuerte Ausführung über die AWS CLI oder die AWS-API.

```
{
```

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

AWS Von verwaltete Richtlinien für Amazon FSx

Eine AWS von verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet wird AWS. Von AWS verwaltete Richtlinien sind so konzipiert, dass sie Berechtigungen für viele häufige Anwendungsfälle bereitstellen, sodass Sie mit der Zuweisung von Berechtigungen für Benutzer, Gruppen und Rollen beginnen können.

Beachten Sie, dass von AWS verwaltete Richtlinien möglicherweise keine Berechtigungen mit den geringsten Berechtigungen für Ihre spezifischen Anwendungsfälle gewähren, da sie für alle - AWS

Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie kundenverwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in verwalteten AWS Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS von verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert, wirkt sich die Aktualisierung auf alle Prinzipalidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie angefügt ist. aktualisiert am AWS wahrscheinlichsten eine von AWS verwaltete Richtlinie, wenn ein neuer gestartet AWS-Service wird oder neue API-Operationen für vorhandene Services verfügbar werden.

Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien im IAM-Benutzerhandbuch.

AmazonFSxServiceRolePolicy

Ermöglicht Amazon FSx, AWS Ressourcen in Ihrem Namen zu verwalten. Weitere Informationen hierzu finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon FSx.

AWS Von verwaltete Richtlinie: AmazonFSxDeleteServiceLinkedRoleAccess

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 serviceverknüpfte Rolle für den Amazon S3-Zugriff zu löschen, die nur von Amazon FSx für Lustre verwendet wird.

Details zu Berechtigungen

Diese Richtlinie enthält Berechtigungen in , `iam` damit Amazon FSx den Löschstatus für die mit dem FSx Service verknüpfte Rolle für den Amazon S3-Zugriff anzeigen, löschen und anzeigen kann.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AmazonFSxDeleteServiceLinkedRoleAccess im Referenzhandbuch zu - AWS verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonFSxFullAccess

Sie können AmazonFSxFullAccess an Ihre IAM-Entitäten anfügen. Amazon FSx fügt diese Richtlinie auch an eine Servicerolle an, die es Amazon FSx ermöglicht, Aktionen in Ihrem Namen durchzuführen.

Bietet vollständigen 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 alle Amazon-FSx-Aktionen mit Ausnahme von `BypassSnaplockEnterpriseRetention`.
- `ds` – Ermöglicht es Prinzipalen, Informationen über die AWS Directory Service Verzeichnisse anzuzeigen.
- `ec2`
  - Ermöglicht es Prinzipalen, Tags unter den angegebenen Bedingungen zu erstellen.
  - So stellen Sie eine verbesserte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereit, die mit einer VPC verwendet werden können.
- `iam` – Ermöglicht es Prinzipalen, eine serviceverknüpfte Amazon-FSx-Rolle im Namen des Benutzers zu erstellen. Dies ist erforderlich, damit Amazon FSx AWS Ressourcen im Namen des Benutzers verwalten kann.
- `logs` – Ermöglicht es Prinzipalen, Protokollgruppen zu erstellen, Streams zu protokollieren und Ereignisse in Protokollstreams zu schreiben. Dies ist erforderlich, damit Benutzer den Zugriff auf das Dateisystem von FSx für Windows File Server überwachen können, indem sie Audit-Zugriffsprotokolle an CloudWatch -Protokolle senden.
- `firehose` – Ermöglicht es Prinzipalen, Datensätze in Amazon Data Firehose zu schreiben. Dies ist erforderlich, damit Benutzer den Zugriff auf das Dateisystem von FSx für Windows File Server überwachen können, indem sie Audit-Zugriffsprotokolle an Firehose senden.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AmazonFSxFullAccess im Referenzhandbuch zu - AWS verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonFSxConsoleFullAccess

Sie können die `AmazonFSxConsoleFullAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Administratorberechtigungen, die vollen Zugriff auf Amazon FSx und Zugriff auf verwandte - AWS Services über die ermöglichen AWS Management Console.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx` – Ermöglicht es Prinzipalen, alle Aktionen in der Amazon-FSx-Managementkonsole auszuführen, mit Ausnahme von `BypassSnaplockEnterpriseRetention`.
- `cloudwatch` – Ermöglicht es Prinzipalen, CloudWatch Alarme und Metriken in der Amazon-FSx-Managementkonsole anzuzeigen.
- `ds` – Ermöglicht es Prinzipalen, Informationen über ein - AWS Directory Service Verzeichnis aufzulisten.
- `ec2`
  - Ermöglicht es Prinzipalen, Tags in Routing-Tabellen zu erstellen, Netzwerkschnittstellen, Routing-Tabellen, Sicherheitsgruppen, Subnetze und die VPC aufzulisten, die einem Amazon FSx-Dateisystem zugeordnet ist.
  - Ermöglicht es Prinzipalen, eine verbesserte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.
- `kms` – Ermöglicht es Prinzipalen, Aliase für AWS Key Management Service Schlüssel aufzulisten.
- `s3` – Ermöglicht es Prinzipalen, einige oder alle Objekte in einem Amazon S3-Bucket (bis zu 1000) aufzulisten.
- `iam` – Gewährt die Berechtigung zum Erstellen einer serviceverknüpften Rolle, die es Amazon FSx ermöglicht, Aktionen im Namen des Benutzers durchzuführen.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AmazonFSxConsoleFullAccess im Referenzhandbuch zu - AWS verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonFSxConsoleReadOnlyAccess

Sie können die `AmazonFSxConsoleReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie gewährt Amazon FSx und verwandten AWS Services Leseberechtigungen, sodass Benutzer Informationen zu diesen Services in der anzeigen können AWS Management Console.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx` – Ermöglicht es Prinzipalen, Informationen über Amazon-FSx-Dateisysteme, einschließlich aller Tags, in der Amazon-FSx-Managementkonsole anzuzeigen.

