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 Lustre Hochleistungsdateisystem zu starten und auszuführen. Sie verwenden Lustre für Workloads, bei denen es auf Geschwindigkeit ankommt, wie z. B. maschinelles Lernen, Hochleistungsrechnen (HPC), Videoverarbeitung und Finanzmodellierung.

Das Lustre Dateisystem wurde für Anwendungen entwickelt, die schnellen Speicher benötigen — bei denen Sie möchten, dass Ihr Speicher mit Ihrer Rechenleistung Schritt hält. Lustrewurde entwickelt, um das Problem der schnellen und kostengünstigen Verarbeitung der ständig wachsenden Datensätze der Welt zu lösen. Es ist ein weit verbreitetes Dateisystem, das für die schnellsten Computer der Welt entwickelt wurde. Es bietet Latenzen von unter einer Millisekunde, einen Durchsatz TBps von bis zu einem Vielfachen und bis zu Millionen von IOPS. Weitere Informationen finden Sie auf der Website. LustreLustre

Als vollständig verwalteter Service FSx erleichtert Amazon Ihnen die Nutzung Lustre für Workloads, bei denen es auf die Speichergeschwindigkeit ankommt. FSx for Lustre macht die herkömmliche Komplexität der Einrichtung und Verwaltung von Lustre Dateisystemen überflüssig, sodass Sie innerhalb weniger Minuten ein bewährtes Hochleistungsdateisystem einrichten und ausführen können. Es bietet außerdem mehrere Bereitstellungsoptionen und Speicherklassen, sodass Sie die Kosten an Ihre Bedürfnisse anpassen können.

FSx for Lustre ist POSIX-kompatibel, 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 Dateisystem mit Ihrem Linux-Betriebssystem. Es bietet auch read-after-write Konsistenz und unterstützt das Sperren von Dateien.

Themen

- Verwenden Sie Amazon FSx for Lustre zum ersten Mal?

Mehrere Bereitstellungsoptionen und Speicherklassen

Amazon FSx for Lustre bietet eine Auswahl an Scratch-Dateisystemen und persistenten Dateisystemen, um unterschiedlichen Datenverarbeitungsanforderungen gerecht zu werden. Scratch-Dateisysteme sind ideal für die temporäre Speicherung und kurzfristigere Verarbeitung von Daten. Daten werden nicht repliziert und bleiben nicht erhalten, wenn ein Dateiserver ausfällt. Persistente Dateisysteme eignen sich ideal für längerfristige Speicherung und Workloads, bei denen der Durchsatz im Vordergrund steht. In persistenten Dateisystemen werden Daten repliziert, und Dateiserver werden ersetzt, wenn sie ausfallen. Weitere Informationen finden Sie unter Bereitstellungs- und Speicherklassenoptionen FSx für Lustre-Dateisysteme.

Amazon FSx for Lustre bietet Speicherklassen für Solid State Drive (SSD) und Hard Disk Drive (HDD), die für unterschiedliche Datenverarbeitungsanforderungen optimiert sind: AWS Interconnect

- Die SSD-Speicherklasse ist für Workloads optimiert, die kleine, zufällige Dateioperationen ausführen und bis zu einem Durchsatz TBps von bis zu einem Durchsatz benötigen. Sie bietet einen konsistenten Latenzzugriff auf Ihren gesamten Datensatz mit einer Latenz von unter einer Millisekunde.
- Die Intelligent-Tiering-Speicherklasse ist für die meisten Workloads geeignet und wird empfohlen, für die keine konsistente niedrige Latenz für Ihren gesamten Datensatz erforderlich ist. Sie bietet vollständig elastischen und kostengünstigen Speicher, einen Durchsatz TBps von bis zu einem Vielfachen und Latenzzeiten von weniger als einer Millisekunde auf Daten, auf die häufig zugegriffen wird, mit einem optionalen SSD-Lesecache.
- Die HDD-Speicherklasse kann für Workloads verwendet werden, die eine konsistente Latenz im einstelligen Millisekundenbereich und einen Durchsatz von bis zu zehn Prozent für Ihren gesamten Datensatz benötigen. GBps Sie können optional einen SSD-Lesecache bereitstellen, der auf 20% Ihrer Festplattenspeicherkapazität ausgelegt ist.

Weitere Informationen finden Sie unter FSx für Lustre-Speicherklassen.

FSx für Lustre und Datenrepositorien

Sie können FSx für Lustre-Dateisysteme Links zu Datenrepositorys auf Amazon S3 oder zu lokalen Datenspeichern herstellen.

FSx für die Integration des Lustre S3-Datenrepositorys

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

FSx für Lustre und lokale Datenrepositorien

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

Zugriff FSx für Lustre-Dateisysteme

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

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

- Amazon EC2 — Sie greifen über den Lustre Open-Source-Client von Ihren EC2 Amazon-Compute-Instances auf Ihr Dateisystem zu. EC2 Amazon-Instances können von anderen Availability Zones innerhalb derselben Amazon Virtual Private Cloud (Amazon VPC) aus auf Ihr Dateisystem zugreifen, sofern Ihre Netzwerkkonfiguration den Zugriff über Subnetze innerhalb der VPC ermöglicht. Nachdem Ihr Amazon FSx for Lustre-Dateisystem bereitgestellt wurde, können Sie mit seinen Dateien und Verzeichnissen genauso arbeiten, wie Sie es mit einem lokalen Dateisystem tun würden.

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

Amazon FSx for Lustre ist mit den beliebtesten Linux-Betriebssystemen kompatibel AMIs, darunter Amazon Linux 2023 und Amazon Linux 2, Red Hat Enterprise Linux (RHEL), CentOS, Ubuntu und SUSE Linux. Der Lustre Client ist in Amazon Linux 2023 und Amazon Linux 2 enthalten. Für RHEL, CentOS und Ubuntu bietet ein AWS Lustre Client-Repository Clients, die mit diesen Betriebssystemen kompatibel sind.

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

Weitere Informationen zu den Clients, Recheninstanzen und Umgebungen, von denen aus Sie auf Lustre-Dateisysteme zugreifen FSx können, finden Sie unter. Zugreifen auf Dateisysteme

Integrationen mit Diensten AWS

Amazon FSx for Lustre lässt sich in Amazon SageMaker AI als Eingabedatenquelle integrieren. Wenn Sie SageMaker KI mit FSx for Lustre verwenden, werden Ihre Trainingsaufgaben für maschinelles Lernen beschleunigt, da der anfängliche Download-Schritt von Amazon S3 entfällt. Darüber hinaus werden Ihre Gesamtbetriebskosten (TCO) reduziert, da Sie das wiederholte Herunterladen gängiger Objekte für iterative Jobs auf demselben Datensatz vermeiden und so Kosten für S3-Anfragen sparen. Weitere Informationen finden Sie unter Was ist KI? SageMaker im Amazon SageMaker AI Developer Guide. Eine exemplarische Vorgehensweise zur Verwendung von Amazon FSx for Lustre als Datenquelle für SageMaker KI finden Sie im AWS Machine Learning Learning-Blog unter Beschleunigen Sie das Training zu Amazon SageMaker AI mithilfe von Amazon FSx for Lustre- und Amazon EFS-Dateisystemen.

FSx for Lustre lässt sich in die Verwendung von Launch Templates integrieren AWS Batch . EC2 AWS Batch ermöglicht die Ausführung von Batch-Computing-Workloads auf dem AWS

Cloud, einschließlich High Performance Computing (HPC), Machine Learning (ML) und anderen asynchronen Workloads. AWS Batch passt die Größe der Instanzen automatisch und dynamisch auf der Grundlage der Anforderungen an die Arbeitsressourcen an. Weitere Informationen finden Sie unter Was ist AWS Batch? im AWS Batch Benutzerhandbuch.

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

Sicherheit und Compliance

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

Annahmen

In diesem Leitfaden gehen wir von den folgenden Annahmen aus:

- Wenn Sie Amazon Elastic Compute Cloud (Amazon EC2) verwenden, gehen wir davon aus, dass Sie mit diesem Service vertraut sind. Weitere Informationen zur Verwendung von Amazon EC2 finden Sie in der EC2 Amazon-Dokumentation.
- Wir gehen davon aus, dass Sie mit der Verwendung von Amazon Virtual Private Cloud (Amazon VPC) vertraut sind. Weitere Informationen zur Verwendung von Amazon VPC finden Sie im Amazon VPC-Benutzerhandbuch.
- Wir gehen davon aus, dass Sie die Regeln für die Standardsicherheitsgruppe für Ihre VPC, die auf dem Amazon VPC-Service basiert, nicht geändert haben. Falls ja, stellen Sie sicher, dass Sie die erforderlichen Regeln hinzufügen, um Netzwerkverkehr von Ihrer EC2 Amazon-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 Hardware- oder Softwarekosten im Voraus an. Sie zahlen nur für die genutzten Ressourcen, ohne Mindestverpflichtungen, Einrichtungskosten oder zusätzliche Gebühren. Informationen zu den Preisen und Gebühren im Zusammenhang mit dem Service finden Sie unter Amazon FSx for Lustre Pricing.

Foren von Amazon FSx for Lustre

Wenn Sie bei der Nutzung von Amazon FSx for Lustre auf Probleme stoßen, schauen Sie in den Foren nach.

Verwenden Sie Amazon FSx for Lustre zum ersten Mal?

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

1. Wenn Sie bereit sind, Ihr erstes Amazon FSx for Lustre-Dateisystem zu erstellen, versuchen Sie esErste Schritte mit Amazon FSx for Lustre.
2. Informationen zur Leistung finden Sie unter Leistung von Amazon FSx for Lustre.
3. Informationen zum Verknüpfen Ihres Dateisystems mit einem Amazon S3 S3-Bucket-Daten-Repository finden Sie unterVerwenden von Datenrepositorys mit Amazon FSx for Lustre.
4. Sicherheitsinformationen FSx zu Amazon for Lustre finden Sie unterSicherheit bei Amazon FSx for Lustre.
5. Informationen zu den Skalierbarkeitsgrenzen von Amazon FSx for Lustre, einschließlich Durchsatz und Dateisystemgröße, finden Sie unterServicekontingente für Amazon FSx for Lustre.
6. Informationen zur Amazon FSx for Lustre-API finden Sie in der Amazon FSx for Lustre-API-Referenz.

Einrichten von Amazon FSx for Lustre

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

Themen

Bei Amazon Web Services registrieren

Führen Sie zur AWS Einrichtung die folgenden Aufgaben aus:

1. Melde dich an für eine AWS-Konto
2. Erstellen eines Benutzers mit Administratorzugriff

Melde dich an für eine AWS-Konto

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

Um sich für eine anzumelden AWS-Konto

1. Öffnen Sie https://portal.aws.amazon.com/billing/die Anmeldung.
2. Folgen Sie den Online-Anweisungen.