- `cloudwatch` – Ermöglicht es Prinzipalen, CloudWatch Alarme und Metriken in der Amazon-FSx-Managementkonsole anzuzeigen.
- `ds` – Ermöglicht es Prinzipalen, Informationen über ein - AWS Directory Service Verzeichnis in der Amazon-FSx-Managementkonsole anzuzeigen.
- `ec2`
  - Ermöglicht es Prinzipalen, Netzwerkschnittstellen, Sicherheitsgruppen, Subnetze und die VPC anzuzeigen, die einem Amazon-FSx-Dateisystem in der Amazon-FSx-Managementkonsole zugeordnet ist.
  - So stellen Sie eine verbesserte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereit, die mit einer VPC verwendet werden können.
- `kms` – Ermöglicht es Prinzipalen, Aliase für AWS Key Management Service Schlüssel in der Amazon-FSx-Managementkonsole anzuzeigen.
- `log` – Ermöglicht es Prinzipalen, die Amazon CloudWatch -Logs-Protokollgruppen zu beschreiben, die dem Konto zugeordnet sind, das die Anforderung stellt. Dies ist erforderlich, damit Prinzipale die vorhandene Konfiguration der Dateizugriffsprüfung für ein FSx for Windows File Server-Dateisystem anzeigen können.
- `firehose` – Ermöglicht es Prinzipalen, die Amazon-Data-Firehose-Bereitstellungsdatenströme zu beschreiben, die dem Konto zugeordnet sind, das die Anforderung stellt. Dies ist erforderlich, damit Prinzipale die vorhandene Konfiguration der Dateizugriffsprüfung für ein FSx for Windows File Server-Dateisystem anzeigen können.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AmazonFSxConsoleReadOnlyAccess im Referenzhandbuch zu - AWS verwalteten Richtlinien.

AWS Von verwaltete Richtlinie: AmazonFSxReadOnlyAccess

Sie können die `AmazonFSxReadOnlyAccess`-Richtlinie an Ihre IAM-Identitäten anfügen.

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx` – Ermöglicht es Prinzipalen, Informationen über Amazon-FSx-Dateisysteme, einschließlich aller Tags, in der Amazon-FSx-Managementkonsole anzuzeigen.
- `ec2` – Um eine verbesserte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.

Informationen zum Anzeigen der Berechtigungen für diese Richtlinie finden Sie unter AmazonFSxReadOnlyAccess im Referenzhandbuch zu - AWS verwalteten Richtlinien.

Amazon-FSx-Updates für - AWS verwaltete Richtlinien

Anzeigen von Details zu Aktualisierungen für - AWS verwaltete Richtlinien für Amazon FSx, seit dieser Service mit der Verfolgung dieser Änderungen begonnen hat. Um automatische Warnungen über Änderungen an dieser Seite zu erhalten, abonnieren Sie den RSS-Feed auf der Amazon-FSx-DokumentverlaufSeite.

Änderung	Beschreibung	Datum
AmazonFSxServiceRolePolicy – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Prinzipalen ermöglicht, eine verbesserte Sicherheitsgruppenvalidierung für alle Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	9. Januar 2024
AmazonFSxReadOnlyAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Prinzipalen ermöglicht, eine verbesserte Sicherheitsgruppenvalidierung für alle Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	9. Januar 2024
AmazonFSxConsoleReadOnlyAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Prinzipal	9. Januar 2024

Änderung	Beschreibung	Datum
	en ermöglicht, eine verbesser te Sicherheitsgruppenvalidieru ng für alle Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	
AmazonFSxFullAcces s – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGro upsForVpc` die es Prinzipal en ermöglicht, eine verbesser te Sicherheitsgruppenvalidieru ng für alle Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	9. Januar 2024
AmazonFSxConsoleFu llAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGro upsForVpc` die es Prinzipal en ermöglicht, eine verbesser te Sicherheitsgruppenvalidieru ng für alle Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.	9. Januar 2024

Änderung	Beschreibung	Datum
AmazonFSxFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, mit der Benutzer eine regions- und kontoübergreifende Datenreplikation für FSx-für-OpenZFS-Dateisysteme durchführen können.	20. Dezember 2023
AmazonFSxConsoleFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, mit der Benutzer eine regions- und kontoübergreifende Datenreplikation für FSx-für-OpenZFS-Dateisysteme durchführen können.	20. Dezember 2023
AmazonFSxFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, mit der Benutzer eine On-Demand-Replikation von Volumes für FSx-für-OpenZFS-Dateisysteme durchführen können.	26. November 2023
AmazonFSxConsoleFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, mit der Benutzer eine On-Demand-Replikation von Volumes für FSx-für-OpenZFS-Dateisysteme durchführen können.	26. November 2023

Änderung	Beschreibung	Datum
AmazonFSxFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Benutzer gemeinsam genutzte VPC-Unterstützung für Multi-AZ-Dateisysteme von FSx für ONTAP anzeigen, aktivieren und deaktivieren können.	14. November 2023
AmazonFSxConsoleFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Benutzer gemeinsam genutzte VPC-Unterstützung für Multi-AZ-Dateisysteme von FSx für ONTAP anzeigen, aktivieren und deaktivieren können.	14. November 2023
AmazonFSxFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Netzwerkkonfigurationen für Multi-AZ-Dateisysteme von FSx für OpenZFS verwalten kann.	9. August 2023
AWS Von verwaltete Richtlinie: AmazonFSxServiceRolePolicy – Aktualisierung auf eine vorhandene Richtlinie	Amazon FSx hat die vorhandene `cloudwatch:PutMetricData` Berechtigung so geändert, dass Amazon FSx CloudWatch Metriken im `AWS/FSx` Namespace veröffentlicht.	24. Juli 2023

Änderung	Beschreibung	Datum
AmazonFSxFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat die Richtlinie aktualisiert, um die `fsx:*` Berechtigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen.	13. Juli 2023
AmazonFSxConsoleFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat die Richtlinie aktualisiert, um die `fsx:*` Berechtigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen.	13. Juli 2023
AmazonFSxConsoleReadOnlyAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Benutzer erweiterte Leistungsmetriken und empfohlene Aktionen für Dateisysteme von FSx für Windows File Server in der Amazon-FSx-Konsole anzeigen können.	21. September 2022
AmazonFSxConsoleFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Benutzer erweiterte Leistungsmetriken und empfohlene Aktionen für Dateisysteme von FSx für Windows File Server in der Amazon-FSx-Konsole anzeigen können.	21. September 2022

Änderung	Beschreibung	Datum
AmazonFSxReadOnlyAccess – Nachverfolgungsrichtlinie gestartet	Diese Richtlinie gewährt schreibgeschützten Zugriff auf alle Amazon-FSx-Ressourcen und alle ihnen zugeordneten Tags.	4. Februar 2022
AmazonFSxDeleteServiceLinkedRoleAccess – Nachverfolgungsrichtlinie gestartet	Diese Richtlinie gewährt Administratorberechtigungen, die es Amazon FSx ermöglichen, seine serviceverknüpfte Rolle für den Amazon S3-Zugriff zu löschen.	7. Januar 2022
AmazonFSxServiceRolePolicy – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Netzwerkkonfigurationen für Dateisysteme von Amazon FSx für NetApp ONTAP verwalten kann.	2. September 2021
AmazonFSxFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Tags in EC2-Routing-Tabellen für eingeschränkte Aufrufe erstellen kann.	2. September 2021
AmazonFSxConsoleFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Multi-AZ-Dateisysteme von Amazon FSx für NetApp ONTAP erstellen kann.	2. September 2021

Änderung	Beschreibung	Datum
AmazonFSxConsoleFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Tags in EC2-Routing-Tabellen für eingeschränkte Aufrufe erstellen kann.	2. September 2021
AmazonFSxServiceRolePolicy – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx CloudWatch Protokollstreams beschreiben und in sie schreiben kann. Dies ist erforderlich, damit Benutzer mithilfe von - CloudWatch Protokollen Dateizugriffs-Auditprotokolle für FSx-für-Windows-File-Server-Dateisysteme anzeigen können.	8. Juni 2021
AmazonFSxServiceRolePolicy – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Amazon-Data-Firehose-Bereitstellungsdatenströme beschreiben und darin schreiben kann. Dies ist erforderlich, damit Benutzer mithilfe von Amazon Data Firehose Audit-Protokolle für den Dateizugriff für ein FSx for Windows File Server-Dateisystem anzeigen können.	8. Juni 2021

Änderung	Beschreibung	Datum
AmazonFSxFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale CloudWatch Protokollgruppen beschreiben und erstellen, Streams protokollieren und Ereignisse in Protokollstreams schreiben können. Dies ist erforderlich, damit Prinzipale mithilfe von CloudWatch Protokollen Dateizugriffs-Auditprotokolle für FSx-für-Windows-File-Server-Dateisysteme anzeigen können.	8. Juni 2021
AmazonFSxFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale Datensätze in Amazon Data Firehose beschreiben und schreiben können. Dies ist erforderlich, damit Benutzer mithilfe von Amazon Data Firehose Audit-Protokolle für den Dateizugriff für ein FSx for Windows File Server-Dateisystem anzeigen können.	8. Juni 2021

Änderung	Beschreibung	Datum
AmazonFSxConsoleFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale die Amazon CloudWatch -Logs-Protokollgruppen beschreiben können, die dem Konto zugeordnet sind, das die Anforderung stellt. Dies ist erforderlich, damit Prinzipale bei der Konfiguration der Dateizugriffsprüfung für ein FSx for Windows File Server-Dateisystem eine vorhandene CloudWatch Protokollgruppe auswählen können.	8. Juni 2021
AmazonFSxConsoleFullAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale die Amazon-Data-Firehose-Bereitstellungsdatenströme beschreiben können, die dem Konto zugeordnet sind, das die Anforderung stellt. Dies ist erforderlich, damit Prinzipale einen vorhandenen Firehose-Bereitstellungsdatenstrom auswählen können, wenn sie die Dateizugriffsprüfung für ein FSx for Windows File Server-Dateisystem konfigurieren.	8. Juni 2021

Änderung	Beschreibung	Datum
AmazonFSxConsoleReadOnlyAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale die Amazon CloudWatch -Logs-Protokollgruppen beschreiben können, die dem Konto zugeordnet sind, das die Anforderung stellt. Dies ist erforderlich, damit Prinzipale die vorhandene Konfiguration der Dateizugriffsprüfung für ein FSx for Windows File Server-Dateisystem anzeigen können.	8. Juni 2021
AmazonFSxConsoleReadOnlyAccess – Aktualisierung einer vorhandenen Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Prinzipale die Amazon-Data-Firehose-Bereitstellungsdatenströme beschreiben können, die dem Konto zugeordnet sind, das die Anforderung stellt. Dies ist erforderlich, damit Prinzipale die vorhandene Konfiguration der Dateizugriffsprüfung für ein FSx for Windows File Server-Dateisystem anzeigen können.	8. Juni 2021

Änderung	Beschreibung	Datum
Amazon FSx hat mit der Verfolgung von Änderungen begonnen	Amazon FSx hat mit der Verfolgung von Änderungen für seine von AWS verwalteten Richtlinien begonnen.	8. Juni 2021

Fehlerbehebung für Identität und Zugriff auf Amazon FSx for Lustre

Verwenden Sie die folgenden Informationen, um häufige Probleme zu diagnostizieren und zu beheben, die bei der Arbeit mit Amazon FSx und IAM auftreten können.