   Während der Anmeldung erhalten Sie einen Telefonanruf oder eine Textnachricht und müssen einen Verifizierungscode über die Telefontasten eingeben.

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

Sicherheitsmethode weisen Sie einem Benutzer Administratorzugriff zu und verwenden Sie nur den Root-Benutzer, um Aufgaben auszuführen, die Root-Benutzerzugriff erfordern.

AWS sendet Ihnen nach Abschluss des Anmeldevorgangs eine Bestätigungs-E-Mail. Du kannst jederzeit deine aktuellen Kontoaktivitäten einsehen und dein Konto verwalten, indem du zu https://aws.amazon.com/gehst und Mein Konto auswählst.

Erstellen eines Benutzers mit Administratorzugriff

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

Sichern Sie Ihre Root-Benutzer des AWS-Kontos

1. Melden Sie sich AWS-Managementkonsoleals Kontoinhaber an, indem Sie Root-Benutzer auswählen und Ihre AWS-Konto E-Mail-Adresse eingeben. Geben Sie auf der nächsten Seite Ihr Passwort ein.

   Hilfe bei der Anmeldung mit dem Root-Benutzer finden Sie unter Anmelden als Root-Benutzer im AWS-Anmeldung Benutzerhandbuch zu.

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

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

Erstellen eines Benutzers mit Administratorzugriff

1. Aktivieren Sie das IAM Identity Center.

   Anweisungen finden Sie unter Aktivieren AWS IAM Identity Center im AWS IAM Identity Center Benutzerhandbuch.

2. Gewähren Sie einem Administratorbenutzer im IAM Identity Center Benutzerzugriff.

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

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 im AWS-Anmeldung Benutzerhandbuch unter Anmeldung beim AWS Access-Portal.

Weiteren Benutzern Zugriff zuweisen

1. Erstellen Sie im IAM-Identity-Center einen Berechtigungssatz, der den bewährten Vorgehensweisen für die Anwendung von geringsten Berechtigungen folgt.

   Anweisungen hierzu finden Sie unter Berechtigungssatz erstellen im AWS IAM Identity Center Benutzerhandbuch.
2. Weisen Sie Benutzer einer Gruppe zu und weisen Sie der Gruppe dann Single Sign-On-Zugriff zu.

   Eine genaue Anleitung finden Sie unter Gruppen hinzufügen im AWS IAM Identity Center Benutzerhandbuch.

Hinzufügen von Berechtigungen zur Verwendung von Datenrepositorys in Amazon S3

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

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

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

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

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

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

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

   JSON

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

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

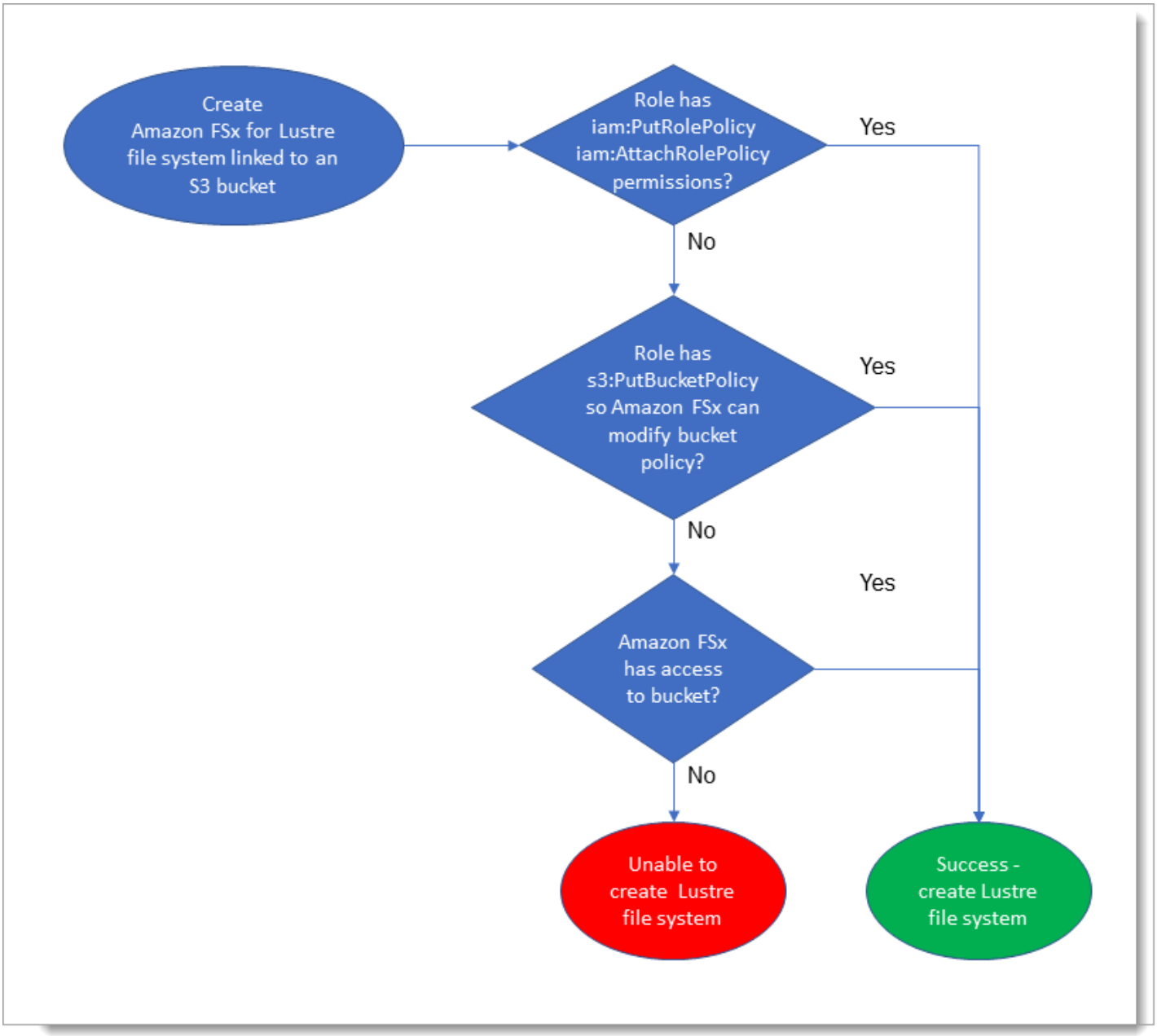
Wie FSx prüft Lustre den Zugriff auf verknüpfte S3-Buckets

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

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



Nächster Schritt

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

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 EC2 Amazon-Instance zu erstellen. Weitere Informationen finden Sie unter Einrichten von Amazon FSx for 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 FSx Amazon-Dateisystem.
- Eine EC2 Amazon-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 EC2 Amazon-Benutzerhandbuch.

Neben Amazon Linux 2023 unterstützt der Lustre Client die Betriebssysteme Amazon Linux 2, Red Hat Enterprise Linux (RHEL), CentOS, Rocky Linux, SUSE Linux Enterprise Server und Ubuntu. Weitere Informationen finden Sie unter LustreDateisystem- und Client-Kernel-Kompatibilität.

- Beachten Sie beim Erstellen Ihrer EC2 Amazon-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.
- 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 Bereitstellungs- und Speicherklassenoptionen FSx für Lustre-Dateisysteme.
- Jedes FSx for Lustre-Dateisystem benötigt eine IP-Adresse für jeden Metadatenserver (MDS) und eine IP-Adresse für jeden Speicherserver (OSS). Weitere Informationen finden Sie unter IP-Adressen für Dateisysteme.
- Ein Amazon S3 S3-Bucket, in dem die Daten gespeichert werden, die Ihr Workload verarbeiten soll. Der S3-Bucket wird das verknüpfte dauerhafte Daten-Repository für Ihr FSx for Lustre-Dateisystem sein.

Schritt 1: Erstellen Sie Ihr FSx for Lustre-Dateisystem

Sie erstellen Ihr Dateisystem in der FSx Amazon-Konsole. Beachten Sie, dass alle FSx for Lustre-Dateisysteme auf Lustre Version 2.15 basieren, wenn sie mit der FSx Amazon-Konsole erstellt wurden.

So erstellen Sie Ihr -Dateisystem:

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Dashboard die Option Dateisystem erstellen, um den Assistenten zur Dateisystemerstellung zu starten.
3. Wählen Sie FSx for Lustreund anschließend Weiter, um die Seite „Dateisystem erstellen“ aufzurufen.

   Beginnen Sie Ihre Konfiguration mit dem Abschnitt Dateisystemdetails.

4. 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.
5. Wählen Sie für Bereitstellung und Speicherklasse eine der folgenden Optionen aus:

   - Wählen Sie Persistent, SSD für längerfristige Speicherung und für latenzempfindliche Workloads. Bei SSD-Speicher wird Ihnen die Menge an Speicher in Rechnung gestellt, die Sie bereitstellen.

     Wählen Sie optional mit aktiviertem EFA, um die Elastic Fabric Adapter (EFA) -Unterstützung für das Dateisystem zu aktivieren. Weitere Informationen zu EFA finden Sie unter. Arbeiten mit EFA-fähigen Dateisystemen
   - Wählen Sie Persistent, Intelligent-Tiering für eine längerfristige Speicherung. Die Intelligent-Tiering-Speicherklasse bietet vollständig elastischen, kostengünstigen Speicher, der für die meisten Workloads geeignet ist, sowie einen optionalen SSD-Lesecache, der SSD-Latenzen für Lesevorgänge von Daten bietet, auf die häufig zugegriffen wird. Bei Intelligent-Tiering werden Ihnen die von Ihnen gespeicherten Daten je nach Größe Ihres Datensatzes in Rechnung gestellt, und Sie müssen keine Dateisystemgröße angeben.

     Wählen Sie optional mit aktiviertem EFA, um die Elastic Fabric Adapter (EFA) -Unterstützung für das Dateisystem zu aktivieren.
   - Wählen Sie Scratch, SSD-Bereitstellung für die temporäre Speicherung und kurzfristigere Verarbeitung von Daten. Bei SSD-Speicher wird Ihnen die Menge an Speicher in Rechnung gestellt, die Sie bereitstellen.
6. Wählen Sie die Durchsatzmenge für Ihr Dateisystem aus. Sie zahlen den Durchsatz, den Sie bereitstellen.