Themen

- Ich bin nicht autorisiert, eine Aktion in Amazon FSx auszuführen
- Ich bin nicht autorisiert, iam durchzuführen:PassRole
- Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Amazon-FSx-Ressourcen gewähren

Ich bin nicht autorisiert, eine Aktion in Amazon FSx auszuführen

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.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht autorisiert, iam durchzuführen:PassRole

Wenn Sie die Fehlermeldung erhalten, dass Sie nicht zum Ausführen der `iam:PassRole` Aktion autorisiert sind, müssen Ihre Richtlinien aktualisiert werden, um eine Rolle an Amazon FSx übergeben zu können.

Einige AWS-Services erlauben die Übergabe einer vorhandenen Rolle an diesen Dienst, sodass keine neue Servicerolle oder serviceverknüpfte Rolle erstellt werden muss. 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.

Wenden Sie sich an Ihren AWS-Administrator, falls Sie weitere Unterstützung benötigen. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb meines AWS-Konto Zugriff auf meine Amazon-FSx-Ressourcen gewähren

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 dazu, ob Amazon FSx diese Funktionen unterstützt, finden Sie unter Funktionsweise von Amazon FSx for Lustre mit IAM.
- Informationen zum Gewähren des Zugriffs auf Ihre Ressourcen für alle Ihre AWS-Konten finden Sie unter Gewähren des Zugriffs für einen IAM-Benutzer in einem anderen Ihrer AWS-Konto im IAM-Benutzerhandbuch.

- Informationen dazu, wie Sie AWS-Konten-Drittanbieter Zugriff auf Ihre Ressourcen bereitstellen, finden Sie unter Gewähren des Zugriffs auf AWS-Konten von externen Benutzern im IAM-Benutzerhandbuch.
- 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 bestimmteAWS 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 angeben werden. Sie können diese Resource-Tags verwenden, um eine attributbasierte Zugriffskontrolle (ABAC) zu implementieren. Weitere Informationen finden Sie unter Was ist ABAC fürAWS? 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 Beispiel`fsx: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 zuzuweisenAWS-Konto.

```
{
  "Statement": [
    {
```

```
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*"
      ]
    }
  ]
}
```

In ähnlicher Weise erlaubt die folgende Richtline 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 TagsMarkieren Ihrer Amazon ECX-Ressourcen mit Tags von Amazon Weitere Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf Amazon FSx for Lustre-Ressourcen zur Steuerung des Zugriffs mit TagsVerwenden von mithilfe von von 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 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 aufAWS 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 TagsErteilen 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 TagsMarkieren Ihrer Amazon ECX-Ressourcen mit Tags 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`Deparment=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example 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 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 gekennzeichnet sind`Department=Finance`, und nur auf Dateisystemen, die mit gekennzeichnet sind`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:task/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Verwenden von serviceverknüpften Rollen für Amazon FSx

Amazon FSx verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen . Eine serviceverknüpfte Rolle ist ein spezieller Typ einer IAM-Rolle, die direkt mit Amazon FSx verknüpft

ist. Serviceverknüpfte Rollen werden von Amazon FSx vordefiniert und schließen alle Berechtigungen ein, die der Service zum Aufrufen anderer - AWS Services in Ihrem Namen erfordert.

Eine serviceverknüpfte Rolle vereinfacht das Einrichten von Amazon FSx, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon FSx definiert die Berechtigungen seiner serviceverknüpften Rollen. Sofern keine andere Konfiguration festgelegt wurde, kann nur Amazon FSx die 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 Berechtigung für den Zugriff auf 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.

Serviceverknüpfte Rollenberechtigungen für Amazon FSx

Amazon FSx verwendet zwei serviceverknüpfte Rollen namens `AWSServiceRoleForAmazonFSx` und `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`*, die bestimmte Aktionen in Ihrem Konto ausführen. Beispiele für diese Aktionen sind das Erstellen von Elastic Network-Schnittstellen für Ihre Dateisysteme in Ihrer VPC und der Zugriff auf Ihr Daten-Repository in einem Amazon S3-Bucket. Für wird `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`*diese serviceverknüpfte Rolle für jedes Amazon FSx for Lustre-Dateisystem erstellt, das Sie erstellen und das mit einem S3-Bucket verknüpft ist.

AWSServiceRoleForAmazonFSx -Berechtigungsdetails

Für erlaubt `AWSServiceRoleForAmazonFSx`die Rollenberechtigungsrichtlinie Amazon FSx, die folgenden administrativen Aktionen im Namen des Benutzers für alle entsprechenden AWS Ressourcen durchzuführen:

Aktualisierungen dieser Richtlinie finden Sie unter . AmazonFSxServiceRolePolicy

> **Note**
>
> Der AWSServiceRoleForAmazonFSx wird von allen Amazon-FSx-Dateisystemtypen verwendet. Einige der aufgelisteten Berechtigungen gelten nicht für FSx for Lustre.