   - Wählen Sie für persistenten SSD-Speicher einen Wert für Durchsatz pro Speichereinheit. Der Durchsatz pro Speichereinheit ist die Menge des Lese- und Schreibdurchsatzes für jedes bereitgestellte 1 Tebibyte (TiB) an Speicher.
   - Wählen Sie für Scratch-SSD-Speicher einen Wert für Durchsatz pro Speichereinheit.
   - Wählen Sie für Intelligent-Tiering-Speicher einen Wert für die Durchsatzkapazität.
7. Geben Sie unter Speicherkapazität (nur SSD-Speicherklasse) die Speicherkapazität für Ihr Dateisystem in TB an:

   - 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.

- Für einen EFA-fähigen, persistenten SSD-Bereitstellungstyp legen Sie diesen Wert in Schritten von 4,8 TiB, 9,6 TiB, 19,2 TiB und 38,4 TiB für die Durchsatzstufen 1000, 500, 250 bzw. 125 TiB fest. MBps

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

8. Wählen Sie für die Metadatenkonfiguration eine der folgenden Optionen, um die Anzahl der Metadaten-IOPS für Ihr Dateisystem bereitzustellen:

   - Wählen Sie Automatisch (nur SSD-Speicherklasse), wenn Amazon FSx for Lustre die Metadaten-IOPS auf Ihrem Dateisystem basierend auf der Speicherkapazität Ihres Dateisystems automatisch bereitstellen und skalieren soll.
   - Wählen Sie Benutzerbereitgestellt, wenn Sie die Anzahl der Metadaten-IOPS angeben möchten, die für Ihr Dateisystem mit SSD- oder Intelligent-Tiering-Speicherklasse bereitgestellt werden sollen. Gültige Werte sind:
     - Für SSD-Dateisysteme sind die Werte,, `1500` `30006000`, `12000` und ein Vielfaches von bis zu einem Maximum von gültig. `12000` `192000`
     - Für Intelligent-Tiering-Dateisysteme sind die gültigen Werte und. `6000` `12000`

   Weitere Informationen zu Metadaten-IOPS finden Sie unter. LustreKonfiguration der Metadaten-Leistung

9. Wählen Sie für den SSD-Lesecache (nur Intelligent-Tiering) entweder Automatisch (proportional zur Durchsatzkapazität) oder Benutzerdefiniert (vom Benutzer bereitgestellt). Mit der Option Automatisch wählt Amazon FSx for Lustre automatisch eine Lese-Cache-Größe, die auf Ihrem bereitgestellten Durchsatz basiert. Wenn Sie die ungefähre Größe Ihres aktiven Arbeitsdatensatzes kennen, können Sie Benutzerdefiniert auswählen, um die Größe des SSD-Lesecaches anzupassen. Weitere Informationen finden Sie unter Verwaltung des bereitgestellten SSD-Lesecache.
10. Wählen Sie als Datenkomprimierungstyp die Option KEINE aus, um die Datenkomprimierung zu deaktivieren, oder wählen Sie LZ4, ob die Datenkomprimierung mit dem LZ4 Algorithmus aktiviert werden soll. Weitere Informationen finden Sie unter LustreDatenkomprimierung.
11. Geben Sie im Abschnitt Netzwerk und Sicherheit die folgenden Informationen zu Netzwerken und Sicherheitsgruppen 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 EC2 Amazon-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_this_security_group*	Regel für eingehenden Lustre Verkehr

> **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.
> - Wenn Sie ein EFA-fähiges Dateisystem erstellen, stellen Sie sicher, dass Sie eine EFA-fähige Sicherheitsgruppe angeben.

- Wählen Sie für Subnetz einen beliebigen Wert aus der Liste der verfügbaren Subnetze aus.

12. 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 EC2 Amazon-Instance-Typ auf das Dateisystem zugegriffen wird. Weitere Informationen finden Sie unter Verschlüsseln von Daten während der Übertragung.

13. Im optionalen Abschnitt Datenrepository-Import/Export 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.
> - Intelligent-Tiering-Dateisysteme unterstützen keine Verknüpfung mit Amazon S3 S3-Datenrepositorys.

14. Bei der optionalen Protokollierung 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 unterVerwaltung der Protokollierung.
15. Unter Backup und Wartung optional können Sie Folgendes tun.

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

- Legen Sie die Startzeit für das wöchentliche Wartungsfenster fest, oder behalten Sie die Standardeinstellung Keine Präferenz bei.

Weitere Informationen erhalten Sie unter Schützen Sie Ihre Daten mit Backups und Wartungsfenster FSx von Amazon for Lustre.

16. Bei der optionalen Option Root Squash 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
17. Erstellen Sie alle Tags, die Sie auf Ihr Dateisystem anwenden möchten.
18. Wählen Sie Weiter, um die Übersichtsseite „Dateisystem erstellen“ aufzurufen.
19. Überprüfen Sie die Einstellungen für Ihr Amazon FSx for Lustre-Dateisystem und wählen Sie Dateisystem erstellen.

Nachdem Sie Ihr Dateisystem erstellt haben, notieren Sie sich den vollständig qualifizierten 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 Dateisystem-Dashboard auswählen und dann Anhängen wählen.

Schritt 2: Installieren und konfigurieren Sie den Lustre Client

Bevor Sie von Ihrer EC2 Amazon-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 Client mit dem Lustre 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 Instances zurückgibt, aktualisieren Sie den Kernel und starten Sie Ihre EC2 EC2 Amazon-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.

   Hinweise zur Installation des Lustre Clients auf anderen Linux-Distributionen finden Sie unterDen Client installieren Lustre.

Schritt 3: Mounten Sie das Dateisystem

Um Ihr Dateisystem zu mounten, 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, dass das FSx Amazon-Dateisystem gemountet iston /mnt/fsx.

Schritt 4: 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 unterIhr Dateisystem mit einem Amazon S3 S3-Bucket verknüpfen.

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

Schritt 5: 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 EC2 Amazon-Konsole. Weitere Informationen finden Sie unter Terminate Your Instance im EC2 Amazon-Benutzerhandbuch.
3. Löschen Sie Ihr Dateisystem auf der Amazon FSx for Lustre-Konsole wie folgt:

   a. Wählen Sie im Navigationsbereich Dateisysteme aus.

   b. Wählen Sie das Dateisystem, das Sie löschen möchten, aus der Liste der Dateisysteme im Dashboard aus.

   c. Klicken Sie bei Aktionen auf Dateisystem löschen.

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

Bereitstellungs- und Speicherklassenoptionen FSx für Lustre-Dateisysteme

Amazon FSx for Lustre bietet zwei Bereitstellungsoptionen für Dateisysteme: persistent und Scratch. Es bietet drei Speicherklassen: SSD (Solid-State-Laufwerk) und HDD (Festplattenlaufwerk). AWS Interconnect

Sie wählen den Bereitstellungstyp und die Speicherklasse des Dateisystems, wenn Sie ein neues Dateisystem mit der AWS-Managementkonsole AWS Command Line Interface (AWS CLI) oder der Amazon FSx for Lustre-API erstellen. Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie Ihr FSx for Lustre-Dateisystem und CreateFileSystemin der Amazon FSx API-Referenz.

Persistente Dateisysteme

Persistente Dateisysteme sind für längerfristige Speicherung und Workloads konzipiert, und die Dateiserver sind hochverfügbar. Bei SSD- und HDD-basierten Dateisystemen werden Daten automatisch innerhalb derselben Availability Zone repliziert, in der sich das Dateisystem befindet. Bei Intelligent-Tiering-Dateisystemen werden Daten über mehrere Availability Zones hinweg repliziert. Die an die Dateiserver angehängten Datenvolumen werden unabhängig von den Dateiservern repliziert, an die sie angeschlossen sind.

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

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

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

Amazon FSx for Lustre unterstützt zwei persistente Bereitstellungstypen: Persistent 1 und Persistent 2.

Bereitstellungstyp Persistent 2

Persistent 2 ist die neueste Generation des Bereitstellungstyps Persistent und eignet sich am besten für Anwendungsfälle, die eine längerfristige Speicherung erfordern und die höchsten IOPS- und Durchsatzraten erfordern. Persistent 2-Dateisysteme unterstützen SSD- und Intelligent-Tiering-Speicherklassen.

Sie können Persistent 2-Dateisysteme mit einer Metadatenkonfiguration und aktiviertem EFA mithilfe der FSx Amazon-Konsole und der FSx Amazon-API erstellen. AWS Command Line Interface

Persistent: 1 Bereitstellungstyp

Der Bereitstellungstyp Persistent 1 eignet sich gut für Anwendungsfälle, die eine längerfristige Speicherung erfordern. Die Bereitstellungstypen Persistent 1 unterstützen die Speicherklassen SSD (Solid State Drive) und HDD (Hard Disk Drive).

Sie können Bereitstellungstypen Persistent 1 nur mithilfe der AWS CLI und der FSx Amazon-API erstellen.

Scratch-Dateisysteme

Scratch-Dateisysteme sind für die temporäre Speicherung und die kurzfristigere Verarbeitung von Daten konzipiert. Daten werden nicht repliziert und bleiben auch dann nicht erhalten, wenn ein Dateiserver ausfällt. Scratch-Dateisysteme bieten einen hohen Burst-Durchsatz, der bis zum Sechsfachen des Basisdurchsatzes von 200 MBps pro TiB Speicherkapazität beträgt. Weitere Informationen finden Sie unter Leistungsmerkmale der SSD- und HDD-Speicherklassen.

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

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

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

Dateisystemgröße (TiB)	Anzahl der Dateiserver	Verfügbarkeit/Haltbarkeit über einen Tag	Verfügbarkeit/Haltbarkeit über eine Woche
1.2	2	99,9 %	99,4%
2.4	2	99,9 %	99,4%
4,8	3	99,8%	99,2%
9,6	5	99,8%	98,6%
50,4	22	99,1%	93,9%

IP-Adressen für Dateisysteme

Jedes Dateisystem FSx für Lustre benötigt eine IP-Adresse für jeden Metadatenserver (MDS) und eine IP-Adresse für jeden Speicherserver (OSS).

Dateisysteme, die die SSD- oder HDD-Speicherklasse verwenden

Typ des Dateisystems	Durchsatz, MBps /TiB	Speicher pro Betriebssystem
Persistent 2 EFA*	125	38,4 TiB pro Betriebssystem
	250	19,2 TiB pro Betriebssystem
	500	9,6 TiB pro Betriebssystem
	1000	4,8 TiB pro Betriebssystem

Typ des Dateisystems	Durchsatz, MBps /TiB	Speicher pro Betriebssystem
Persistent 2 Nicht-EFA*	125, 250, 500, 1000	2,4 TiB pro Betriebssystem
Persistent 1 SSD	50, 100, 200	2,4 TiB pro Betriebssystem
Persistente Festplatte	12	6 TiB pro Betriebssystem
	40	1,8 TiB pro Betriebssystem
Kratzer 2	200	2,4 TiB pro Betriebssystem
Kratzer 1	200	3,6 TiB pro Betriebssystem

Dateisysteme, die die Intelligent-Tiering-Speicherklasse verwenden

Typ des Dateisystems	Durchsatz pro Betriebssystem
Intelligentes Tiering*	4000 pro Betriebssystem MBps

> **Note**
>
> * Amazon stellt FSx einen Metadatenserver für jeweils 12.000 Metadaten-IOPS auf Persistent 2 SSD- und Intelligent-Tiering-Dateisystemen bereit, die mit Metadatenkonfiguration konfiguriert sind.
> Die Intelligent-Tiering-Dateisysteme von Amazon FSx for Lustre unterstützen maximal 512 TiB Speicher pro Betriebssystem.

FSx für Lustre-Speicherklassen

Amazon FSx for Lustre bietet Speicherklassen für Solid State Drive (SSD) und Hard Disk Drive (HDD), die für unterschiedliche Datenverarbeitungsanforderungen optimiert sind: AWS Interconnect

- Die SSD-Speicherklasse bietet Zugriff mit geringer Latenz (unter einer Millisekunde) auf Ihren gesamten Datensatz. Die SSD-Speicherklasse wird bereitgestellt, was bedeutet, dass Sie eine Dateisystemgröße angeben und die Speicherkosten für die Menge des bereitgestellten Speichers zahlen. Verwenden Sie die SSD-Speicherklasse für latenzempfindliche Workloads, die die Leistung eines All-Flash-Speichers für alle Daten erfordern.

  Persistent 2-Dateisysteme mit SSD-Speicher unterstützen im Vergleich zu Persistent 1-Dateisystemen einen höheren Durchsatz MBps pro Speichereinheit (d. h. 250, 500 oder 1000 pro TiB). Bei einem Persistent 1-Dateisystem mit SSD-Speicher beträgt der Durchsatz pro Speichereinheit entweder 50, 100 oder 200 MBps pro TiB. Bei einem Scratch-Dateisystem mit SSD-Speicher beträgt der Durchsatz pro Speichereinheit 200 MBps pro TiB.
- Die Intelligent-Tiering-Speicherklasse bietet vollständig elastischen, intelligent gestaffelten Speicher. Elastizität bedeutet, dass Sie für die Menge der gespeicherten Daten zahlen und keine Dateisystemgröße angeben müssen. Intelligentes Tiering bedeutet, dass Sie automatisch weniger für das Speichern von Daten zahlen, auf die Sie in letzter Zeit nicht zugegriffen haben. Bei dieser Speicherklasse werden die Kosten automatisch optimiert, indem kalte Daten auf kostengünstigere Speicherstufen aufgeteilt werden. Sie können einen optionalen SSD-Lesecache für den Zugriff auf Ihre häufig abgerufenen Daten mit geringer Latenz (unter einer Millisekunde) bereitstellen. Die Intelligent-Tiering-Speicherklasse bietet für die meisten Workloads das beste Preis-Leistungs-Verhältnis. Verwenden Sie die Intelligent-Tiering-Speicherklasse für Workloads, die Cache-freundlich sind und nicht die Leistung eines All-Flash-Speichers für alle Daten erfordern. Intelligent-Tiering-Dateisysteme unterstützen Durchsatzkapazitäten in Schritten von 4000. MBps
- Die HDD-Speicherklasse kann für Workloads verwendet werden, die eine konsistente Latenz im einstelligen Millisekundenbereich für alle Daten benötigen. Sie können einen optionalen SSD-Lesecache bereitstellen, der auf 20% Ihrer Festplattenspeicherkapazität ausgelegt ist, um Zugriff mit geringer Latenz auf häufig abgerufene Daten zu ermöglichen. Beim Festplattenspeicher geben Sie eine Dateisystemgröße an und zahlen für die Menge an Speicher, die Sie bereitstellen. Bei einem Persistent 1-Dateisystem mit Festplattenspeicher beträgt der Durchsatz pro Speichereinheit entweder 12 oder 40 MBps pro TiB.

Weitere Informationen zur Leistung dieser Speicherklassen finden Sie unter Leistungsmerkmale der SSD- und HDD-Speicherklassen undLeistungsmerkmale der Intelligent-Tiering-Speicherklasse.

Wie die Intelligent-Tiering-Speicherklasse Daten einteilt

Die Amazon FSx Intelligent-Tiering-Speicherklasse speichert Daten automatisch in drei Zugriffsebenen. Sie wurde entwickelt, um die Speicherkosten zu optimieren, indem Daten automatisch auf die kostengünstigste Zugriffsebene verschoben werden, ohne dass sich dies auf die Leistung oder den Betriebsaufwand auswirkt. Die Intelligent-Tiering-Speicherklasse stuft Daten automatisch auf der Grundlage der letzten Zugriffszeit ab und optimiert so automatisch die Kosten für weniger aktive Daten:

- Daten, auf die in den letzten 30 Tagen zugegriffen wurde, werden in der Stufe „Häufiger Zugriff“ gespeichert.
- Daten, auf die an 30 aufeinanderfolgenden Tagen nicht zugegriffen wurde, werden automatisch in die Stufe für seltenen Zugriff verschoben und kosten weniger als Daten in der Stufe für häufigen Zugriff.
- Daten, auf die innerhalb von 90 aufeinanderfolgenden Tagen nicht zugegriffen wurde, werden automatisch in den Tarif Archive Instant Access verschoben und kosten weniger als Daten im Tarif für seltenen Zugriff.

Wenn Sie auf Daten der Stufen Infrequent Access oder Archive Instant Access zugreifen, werden die Daten automatisch wieder in die Stufe für häufigen Zugriff verschoben. Jeder Zugriff auf nicht zwischengespeicherte Daten weist unabhängig von der Datenebene dieselben Leistungsmerkmale auf, und es fallen keine zusätzlichen IOPS-, Abruf- oder Übergangskosten an, die über Ihre normalen Betriebskosten hinausgehen. read/write

Art der Bereitstellung, Verfügbarkeit

Die Bereitstellungstypen Scratch 2, Persistent 1 und Persistent 2 sind in den folgenden Versionen verfügbar AWS-Regionen:

AWS-Region	Persistent 2	Hartnäckig 1	Kratzer 2
US East (Ohio)	✓	✓	✓
USA Ost (Nord-Virginia)	✓	✓	✓

AWS-Region	Persistent 2	Hartnäckig 1	Kratzer 2
Lokale Zone USA Ost (Atlanta)	✓ *		
Lokale Zone USA Ost (Dallas)	✓ *		
USA West (Nordkalifornien)	✓	✓	✓
Lokale Zone USA West (Los Angeles)		✓	✓
USA West (Oregon)	✓	✓	✓
Lokale Zone USA West (Phoenix)	✓ *		
Afrika (Kapstadt)		✓	✓
Asien-Pazifik (Hongkong)	✓	✓	✓
Asien-Pazifik (Hyderabad)		✓	✓
Asien-Pazifik (Jakarta)		✓	✓
Asien-Pazifik (Malaysia)	✓ *		
Asien-Pazifik (Melbourne)		✓	✓
Asien-Pazifik (Mumbai)	✓	✓	✓
Asien-Pazifik (Osaka)		✓	✓
Asien-Pazifik (Seoul)	✓	✓	✓
Asien-Pazifik (Singapur)	✓	✓	✓
Asien-Pazifik (Sydney)	✓	✓	✓
Asien-Pazifik (Taipeh)	✓ *		
Asien-Pazifik (Thailand)	✓ *		
Asien-Pazifik (Tokio)	✓	✓	✓

AWS-Region	Persistent 2	Hartnäckig 1	Kratzer 2
Canada (Central)	✓	✓	✓
Kanada West (Calgary)	✓ *		
Europe (Frankfurt)	✓	✓	✓
Europa (Irland)	✓	✓	✓
Europa (London)	✓	✓	✓
Europa (Milan)		✓	✓
Europa (Paris)		✓	✓
Europa (Spain)		✓	✓
Europa (Stockholm)	✓	✓	✓
Europa (Zürich)		✓	✓
Israel (Tel Aviv)	✓ *		✓
Mexiko (Zentral)	✓ *		
Middle East (Bahrain)		✓	✓
Naher Osten (VAE)		✓	✓
Südamerika (São Paulo)		✓	✓
AWS GovCloud (US-Ost)		✓	✓
AWS GovCloud (US-West)		✓	✓

Note

* Diese AWS-Regionen unterstützen die Dateisysteme Persistent-125 und Persistent-250 mit SSD-Speicherklasse ohne EFA.

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 Amazon S3 S3-Daten-Repository verknüpft sind, nicht unterstützt. Weitere Informationen finden Sie unter Schützen Sie Ihre Daten mit Backups.
> - Intelligent-Tiering-Dateisysteme unterstützen keine Verknüpfung mit Amazon S3 S3-Datenrepositorys.

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

> **Note**
>
> Datenrepository-Verknüpfungen, automatischer Export und Unterstützung für mehrere Daten-Repositorys sind auf FSx Lustre 2.10-Dateisystemen oder `Scratch 1` Dateisystemen nicht verfügbar.

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 EC2 Amazon-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 and/or 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. Direct Connect

> **Important**
>
> Wenn Sie eines 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.

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

Unterstützung von POSIX-Metadaten für Datenrepositorys

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 zugehörige 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 in diesem Dateisystem dieselben POSIX-Metadaten haben, einschließlich Eigentum und Berechtigungen.

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

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

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

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

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

- S3-Objektschlüssel — Der Pfad zum Link, relativ zum Mount-Verzeichnis FSx für Lustre
- 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 keine `setuid` 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. Beendet den Zeitwert mit`ns`; andernfalls interpretiert Lustre FSx den Wert als Millisekunden.
- `x-amz-meta-file-mtime`— Die letzte Änderung in Nanosekunden seit Beginn der Unix-Epoche. Beendet den Zeitwert mit`ns`; andernfalls interpretiert FSx for Lustre den Wert als Millisekunden.
- `x-amz-meta-user-agent`— Der Benutzeragent, der während des Lustre-Imports ignoriert wurde. FSx Während des Exports wird dieser Wert FSx für Lustre auf gesetzt. `aws-fsx-lustre`

Beim Import von Objekten aus S3, denen keine POSIX-Berechtigungen zugeordnet sind, ist die POSIX-Standardberechtigung, die FSx für Lustre einer Datei zugewiesen wird, `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 Amazon 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 Datenrepository-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

Hardlinks 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 Datenrepository-Verknüpfungen (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 FSx Amazon-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 Datenrepositorys

   *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 FSx Amazon-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.