- `ds` – Ermöglicht Amazon FSx das Anzeigen, Autorisieren und Aufheben der Autorisierung von Anwendungen in Ihrem AWS Directory Service Verzeichnis.
- `ec2` – Ermöglicht Amazon FSx Folgendes:
  - Netzwerkschnittstellen anzeigen, erstellen und die Zuordnung aufheben, die einem Amazon FSx-Dateisystem zugeordnet sind.
  - Zeigen Sie eine oder mehrere Elastic IP-Adressen an, die einem Amazon FSx-Dateisystem zugeordnet sind.
  - Zeigen Sie Amazon-VPCs, Sicherheitsgruppen und Subnetze an, die einem Amazon-FSx-Dateisystem zugeordnet sind.
  - So stellen Sie eine verbesserte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereit, die mit einer VPC verwendet werden können.
  - Erstellen Sie eine Berechtigung für einen von AWSautorisierten Benutzer, um bestimmte Operationen auf einer Netzwerkschnittstelle auszuführen.
- `cloudwatch` – Ermöglicht Amazon FSx, Metrikdatenpunkte in CloudWatch unter dem AWS/FSx-Namespace zu veröffentlichen.
- `route53` – Ermöglicht Amazon FSx, eine Amazon VPC einer privat gehosteten Zone zuzuordnen.
- `logs` – Ermöglicht Amazon FSx das Beschreiben und Schreiben in CloudWatch Logs-Protokollstreams. Auf diese Weise können Benutzer Dateizugriffs-Auditprotokolle für ein FSx for Windows File Server-Dateisystem an einen CloudWatch Logs-Stream senden.
- `firehose` – Ermöglicht Amazon FSx das Beschreiben und Schreiben in Amazon-Data-Firehose-Bereitstellungsdatenströme. Auf diese Weise können Benutzer die Dateizugriffs-Auditprotokolle für ein FSx for Windows File Server-Dateisystem in einem Amazon Data Firehose-Bereitstellungs-Stream 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 beschriebenAmazon-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 Serviceverknüpfte Rollenberechtigungen im IAM-Benutzerhandbuch.

AWSServiceRoleForFSxS3Access Berechtigungsdetails

Für erlaubt `AWSServiceRoleForFSxS3Access_`*`file-system-id`*die Rollenberechtigungsrichtlinie Amazon FSx, 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.

Erstellen einer serviceverknüpften Rolle für Amazon FSx

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein Dateisystem in der AWS CLI, AWS Management Consoleder oder der API erstellen AWS , 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.

Bearbeiten einer serviceverknüpften Rolle für Amazon FSx

Amazon FSx erlaubt es Ihnen nicht, diese serviceverknüpften Rollen zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der Rollenname 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 serviceverknüpften 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

Sie können die IAM-Konsole, die IAM-CLI oder die IAM-API verwenden, um die AWSServiceRoleForAmazonFSx-serviceverknüpfte Rolle zu löschen. 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 für Linux-Instances.

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 Lustre-Dateiservern
Benutzerdefinierte TCP-Regel	TCP	988	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

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
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-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 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-Da	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre-Dateiservern 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-Dateisystemen zugeordnet sind.	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre-Dateiservern 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-Dateisystemen zugeordnet sind.	Lustre-Verkehr zwischen FSx for Lustre-Dateiservern 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-Dateisystemen zugeordnet sind	Ermöglicht Lustre-Verkehr zwischen FSx for Lustre-Dateiservern 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 ein AWS-Service in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services in Geltungsbereich nach Compliance-Programm. Wählen Sie das Compliance-Programm, das Sie interessiert. Allgemeine Informationen finden Sie unter AWS-Compliance-Programme.

Sie können Auditberichte von Drittanbietern unter AWS Artifact herunterladen. Weitere Informationen finden Sie unter Berichte herunterladen in AWS Artifact.

Ihre Compliance-Verantwortung bei der Verwendung von AWS-Services ist von der Sensibilität Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen und Vorschriften abhängig. AWS stellt die folgenden Ressourcen zur Unterstützung der Compliance bereit:

- Kurzanleitungen für Sicherheit und Compliance – In diesen Bereitstellungsleitfäden werden Überlegungen zur Architektur erörtert und Schritte zum Bereitstellen von Basisumgebungen auf AWS zur Verfügung gestellt, die auf Sicherheit und Compliance ausgerichtet sind.
- Erstellung einer Architektur mit HIPAA-konformer Sicherheit und Compliance in Amazon Web Services – In diesem Whitepaper wird beschrieben, wie Unternehmen mithilfe von AWS HIPAA-berechtigte Anwendungen erstellen können.

  > **Note**
  >
  > Nicht alle AWS-Services sind HIPAA-berechtigt. Weitere Informationen finden Sie in der Referenz für HIPAA-berechtigte Services.

- AWS-Compliance-Ressourcen – Diese Arbeitsbücher und Leitfäden könnten für Ihre Branche und Ihren Standort relevant sein.
- AWS-Compliance-Leitfäden für Kunden – Verstehen Sie das Modell der geteilten Verantwortung aus dem Blickwinkel der Einhaltung von Vorschriften. In den Leitfäden werden die bewährten Methoden zum Schutz von AWS-Services zusammengefasst 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.
- Auswertung von Ressourcen mit Regeln im AWS ConfigEntwicklerhandbuch – Der AWS Config-Service bewertet, wie gut Ihre Ressourcenkonfigurationen mit internen Praktiken, Branchenrichtlinien und Vorschriften übereinstimmen.
- AWS Security Hub – Dieser AWS-Service bietet einen umfassenden Überblick über Ihren Sicherheitsstatus innerhalb von 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.
- AWS Audit Manager – Dieser AWS-Service hilft Ihnen, Ihre AWS-Nutzung kontinuierlich zu überprüfen, um den Umgang mit Risiken und die Compliance von Branchenstandards zu vereinfachen.