Ihr Dateisystem mit einem Amazon S3 S3-Bucket verknüpfen

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

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

> **Note**
>
> Datenrepository-Verknüpfungen, automatischer Export und Unterstützung für mehrere Daten-Repositorys sind FSx für Lustre 2.10-Dateisysteme oder Dateisysteme 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, geändert oder aus dem Datenrepository 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, dass widersprüchliche Schreibvorgänge an mehreren Speicherorten auftreten.
> - 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 die Leistung der Datenbewegung zwischen Amazon FSx und S3 beeinträchtigt wird.

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://`*`bucket-name`*`/`*`prefix`*`/` sein. Diese Eigenschaft gibt an, aus welchem Bereich des S3-Datenrepositorys Dateien importiert oder exportiert werden. FSx for Lustre fügt Ihrem Datenrepository-Pfad ein abschließendes „/“ an, falls Sie keinen angeben. Wenn

Sie beispielsweise einen Datenrepository-Pfad von angeben`s3://amzn-s3-demo-bucket/my-prefix`, FSx denn Lustre interpretiert ihn als. `s3://amzn-s3-demo-bucket/my-prefix/`

Zwei Datenrepository-Assoziationen dürfen sich nicht überlappen. Wenn beispielsweise ein Datenrepository mit Pfad mit dem Dateisystem verknüpft `s3://amzn-s3-demo-bucket/my-prefix/` ist, können Sie keine weitere Datenrepository-Assoziation mit dem Datenrepository-Pfad `s3://amzn-s3-demo-bucket/my-prefix/my-sub-prefix` erstellen.

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

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

Themen

Einen Link zu einem S3-Bucket erstellen

Die folgenden Verfahren führen Sie Schritt für Schritt durch den Prozess der Erstellung einer Datenrepository-Zuordnung FSx für ein for Lustre-Dateisystem zu einem vorhandenen S3-Bucket mithilfe von AWS-Managementkonsole 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 unterHinzufügen von Berechtigungen zur Verwendung von Datenrepositorys in Amazon S3.

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

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

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, das Schritt 1: Erstellen Sie Ihr FSx for Lustre-Dateisystem im Abschnitt Erste Schritte beschrieben ist.
3. Öffnen Sie den Abschnitt Data Repository 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 übergeordneten Verzeichnisses (z. B.`/ns1`) oder eines Unterverzeichnisses (z. B.`/ns1/subdir`) innerhalb des FSx Amazon-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://amzn-s3-demo-bucket/my-`

`prefix`). Zwei Datenrepository-Verknüpfungen dürfen sich nicht überlappen. Die Einstellung für den Datenrepository-Pfad muss für alle Datenrepositoryzuordnungen 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 unter Einstellungen importieren — 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 unterAutomatischer Import 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 FSx Amazon-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 übergeordneten Verzeichnisses (z. B.`/ns1`) oder eines Unterverzeichnisses (z. B.`/ns1/subdir`) innerhalb des FSx Amazon-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://amzn-s3-demo-bucket/my-prefix`). Zwei Datenrepository-Verknüpfungen dürfen sich nicht überlappen. Die Einstellung für den Datenrepository-Pfad muss für alle Datenrepositoryzuordnungen 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 unter Einstellungen importieren — 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 unterAutomatischer Import 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 Erstellen aus.

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

Das folgende Beispiel erstellt eine Datenrepository-Zuordnung, die ein FSx Amazon-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://amzn-s3-demo-bucket/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-Managementkonsole AWS CLI, der und der FSx Amazon-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 FSx Amazon-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 unterAutomatischer Import 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 Datenrepository-Verknüpfung FSx gibt Amazon die Beschreibung der aktualisierten Datenrepository-Verknüpfung 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 FSx Amazon-Dateisystem zu einem vorhandenen S3-Bucket mithilfe von AWS-Managementkonsole 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 FSx Amazon-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. Im Dialogfeld Löschen können Sie Daten im Dateisystem löschen wählen, um die Daten im Dateisystem, die der Datenrepository-Zuordnung entsprechen, physisch zu löschen.

Wählen Sie diese Option, wenn Sie planen, eine neue Datenrepository-Zuordnung zu erstellen, die denselben Dateisystempfad verwendet, aber auf ein anderes S3-Bucket-Präfix verweist, oder wenn Sie die Daten in Ihrem Dateisystem nicht mehr benötigen.

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 FSx Amazon-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
```

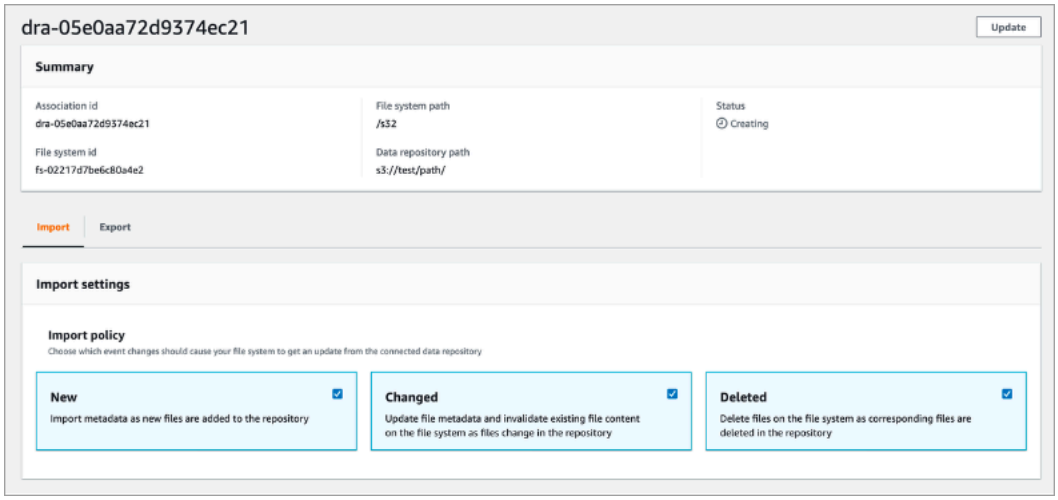
Nach dem erfolgreichen Löschen der Datenrepository-Zuordnung FSx gibt Amazon die Beschreibung als JSON zurück.

Details zur Datenrepository-Zuordnung anzeigen

Sie können die Details einer Datenrepository-Verknüpfung mithilfe der FSx for Lustre-Konsole AWS 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 FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Dashboard Dateisysteme und dann das Dateisystem aus, für das Sie die Details einer Datenrepository-Zuordnung anzeigen möchten.
3. Wählen Sie die Registerkarte Daten-Repository.
4. Wählen Sie im Bereich Datenrepository-Verknüpfungen die Datenrepository-Zuordnung aus, die Sie anzeigen möchten. Die Übersichtsseite mit den DRA-Details wird angezeigt.



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 erstellt FSx die Datenrepository-Verknüpfung 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 Datenrepository-Zuordnung korrigiert ist.

  Ein DRA kann aus folgenden Gründen falsch konfiguriert werden:

  - Amazon FSx fehlen die erforderlichen IAM-Berechtigungen für den Zugriff auf den S3-Bucket.
  - Die Konfiguration der FSx Ereignisbenachrichtigung im S3-Bucket wurde gelöscht oder geändert.
  - Der S3-Bucket enthält bereits Ereignisbenachrichtigungen, die sich mit FSx Ereignistypen überschneiden.

  Nach der Behebung des zugrundeliegenden Problems kehrt der DRA innerhalb von 15 Minuten automatisch in den Status Verfügbar zurück, oder Sie können die Statusänderung sofort mithilfe des AWS CLI Befehls update-data-repository-associationauslösen.
- 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 FSx Amazon-Konsole AWS Command Line Interface, der und der FSx Amazon-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 FSx , dass Amazon 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 FSx befolgt Amazon die Standard-Verschlüsselungsrichtlinie Ihres S3-Buckets.

Standardmäßig FSx unterstützt Amazon S3-Buckets, die mit SSE-S3 verschlüsselt wurden. Wenn Sie Ihr FSx Amazon-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 ermöglicht, Objekte in Ihrem S3-Bucket mit Ihrem KMS-Schlüssel FSx zu verschlüsseln und zu entschlüsseln.

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

```
{
    "Sid": "Allow access through S3 for the FSx SLR to use the KMS key on the objects
 in the given S3 bucket",
    "Effect": "Allow",
    "Principal": {
        "AWS": "arn:aws:iam::aws_account_id:role/aws-service-role/s3.data-
source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fsx_file_system_id"
    },
    "Action": [
        "kms:Encrypt",
        "kms:Decrypt",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*",
        "kms:DescribeKey"
    ],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "aws_account_id",
            "kms:ViaService": "s3.bucket-region.amazonaws.com"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
        }
    }
}
```

Note

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 FSx Amazon-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:ViaService": "s3.bucket-region.amazonaws.com",
          "kms:CallerAccount": "aws_account_id"
        },
        "StringLike": {
            "kms:EncryptionContext:aws:s3:arn": "arn:aws:s3:::bucket_name/*"
        },
        "ArnLike": {
          "aws:PrincipalArn": "arn:aws_partition:iam::aws_account_id:role/aws-service-
role/s3.data-source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fs-*"
        }
      }
}
```

Zugreifen auf serverseitig verschlüsselte Amazon S3 S3-Buckets in einer anderen AWS-Konto oder von einer gemeinsam genutzten VPC

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-Spiegelreflexkamera), 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 FSx Amazon-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 Automatischer Import 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 Daten-Repositorys 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 ausgeführt.

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 beim automatischen Import als auch beim Import von Datenrepositorys werden POSIX-Metadaten importiert. Weitere Informationen finden Sie unter Unterstützung von POSIX-Metadaten für Datenrepositorys.

> **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, bei denen es sich nicht um Symlinks handelt, können importiert werden (d. h., es wird ein Inode im 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.

Automatischer Import von Updates aus Ihrem S3-Bucket

Sie können Lustre so konfigurieren FSx , 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 Verzeichnis befinden, AWS-Region damit Updates automatisch importiert werden 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 Managementkonsole AWS CLI, die oder die AWS API aktualisieren.

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

> **Important**
>
> - Wenn ein Objekt in S3 geändert wird, wobei alle automatischen Importrichtlinien aktiviert und der automatische Export deaktiviert sind, wird der Inhalt dieses Objekts immer in eine entsprechende Datei im Dateisystem importiert. Wenn am Zielort bereits eine Datei vorhanden ist, wird die Datei überschrieben.
> - Wenn eine Datei sowohl im Dateisystem als auch in S3 geändert wird und alle automatischen Import- und Exportrichtlinien aktiviert sind, kann entweder die Datei im

Dateisystem oder das Objekt in S3 durch die andere überschrieben werden. Es ist nicht garantiert, dass eine spätere Bearbeitung an einem Ort eine frühere Bearbeitung an einem anderen Ort überschreibt. Wenn Sie dieselbe Datei sowohl im Dateisystem als auch im S3-Bucket ändern, sollten Sie die Koordination auf Anwendungsebene sicherstellen, um solche Konflikte zu vermeiden. FSx for Lustre verhindert nicht, dass widersprüchliche Schreibvorgänge an mehreren Speicherorten auftreten.

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

- Neu — FSx für Lustre werden Datei- und Verzeichnismetadaten nur dann automatisch aktualisiert, wenn dem verknüpften S3-Datenrepository neue Objekte hinzugefügt werden.
- Geändert — FSx für Lustre werden Datei- und Verzeichnismetadaten nur dann automatisch aktualisiert, wenn ein vorhandenes Objekt im Daten-Repository geändert wird.
- Gelöscht — FSx für Lustre werden Datei- und Verzeichnismetadaten nur dann automatisch aktualisiert, wenn ein Objekt im Daten-Repository gelöscht wird.
- Beliebige Kombination aus Neu, Geändert und Gelöscht — FSx bei Lustre werden Datei- und Verzeichnismetadaten automatisch aktualisiert, wenn eine der angegebenen Aktionen im S3-Daten-Repository 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 denn 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 Linked 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 zur Aktualisierung Ihrer Dateisystemdatei und Ihrer Verzeichnismetadaten auf der Grundlage von Änderungen im verknüpften S3-Datenrepository festlegen, 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-Daten-Repository 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, z. B. für. `GetBucketAcl` Dadurch wird der Lebenszyklusstatus des Datenrepositorys auf „Fehlkonfiguriert“ gesetzt. 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 Lustre automatisch neue, geänderte oder gelöschte Dateien aus dem verknüpften S3-Bucket importieren kann: FSx

- 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), FSx löscht Lustre das entsprechende Verzeichnis im Dateisystem nur, wenn es leer ist.

Importeinstellungen werden aktualisiert

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

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

Überwachung des automatischen Imports

Wenn die Änderungsrate in Ihrem S3-Bucket die Geschwindigkeit übersteigt, mit der der automatische Import diese Änderungen verarbeiten kann, werden die entsprechenden Metadatenänderungen, die in Ihr FSx for Lustre-Dateisystem importiert werden, verzögert. In diesem Fall können Sie anhand der `AgeOfOldestQueuedMessage` Metrik das Alter der ältesten Änderung überwachen, die darauf wartet, vom automatischen Import verarbeitet zu werden. Weitere Informationen zu dieser Metrik finden Sie unterFSx für Lustre S3-Repository-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 Ihr FSx for Lustre-Dateisystem weiterhin 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 Synchronisierung der Dateisystemänderungen mit S3 fort. Um die Metadaten neuer und geänderter Objekte in S3 mit Ihrem FSx for Lustre-Dateisystem zu synchronisieren, die nicht importiert wurden oder aus einer Zeit stammen, in der sich die Datenrepository-Zuordnung in einem falsch konfigurierten Zustand befand, führen Sie eine Aufgabe zum Importieren von Datenrepositorys aus. Bei Aufgaben zum Importieren von Datenrepositorys 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 kann. 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 nach Abschluss der S3-Änderung neu erstellen, 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 and/or 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 FSx für Lustre verfügbaren Metriken finden Sie unterÜberwachung mit Amazon CloudWatch.

Verwenden von Datenrepository-Aufgaben zum Importieren von Änderungen

Die Aufgabe Datenrepository importieren importiert Metadaten von Objekten, die in Ihrem S3-Daten-Repository neu sind oder geändert wurden, und erstellt eine neue Datei- oder Verzeichnisliste für jedes neue Objekt im S3-Daten-Repository. 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 FSx Amazon-Konsole und CLI zu importieren. Beachten Sie, dass Sie eine Datenrepository-Aufgabe für mehrere verwenden können DRAs.

Um Änderungen an Metadaten zu importieren (Konsole)

1. Öffnen Sie die FSx Amazon-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 den Amazon den Bericht liefern FSx soll, geben Sie einen relativen Pfad in einem verknüpften S3-Datenrepository als Berichtspfad ein.
8. Wählen Sie 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 FSx gibt Amazon die Aufgabenbeschreibung als JSON zurück.

Nachdem Sie die Aufgabe zum Importieren von Metadaten aus dem verknüpften Datenrepository erstellt haben, können Sie den Status der Aufgabe zum Importieren des Datenrepositorys überprüfen. Weitere Informationen zum Anzeigen von Datenrepository-Aufgaben finden Sie unterZugreifen auf Datenrepository-Aufgaben.

Vorladen von Dateien in Ihr Dateisystem

Sie können optional Inhalte einzelner Dateien oder Verzeichnisse vorab in Ihr Dateisystem laden.

Dateien mithilfe von HSM-Befehlen importieren

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. *`path/to/file`*Ersetzen Sie es 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 vorladen, 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, FSx lädt Amazon Ihre Dateien parallel aus Ihrem Amazon S3 S3-Daten-Repository. Wenn eine Datei bereits in das Dateisystem geladen wurde, wird sie durch den `hsm_restore` Befehl nicht erneut geladen.

```
nohup find local/directory -type f -print0 | xargs -0 -n 1 -P 8 sudo lfs hsm_restore &
```

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

Schritt zur Validierung

Sie können das unten aufgeführte Bash-Skript ausführen, um herauszufinden, wie viele Dateien oder Objekte sich in einem archivierten (veröffentlichten) Zustand befinden.

Um die Leistung des Skripts zu verbessern, insbesondere in Dateisystemen mit einer großen Anzahl von Dateien, werden CPU-Threads automatisch anhand der `/proc/cpuproc` Datei bestimmt. Das heißt, Sie werden eine schnellere Leistung mit einer EC2 Amazon-Instance mit einer höheren vCPU-Anzahl feststellen.

1. Richten Sie das Bash-Skript ein.

```
#!/bin/bash

# Check if a directory argument is provided
```

```
if [ $# -ne 1 ]; then
    echo "Usage: $0 /path/to/lustre/mount"
    exit 1
fi

# Set the root directory from the argument
ROOT_DIR="$1"

# Check if the provided directory exists
if [ ! -d "$ROOT_DIR" ]; then
    echo "Error: Directory $ROOT_DIR does not exist."
    exit 1
fi

# Automatically detect number of CPUs and set threads
if command -v nproc &> /dev/null; then
    THREADS=$(nproc)
elif [ -f /proc/cpuinfo ]; then
    THREADS=$(grep -c ^processor /proc/cpuinfo)
else
    echo "Unable to determine number of CPUs. Defaulting to 1 thread."
    THREADS=1
fi

# Output file
OUTPUT_FILE="released_objects_$(date +%Y%m%d_%H%M%S).txt"

echo "Searching in $ROOT_DIR for all released objects using $THREADS threads"
echo "This may take a while depending on the size of the filesystem..."

# Find all released files in the specified lustre directory using parallel
# If you  get false positives for file names/paths that include the word
 'released',
# you can grep 'released exists archived' instead of just 'released'
time sudo lfs find "$ROOT_DIR" -type f | \
parallel --will-cite -j "$THREADS" -n 1000 "sudo lfs hsm_state {} | grep released"
 > "$OUTPUT_FILE"

echo "Search complete. Released objects are listed in $OUTPUT_FILE"
echo "Total number of released objects: $(wc -l <"$OUTPUT_FILE")"
```

2. Machen Sie das Skript ausführbar:

```
$ chmod +x find_lustre_released_files.sh
```

3. Führen Sie das Skript wie im folgenden Beispiel aus:

```
$ ./find_lustre_released_files.sh /fsxl/sample
Searching in /fsxl/sample for all released objects using 16 threads
This may take a while depending on the size of the filesystem...
real 0m9.906s
user 0m1.502s
sys 0m5.653s
Search complete. Released objects are listed in
 released_objects_20241121_184537.txt
Total number of released objects: 30000
```

Wenn freigegebene Objekte vorhanden sind, führen Sie eine Massenwiederherstellung der gewünschten Verzeichnisse durch, in die die Dateien von S3 FSx für Lustre übertragen werden sollen, wie im folgenden Beispiel:

```
$ DIR=/path/to/lustre/mount
$ nohup find $DIR -type f -print0 | xargs -0 -n 1 -P 8 sudo lfs hsm_restore &
```

Beachten Sie, dass `hsm_restore` dies bei Millionen von Dateien eine Weile dauern kann.

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 Datenrepositorys.

> **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**
>
> Der automatische Export ist FSx für Lustre 2.10-Dateisysteme oder Dateisysteme nicht verfügbar. `Scratch 1`

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 Einstellungen für den automatischen Export jederzeit mithilfe der FSx Managementkonsole AWS CLI, der und der AWS API aktualisieren.

> **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, dass widersprüchliche Schreibvorgänge an mehreren Speicherorten auftreten.

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

- Neu — FSx für Lustre wird das S3-Daten-Repository nur dann automatisch aktualisiert, wenn eine neue Datei, ein neues Verzeichnis oder ein neuer Symlink im Dateisystem erstellt wird.
- Geändert — FSx bei Lustre wird das S3-Daten-Repository nur dann automatisch aktualisiert, 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 bei Lustre wird das S3-Daten-Repository nur dann automatisch aktualisiert, wenn eine Datei, ein Verzeichnis oder ein Symlink im Dateisystem gelöscht wird.
- Beliebige Kombination aus „Neu“, „Geändert“ und „Gelöscht“ — FSx bei Lustre wird das S3-Daten-Repository automatisch aktualisiert, wenn eine der angegebenen Aktionen im Dateisystem stattfindet. 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 denn Lustre aktualisiert das S3-Daten-Repository nicht automatisch, wenn Dateien zum Dateisystem hinzugefügt, geändert oder aus dem Dateisystem gelöscht werden. Wenn Sie keine Exportrichtlinie konfigurieren, ist der automatische Export deaktiviert. Sie können Änderungen immer noch manuell exportieren, indem Sie eine Aufgabe zum Exportieren eines Datenrepositorys verwenden, wie unter 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.