Amazon FSx for Lustre und Schnittstellen-VPC-Endpunkte (AWS PrivateLink)

Sie können die Sicherheit Ihrer VPC erhöhen, indem Sie Amazon FSx so konfigurieren, dass ein Schnittstellen-VPC-Endpunkt verwendet wird. Die Schnittstellen-VPC-Endpunkte werden mit bereitgestellt AWS PrivateLink, einer Technologie, die es Ihnen ermöglicht, ohne Internet-Gateway, NAT-Gerät, VPN-Verbindung oderAWS Direct Connect -Verbindung privat auf Amazon FSx-APIs zuzugreifen. Die Instances in Ihrer VPC benötigen für die Kommunikation mit Amazon-FSx-APIs keine öffentlichen IP-Adressen. Der Datenverkehr zwischen Ihrer VPC und Amazon FSx verlässt dasAWS Netzwerk nicht.

Jeder Schnitten-VPC-Endpunkt wird durch eine oder mehrere Elastic Network-Schnittstellen in Ihren Subnetzen dargestellt. Eine Netzwerkschnittstelle stellt eine private IP-Adresse bereit, die als Einstiegspunkt für Datenverkehr zur Amazon FSx API dient.

Überlegungen zu VPC-Endpunkten der Amazon-FSx-Endpunkte

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Amazon FSx einrichten, stellen Sie sicher, dass Sie die Eigenschaften und Einschränkungen des Schnittstellen-VPC-Endpunkts im Amazon VPC-Benutzerhandbuch einsehen.

Sie können alle Amazon-FSx-API-Operationen von Ihrer VPC aus aufrufen. Sie können beispielsweise ein FSx for Lustrere-Dateisystem erstellen, indem Sie die CreateFileSystem API aus Ihrer VPC aufrufen. Die vollständige Liste der Amazon FSx-APIs finden Sie unter Aktionen in der Amazon FSx-API-Referenz.

VPC-Peering-ing-ing-ing-ing-ing-Überlegungen

Sie können andere VPCs mit Schnitten-VPC-Endpunkten über VPC-Peering mit der VPC Peering-Endpunkten über VPC-Peering mit der VPC 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 herstellenAWS-Konto. Die VPCs können auch in zwei verschiedenen bestehenAWS-Regionen.

Der Datenverkehr zwischen über Peering verbundenen VPCs bleibt im AWS-Netzwerk und wird nicht über das öffentliche Internet übertragen. Sobald zwischen VPCs eine Peering-Verbindung besteht, können Ressourcen wie Amazon-Elastic-Compute-Cloud Elastic Compute Cloud (Amazon EC2) -

Instances in beiden VPCs über Schnitten-VPC-Endpunkte, die in einem der VPCs erstellt wurden, auf die Amazon FSx-API zugreifen.

Erstellen eines Schnitten-VPC-Endpunkts für die Amazon FSx API

Sie können einen VPC-Endpunkt für die Amazon-FSx-API mithilfe der Amazon-VPC-Konsole oder derAWS Command Line Interface erstellen.AWS CLI Weitere Informationen finden Sie unter Erstellen eines Schnitten-VPC-Endpunkts im Amazon VPC-Endpunkt im Amazon VPC-Endpunkt 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 einen der folgenden ing-Endpunkte, um einen Schnittstellen-VPC-Endpunkt für Amazon FSx zu erstellen:

- **`com.amazonaws.`*`region`*`.fsx`**— Erstellt einen Endpunkt für Amazon FSx API-Operationen.
- **`com.amazonaws.`*`region`*`.fsx-fips`**— Erstellt einen Endpunkt für die Amazon FSx API, der den Federal Information Processing Standard (FIPS) 140-2 erfüllt.

Um die private DNS-Option verwenden zu können, müssen Sie`enableDnsHostnames`und`enableDnsSupport` Ihrer VPC festlegen. Weitere Informationen finden Sie unter Anzeigen und Aktualisieren der DNS-Unterstützung für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Wenn Sie einen privaten DNS für den Endpunkt aktivieren, können Sie mit dem VPC-Endpunkt mittels seines standardmäßigen DNS-Namens, beispielsweiseAWS-Region, an Amazon FSx API-Anforderungen an Amazon FSx senden`fsx.us-east-1.amazonaws.com`.AWS-Regionen Für China (Peking) und China (Ningxia)AWS-Regionen können Sie API-Anforderungen mit dem VPC-Endpunkt mittels`fsx-api.cn-north-1.amazonaws.com.cn` bzw.`fsx-api.cn-northwest-1.amazonaws.com.cn` senden.

Weitere Informationen finden Sie unter Zugriff auf einen Service über einen Schnitten-VPC-Endpunkt im Amazon VPC-Endpunkt im Amazon VPC-Endpunkt im Amazon VPC-Endpunkt.

Erstellen einer VPC-Richtlinie für Amazon FSx

Zur weiteren Kontrolle des Zugriffs auf die Amazon FSx API können Sie Ihrem VPC-Endpunkt optional eineAWS Identity and Access Management (IAM) -Richtlinie anfügen. 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 die Kontingente bei der Arbeit mit Amazon FSx for Lustre.

Themen

Kontingente, die Sie erhöhen können

Im Folgenden sind die Kontingente für Amazon FSx for Lustre pro AWS Konto und AWS Region aufgeführt, die Sie erhöhen können.