> **Note**
>
> Während der Exportvorgänge die Zugriffszeit (`atime`) und die Änderungszeit (`mtime`) mit S3 synchronisiert werden, lösen Änderungen an diesen Zeitstempeln allein noch keinen automatischen Export aus. Nur Änderungen am Dateiinhalt oder an anderen Metadaten (wie Eigentum oder Berechtigungen) lösen einen automatischen Export nach S3 aus.

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 FSx für Lustre S3-Repository-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.

Gehen Sie wie folgt vor, um Daten und Metadatenänderungen im Dateisystem mithilfe der FSx Amazon-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 FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Navigationsbereich Dateisysteme und anschließend Ihr Lustre Dateisystem aus.
3. Wählen Sie die Registerkarte Daten-Repository.

4. Wählen Sie im Bereich Datenrepository-Verknüpfungen die Datenrepository-Zuordnung aus, für die Sie die Exportaufgabe erstellen möchten.
5. Wählen Sie für Aktionen die Option Aufgabe exportieren aus. Diese Option ist nicht verfügbar, wenn das Dateisystem nicht mit einem Daten-Repository auf S3 verknüpft ist. Das Aufgabendialogfeld Exportdaten-Repository erstellen wird angezeigt.
6. (Optional) Geben Sie bis zu 32 Verzeichnisse oder Dateien an, die aus Ihrem FSx Amazon-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 den Bericht liefern FSx soll, geben Sie einen relativen Pfad im verknüpften S3-Datenrepository des Dateisystems als Berichtspfad ein.
8. Wählen Sie 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.

Um Änderungen zu exportieren (CLI)

- Verwenden Sie den `create-data-repository-task`CLI-Befehl, um Daten und Metadatenänderungen in 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 FSx gibt Amazon 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 Datenrepository erstellt haben, können Sie den Status der Aufgabe zum Exportieren des Datenrepositorys überprüfen. Weitere Informationen zum Anzeigen von Datenrepository-Aufgaben finden Sie unterZugreifen auf Datenrepository-Aufgaben.

Exportieren von Dateien mithilfe von HSM-Befehlen

> **Note**
>
> Um Änderungen an den Daten und Metadaten Ihres FSx for Lustre-Dateisystems in ein dauerhaftes Daten-Repository auf Amazon S3 zu exportieren, verwenden Sie die unter beschriebene automatische Exportfunktion. Exportieren Sie Updates automatisch in Ihren S3-Bucket Sie können auch Aufgaben zum Exportieren von Datenrepositorys verwenden, die unter beschrieben sind. Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen

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

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

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

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

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

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

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

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

Datenrepository-Aufgaben

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

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

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

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

Arten von Datenrepository-Aufgaben

Es gibt drei Arten von Datenrepository-Aufgaben:

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

Weitere Informationen finden Sie unter Eine Datenrepository-Aufgabe erstellen.

Themen

Den Status und die Details einer Aufgabe verstehen

Eine Datenrepository-Aufgabe enthält beschreibende Informationen und einen Lebenszyklusstatus.

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

- Der Aufgabentyp:
  - `EXPORT_TO_REPOSITORY`weist auf eine Exportaufgabe hin.
  - `IMPORT_METADATA_FROM_REPOSITORY`weist auf eine Importaufgabe hin.
  - `RELEASE_DATA_FROM_FILESYSTEM`weist auf eine Release-Aufgabe hin.
- Das Dateisystem, auf dem die Aufgabe ausgeführt wurde.
- Die Zeit der Erstellung der Aufgabe.
- Der Status der Aufgabe.
- Die Gesamtzahl der Dateien, die von der Aufgabe verarbeitet wurden.
- 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 ist. Detaillierte Informationen zu Dateien, bei denen Fehler aufgetreten sind, sind in einem Bericht zum Abschluss der Aufgabe verfügbar. Weitere Informationen finden Sie unter Mit Berichten über den Abschluss von Aufgaben arbeiten.
- Die Uhrzeit, zu der die Aufgabe gestartet wurde.
- Die Uhrzeit, zu der der Aufgabenstatus zuletzt aktualisiert wurde. Der Aufgabenstatus wird alle 30 Sekunden aktualisiert.

Eine Datenrepository-Aufgabe kann einen der folgenden Status haben:

- PENDING bedeutet, dass Amazon die Aufgabe nicht gestartet FSx hat.

- EXECUTING gibt an, dass Amazon FSx die Aufgabe bearbeitet.
- FAILED bedeutet, dass Amazon die Aufgabe FSx 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 unterBehebung von Fehlern bei Datenrepository-Aufgaben.
- SUCCEED bedeutet, dass Amazon die Aufgabe erfolgreich FSx abgeschlossen hat.
- CANCELED gibt an, dass die Aufgabe storniert und nicht abgeschlossen wurde.
- CANCELING bedeutet, dass Amazon FSx gerade dabei ist, die Aufgabe abzubrechen.

Weitere Informationen zum Zugriff auf bestehende Datenrepository-Aufgaben finden Sie unter. Zugreifen auf Datenrepository-Aufgaben

Verwenden von Datenrepository-Aufgaben

In den folgenden Abschnitten finden Sie detaillierte Informationen zur Verwaltung von Datenrepository-Aufgaben. Sie können Datenrepository-Aufgaben mithilfe der FSx Amazon-Konsole, CLI oder API erstellen, duplizieren, Details anzeigen und stornieren.

Themen

- Eine Datenrepository-Aufgabe erstellen
- Eine Aufgabe duplizieren
- Zugreifen auf Datenrepository-Aufgaben
- Abbrechen einer Datenrepository-Aufgabe

Eine Datenrepository-Aufgabe erstellen

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

Sie können drei Arten von Datenrepository-Aufgaben erstellen:

- Die Aufgabe Datenrepository exportieren exportiert Daten aus Ihrem Lustre Dateisystem in einen verknüpften S3-Bucket. Weitere Informationen finden Sie unter Verwenden von Datenrepository-Aufgaben zum Exportieren von Änderungen.

- Die Aufgabe Datenrepository importieren importiert aus einem verknüpften S3-Bucket in Ihr Lustre Dateisystem. Weitere Informationen finden Sie unter Verwenden von Datenrepository-Aufgaben zum Importieren von Änderungen.
- Die Aufgabe Datenrepository 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.

Eine Aufgabe duplizieren

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

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

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

Um eine bestehende Aufgabe zu duplizieren

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

4. Wählen Sie Erstellen aus.

Zugreifen auf Datenrepository-Aufgaben

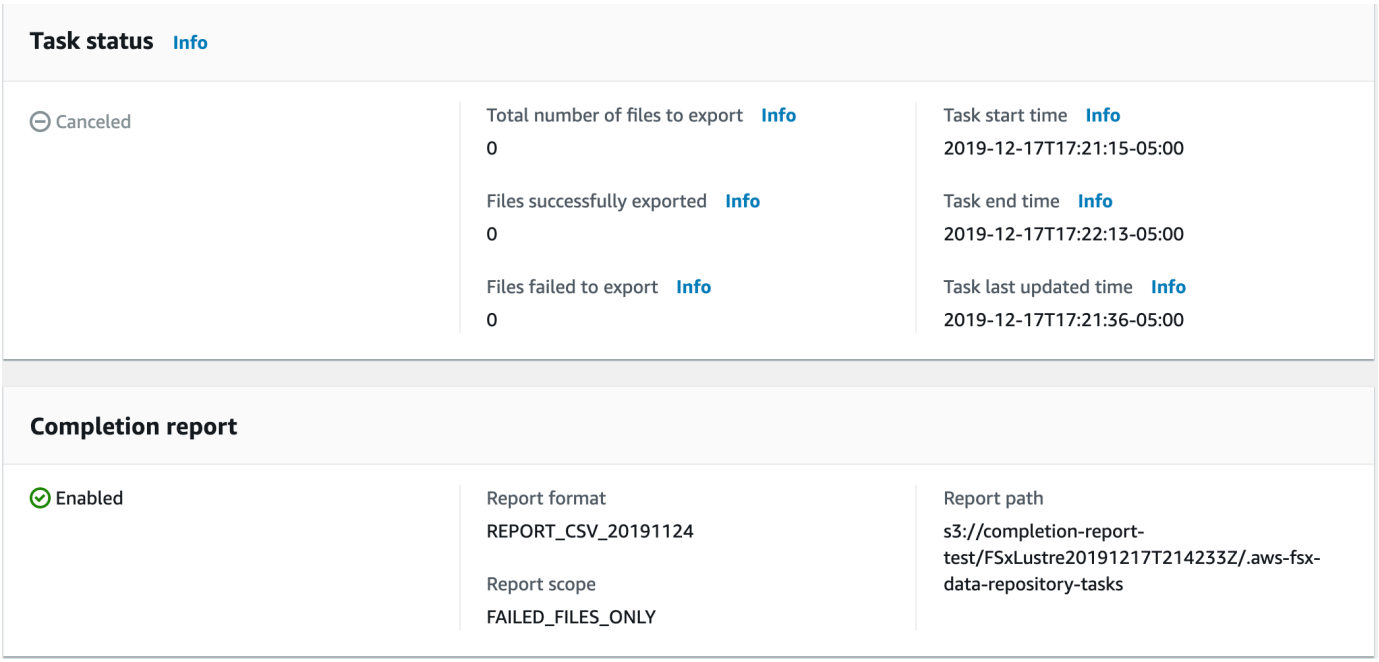
Nachdem Sie eine Datenrepository-Aufgabe erstellt haben, können Sie über die FSx Amazon-Konsole, CLI und API auf die Aufgabe und alle vorhandenen Aufgaben in Ihrem Konto zugreifen. Amazon FSx stellt die folgenden detaillierten Aufgabeninformationen bereit:

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

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

Um Datenrepository-Aufgaben und Aufgabendetails anzuzeigen (Konsole)

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Navigationsbereich das Dateisystem aus, für das Sie Datenrepository-Aufgaben anzeigen möchten. Die Seite mit den Dateisystemdetails wird angezeigt.
3. Wählen Sie auf der Seite mit den Dateisystemdetails die Registerkarte Datenrepository aus. Alle Aufgaben für dieses Dateisystem werden im Bereich Datenrepository-Aufgaben angezeigt.
4. Um die Details einer Aufgabe zu sehen, wählen Sie im Aufgabenbereich „Datenrepository“ die Option „Aufgaben-ID “ oder „Aufgabenname“. Die Seite mit den Aufgabendetails wird angezeigt.