Ressource	Standard	Beschreibung
Dateisysteme Lustre Persistent_1	100	Die maximale Anzahl von Amazon FSx for Lustre Persistent_1-Dateisystemen, die Sie in diesem Konto erstellen können.
Dateisysteme Lustre Persistent_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 Dateisysteme von Amazon FSx für Lustre Persistent_1 in diesem Konto konfigurieren können.
Lustre Persistent_2-Dateispeicherkapazität	100800	Die maximale Speicherkapazität (in GiB), die Sie für alle Dateisysteme von Amazon FSx für Lustre Persistent_2 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 aus.
5. Wählen Sie Kontingenterhöhung anfordern und folgen Sie den Anweisungen, um eine Kontingenterhöhung anzufordern.
6. Um den Status der Kontingentanforderung anzuzeigen, wählen Sie im Navigationsbereich der Konsole die Option Verlauf der Kontingentanforderung aus.

Weitere Informationen finden Sie unter Beantragen einer Kontingenterhöhung im Service-Quotas-Benutzerhandbuch.

Ressourcenkontingente für jedes Dateisystem

Im Folgenden sind die Limits für Amazon-FSx-for-Lustre-Ressourcen für jedes Dateisystem in einer -AWSRegion aufgeführt.

Ressource	Limit pro Dateisystem
Maximale Anzahl von Tags	50
Maximale Aufbewahrungsdauer für automatisierte Backups	90 Tage
Maximale Anzahl von Backup-Kopieranforderungen, die pro Konto an eine einzelne Zielregion ausgeführt werden.	5
Anzahl der Dateiaktualisierungen aus dem verknüpften S3-Bucket pro Dateisystem	10 Millionen/Monat
Minimale Speicherkapazität, SSD-Dateisysteme	1,2 TiB
Minimale Speicherkapazität, HDD-Dateisysteme	6 TiB
Minimaler Durchsatz pro Speichereinheit, SSD	50 MBps

Ressource	Limit pro Dateisystem
Maximaler Durchsatz pro Speichereinheit, SSD	1 000 MBps
Minimaler Durchsatz pro Speichereinheit, HDD	12 MBps
Maximaler Durchsatz pro Speichereinheit, HDD	40 MBps

Weitere Überlegungen

Beachten Sie außerdem Folgendes:

- Sie können jeden AWS Key Management Service (AWS KMS)-Schlüssel auf bis zu 125 Dateisystemen von Amazon FSx für Lustre verwenden.
- Eine Liste der AWS Regionen, in denen Sie Dateisysteme erstellen können, finden Sie unter Amazon-FSx-Endpunkte und -Kontingente im Allgemeine 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

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 Daten-Repositorys 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 Dateisystem-Mount-Befehl 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-systemsAWS CLIBefehls oder der DescribeFileSystemsAPI-Operation abrufen.

Das Dateisystem-Mount hängt und schlägt dann mit einem Timeout-Fehler fehl

Der Mount-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

Das automatische Mounten schlägt fehl und die Instanz 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 anAWS 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 davon 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 (CreateDataRepositoryAssociationentspricht 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 (CreateFileSystemist 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 Daten-Repositorys in Amazon S3.
2. Aktualisieren Sie mithilfe der Amazon FSx CLI oder API die Dateisysteme `AutoImportPolicy` mit dem `update-file-system` CLI-Befehl (UpdateFileSystementspricht 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 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 (UpdateFileSystementspricht 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 beschriebenLayout des Dateisystemspeichers. 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 Verwalten 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 ann`proc`, 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 k `ill -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 |egrep '( 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 unterEntfernen von Daten in Ihrem Dateisystem.

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

Wir empfehlen, zu verwendenAWS 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.

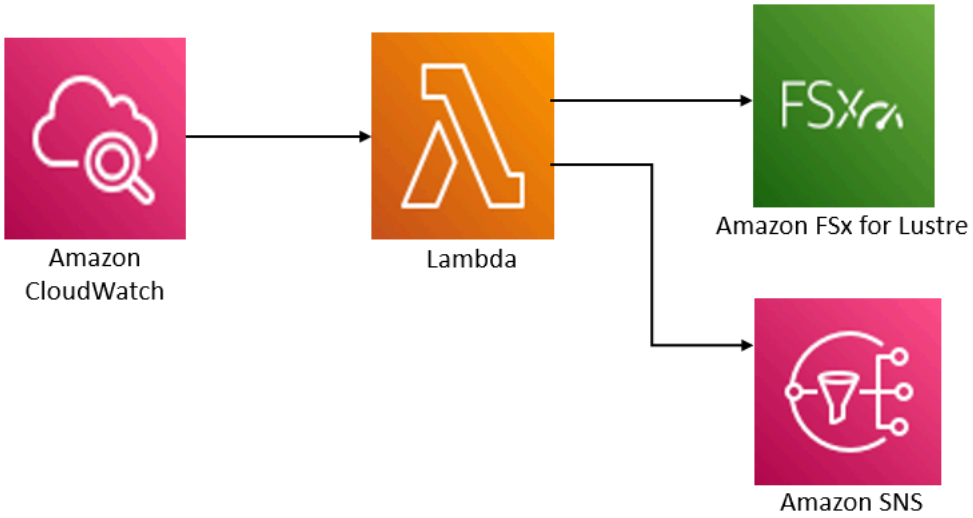
Die Lösung stellt automatisch alle erforderlichen Komponenten bereit und verwendet die folgenden Parameter:

- 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 erstelltAWS 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-Lustre`CreateBackup`-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 ab`DescribeBackups`. 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.

5. Überprüfen und bestätigen Sie für Review die Einstellungen. Sie müssen das Kontrollkästchen aktivieren, um zu bestätigen, dass die Vorlage IAM-Ressourcen erstellt.
6. 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: 25. März 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
Lustre-Client-Unterstützung für Amazon Linux 2023 hinzugefügt	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.	25. März 2024
Lustre-Client-Unterstützung für Centos, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.9 hinzugefügt	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.	9. Januar 2024
Amazon FSx hat die verwalteten Richtlinien von AmazonFSx FullAccess, AmazonFSx ConsoleFullAccess, AmazonF SxReadOnlyAccess und AmazonF SxConsole	Amazon FSx hat die Richtlinien von AmazonFSxFullAccess, AmazonF, AmazonFSx ConsoleFullAccess, AmazonF SxReadOnlyAccess und AmazonF SxServiceRolePolicy aktualisiertSxCons	9. Januar 2024

ReadOnlyAccess aktualisiert SxServiceRolePolicy AWS	oleReadOnlyAccess, um die Genehmigung hinzuzufügen. `ec2:GetSecurityGroupsForVpc` Weitere Informationen finden Sie unter Amazon FSx-Updates für AWS verwaltete Richtlinien.	
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 AmazonF SxFullAccess und AmazonF aktualisiert. SxConsoleFullAccess AWS	Amazon FSx hat die AmazonF SxFullAccess - und SxConsole FullAccess AmazonF-R ichtlinien 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 verwaltet en Richtlinien aktualisiert. SxConsoleFullAccess AWS	Amazon FSx hat die SxConsoleFullAccess Richtlini en von AmazonF SxFullAcc ess und AmazonF aktualisi ert, um die Genehmigung hinzuzufügen. `fsx:CopyS napshotAndUpdateVo lume` Weitere Informationen finden Sie unter Amazon FSx-Updates für AWS verwaltete Richtlinien.	26. November 2023
Support für die Skalierung der Durchsatzkapazität hinzugefü gt	Sie können jetzt die Durchsatz kapazität 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 verwaltet en Richtlinien aktualisiert. SxConsoleFullAccess AWS	Amazon FSx hat die AmazonF SxFullAccess - und SxConsole FullAccess AmazonF-R ichtlinien aktualisiert, um die Berechtigungen und hinzuzufü gen. `fsx:DescribeShared VPCConfiguration` `fsx:UpdateSharedVP CConfiguration` 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-Dateisysteme 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-Dateisystem.	29. August 2023
Zusätzliche AWS-Region Unterstützung für den Bereitstellungstyp Persistent_1 hinzugefügt	Persistent_1 FSx for Lustre Lustre-Dateisysteme sind jetzt in Israel (Tel Aviv) verfügbar. AWS-Region Weitere Informationen finden Sie unter Bereitstellungsoptionen für FSx for Lustre-Dateisysteme.	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 AmazonF SxServiceRolePolicy AWS verwaltete Richtlinie aktualisiert	Amazon FSx hat die `cloudwatch:PutMetricData` Erlaubnis im SxServiceRolePolicy AmazonF aktualisiert. Weitere Informationen finden Sie unter Amazon FSx-Updates für AWS verwaltete Richtlinien.	24. Juli 2023
Amazon FSx hat die von AmazonF SxFullAccess AWS verwaltete Richtlinie aktualisiert	Amazon FSx hat die SxFullAccess AmazonF-Richtlinie aktualisiert, um die `fsx:*` Genehmigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen. Weitere Informationen finden Sie in der SxFullAccessAmazonF-Richtlinie.	13. Juli 2023

Amazon FSx hat die von AmazonF SxConsoleFullAcces s AWS verwaltete Richtlinie aktualisiert	Amazon FSx hat die SxConsoleFullAcces s AmazonF-Richtlinie aktualisiert, um die `fsx:*` Genehmigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen. Weitere Informationen finden Sie in der SxConsoleFullAcces sAmazonF-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 hinzugefü gt	FSx for Lustre bietet jetzt CloudWatch Amazon-Metriken, die automatis che Import- und Exportakt ualisierungen für Dateisyst eme 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 Datenrepositorys mit Lustre 2.12-Dateisystemen mit den Bereitstellungstypen Persistent_1 oder Scratch_2 zu verknüpfen. Weitere Informationen finden Sie unter Verwenden von Datenrepositorys 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-Region Unterstützung für den Bereitstellungstyp Persistent_2 hinzugefügt	Persistent_2 SSD FSx der nächsten Generation für Lustre-Dateisysteme sind jetzt in Europa (Stockholm), im asiatisch-pazifischen Raum (Hongkong), im asiatisch-pazifischen Raum (Mumbai) und im asiatisch-pazifischen Raum (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-Region 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 Verknüpfen Ihres Dateisystems mit einem S3-Bucket.	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 Datenrepositorys 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 Datenrepositorys, 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 typischer weise 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 Daten-Repository hinzugefügt wurden, und Dateien, die sich in einem verknüpften Daten-Repository 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 kurzfristigere 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 Datenrepositorys.	23. Dezember 2019

Neue Funktion für Datenrepository-Aufgaben veröffentlicht	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 Übertragung von Daten und Metadaten mithilfe von Datenrepository-Aufgaben.	23. Dezember 2019
Zusätzliche AWS-Region Unterstützung hinzugefügt	FSx for Lustre ist jetzt in der Region Europa (London) verfügbar. AWS-RegionInformationen zu den regionsspezifischen Grenzwerten von FSx for Lustre finden Sie unter Grenzwerte.	9. Juli 2019
Zusätzliche Unterstützung hinzugefügt AWS-Region	FSx for Lustre ist jetzt im asiatisch-pazifischen Raum (Singapur) erhältlich. AWS-RegionInformationen zu den regionsspezifischen Grenzwerten von FSx for Lustre finden Sie unter Grenzwerte.	26. Juni 2019
Lustre-Client-Unterstützung für Amazon Linux und Amazon Linux 2 hinzugefügt	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 Installation des Lustre-Clients.	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.