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

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

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

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

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

  ```
  {
      "DataRepositoryTasks": [
          {
              "Lifecycle": "EXECUTING",
              "Paths": [],
              "Report": {
                  "Path":"s3://dataset-01/reports",
                  "Format":"REPORT_CSV_20191124",
                  "Enabled":true,
                  "Scope":"FAILED_FILES_ONLY"
              },
  ```

```
            "StartTime": 1591863862.288,
            "EndTime": ,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef3",
            "Status": {
                "SucceededCount": 4255,
                "TotalCount": 4200,
                "FailedCount": 55,
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789a7",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef3"
        },
        {
            "Lifecycle": "FAILED",
            "Paths": [],
            "Report": {
                "Enabled": false,
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef1",
            "Status": {
                "SucceededCount": 1153,
                "TotalCount": 1156,
                "FailedCount": 3,
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef1"
        },
        {
            "Lifecycle": "SUCCEEDED",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-04/reports",
                "Format":"REPORT_CSV_20191124",
```

```
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-04299453935122318",
            "Status": {
                "SucceededCount": 258,
                "TotalCount": 258,
                "FailedCount": 0,
                "LastUpdatedTime": 1771848950.012,
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1771848950.012,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef0"
        }
    ]
}
```

Aufgaben nach Dateisystem anzeigen

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

Um Aufgaben nach Dateisystem (Konsole) aufgeschlüsselt anzuzeigen

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

Um Aufgaben per Dateisystem (CLI) abzurufen

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

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

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

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

```
            "TaskId": "task-0123456789abcdef0",
            "Status": {
                "SucceededCount": 258,
                "TotalCount": 258,
                "FailedCount": 0,
                "LastUpdatedTime": 1771848950.012,
            },
            "FileSystemId": "fs-0123456789abcdef0",
            "CreationTime": 1771848950.012,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef0"
        }
    ]
}
```

Abbrechen einer Datenrepository-Aufgabe

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

- Amazon verarbeitet FSx keine Dateien, die sich in der Warteschlange zur Verarbeitung befinden.
- Amazon verarbeitet FSx weiterhin alle Dateien, die sich derzeit in Bearbeitung befinden.
- Amazon FSx setzt keine Dateien zurück, die die Aufgabe bereits verarbeitet hat.

Um eine Datenrepository-Aufgabe abzubrechen (Konsole)

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

Um eine Datenrepository-Aufgabe abzubrechen (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 Datenrepository-Aufgabe abzubrechen.

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

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

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

Mit Berichten über den Abschluss von Aufgaben arbeiten

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

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

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

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

- Pfade, die mit einem der folgenden Zeichen beginnen, sind in einfachen Anführungszeichen enthalten: `@ + - =`
- Zeichenfolgen, die mindestens eines der folgenden Zeichen enthalten, sind in doppelten Anführungszeichen enthalten: `" ,`

- Alle doppelten Anführungszeichen werden durch ein zusätzliches doppeltes Anführungszeichen maskiert.

Im Folgenden finden Sie einige Beispiele für die Berichtskodierung:

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

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

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

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

Weitere Informationen zu Aufgabenfehlern und deren Behebung finden Sie unterBehebung von Fehlern bei Datenrepository-Aufgaben.

Behebung von Fehlern bei Datenrepository-Aufgaben

Sie können die Protokollierung in Logs aktivieren, um Informationen über Fehler zu CloudWatch protokollieren, die beim Import oder Export von Dateien mithilfe von Datenrepository-Aufgaben aufgetreten sind. Informationen zu CloudWatch Protokoll-Ereignisprotokollen finden Sie unterDatenrepository-Ereignisprotokolle.

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

Für Datenrepository-Aufgaben stellt Amazon optional FSx auch Informationen zu den spezifischen Dateien und Verzeichnissen, bei denen Fehler aufgetreten sind, in einem Abschlussbericht zur

Verfügung. Der Bericht über den Abschluss der Aufgabe enthält den Datei- oder Verzeichnispfad auf dem Lustre Dateisystem, bei dem der Fehler aufgetreten ist, seinen Status und die Fehlerursache. Weitere Informationen finden Sie unter Mit Berichten über den Abschluss von Aufgaben arbeiten.

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

Fehlercode	Erklärung
`FileSizeTooLarge`	Die von Amazon S3 unterstützte maximale Objektgröße beträgt 5 TiB.
`InternalError`	Im FSx Amazon-Dateisystem ist bei einer Import-, Export- oder Release-Aufgabe ein Fehler aufgetreten. Im Allgemeinen bedeutet dieser Fehlercode, dass sich das FSx Amazon-Dateisystem, auf dem die fehlgeschlagene Aufgabe ausgeführt wurde, im Lebenszyklusstatus FAILED befindet. In diesem Fall können die betroffenen Dateien aufgrund von Datenverlust möglicherweise nicht wiederhergestellt werden. Andernfalls können Sie HSM-Befehle (Hierarchical Storage Management) verwenden, um die Dateien und Verzeichnisse in das Datenrepository auf S3 zu exportieren. Weitere Informationen finden Sie unter Exportieren von Dateien mithilfe von HSM-Befehlen.
`OperationNotPermitted`	Amazon FSxkonnte die Datei nicht veröffentlichen, da sie nicht in einen verknüpften S3-Bucket exportiert wurde. Sie müssen automatische Export- oder Export-Datenrepository-Aufgaben verwenden, um sicherzustellen, dass Ihre Dateien zuerst in Ihren verknüpften Amazon S3 S3-Bucket exportiert werden.

Fehlercode	Erklärung
`PathSizeTooLong`	Der Exportpfad ist zu lang. Die von S3 unterstützte maximale Länge des Objektschlüssels beträgt 1.024 Zeichen.
`ResourceBusy`	Amazon FSxkonnte die Datei nicht exportieren oder veröffentlichen, da ein anderer Client im Dateisystem auf sie zugegriffen hat. Sie können es erneut versuchen, DataRepositoryTask nachdem Ihr Workflow das Schreiben in die Datei abgeschlossen hat.

Fehlercode	Erklärung
`S3AccessDenied`	Der Zugriff auf Amazon S3 wurde für eine Export- oder Importaufgabe des Datenrepositorys verweigert. Für Exportaufgaben muss das FSx Amazon-Dateisystem über die Berechtigung verfügen, den `S3:PutObject` Vorgang zum Exportieren in ein verknüpftes Datenrepository auf S3 auszuführen. Diese Berechtigung wird in der `AWSServiceRoleForFSxS3Access_` *`fs-0123456789abcdef0`* serviceverknüpften Rolle erteilt. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon FSx. Da bei Exportaufgaben Daten außerhalb der VPC eines Dateisystems fließen müssen, kann dieser Fehler auftreten, wenn das Ziel-Repository über eine Bucket-Richtlinie verfügt, die einen der globalen Bedingungsschlüssel `aws:SourceVpc` oder `aws:SourceVpce` IAM-Bedingungsschlüssel enthält. Für Importaufgaben muss das FSx Amazon-Dateisystem über die Berechtigung verfügen, die `S3:GetObject` AND-Operationen für den `S3:HeadObject` Import aus einem verknüpften Daten-Repository auf S3 auszuführen. Wenn Ihr S3-Bucket für Importaufgaben serverseitige Verschlüsselung mit in AWS Key Management Service (SSE-KMS) gespeicherten kundenverwalteten Schlüsseln verwendet, müssen Sie die Richtlinienkonfigurationen unter befolgen. Arbeiten mit serverseitig verschlüsselten Amazon S3 S3-Buckets

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

Fehlercode	Erklärung
`S3ObjectInUnsupportedTier`	Amazon FSx hat erfolgreich ein Objekt ohne Symlink aus einer Speicherklasse S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive importiert. Das `FileStatus` wird im Bericht über den `succeeded with warning` Abschluss der Aufgabe enthalten sein. Die Warnung weist darauf hin, dass Sie zum Abrufen der Daten zuerst das Objekt S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive wiederherstellen und dann einen `hsm_restore` Befehl verwenden müssen, um das Objekt zu importieren.
`S3ObjectNotFound`	Amazon FSx konnte die Datei nicht importieren oder exportieren, da sie nicht im Datenspeicher vorhanden ist.
`S3ObjectPathNotPosixCompliant`	Das Amazon S3 S3-Objekt ist vorhanden, kann aber nicht importiert werden, da es kein POSIX-kompatibles Objekt ist. Informationen zu unterstützten POSIX-Metadaten finden Sie unter. Unterstützung von POSIX-Metadaten für Datenrepositorys
`S3ObjectUpdateInProgressFromFileRename`	Amazon FSxkonnte die Datei nicht veröffentlichen, da der automatische Export eine Umbenennung der Datei verarbeitet. Der automatische Umbenennungsprozess für den Export muss abgeschlossen sein, bevor die Datei veröffentlicht werden kann.

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

Dateien werden freigegeben

Aufgaben im Release-Daten-Repository geben Dateidaten aus Ihrem FSx for Lustre-Dateisystem frei, um Speicherplatz für neue Dateien freizugeben. Beim Freigeben einer Datei bleiben die Dateiliste und die Metadaten erhalten, die lokale Kopie des Dateiinhalts wird jedoch 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**
>
> Repository-Aufgaben FSx für Release-Daten sind auf Lustre 2.10-Dateisystemen nicht verfügbar.

Die Parameter Dateisystempfade bis zur Veröffentlichung und Mindestdauer seit dem letzten Zugriff bestimmen, 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` `mtime`, 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 mithilfe 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 FSx Amazon-Konsole und CLI aus dem Dateisystem freigeben. Beim Freigeben einer Datei werden die Dateiliste und die Metadaten beibehalten, die lokale Kopie des Dateiinhalts wird jedoch entfernt.

Um Dateien freizugeben (Konsole)

1. Öffnen Sie die FSx Amazon-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.
6. Geben Sie unter Zu veröffentlichende Dateisystempfade bis zu 32 Verzeichnisse oder Dateien an, die aus Ihrem FSx Amazon-Dateisystem freigegeben werden sollen, indem Sie die Pfade zu diesen Verzeichnissen oder Dateien angeben. Die Pfade, die Sie angeben, müssen sich auf den Bereitstellungspunkt 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`m`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 Ort anzugeben, an dem Amazon den Bericht liefern FSx soll, geben Sie als Berichtspfad einen relativen Pfad im verknüpften S3-Datenrepository des Dateisystems 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 FSx gibt Amazon 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 Datenrepository-Aufgaben.

Amazon FSx mit Ihren lokalen Daten verwenden

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

Zur Verwendung FSx für Lustre mit Ihren lokalen Daten

1. Erstellen eines Dateisystems. Weitere Informationen finden Sie Schritt 1: 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 FSx Amazon-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 EC2 In-Cloud-Amazon-Instances aus, die Ihr Dateisystem mounten.
5. Wenn Sie fertig sind, kopieren Sie die Endergebnisse aus Ihrem Dateisystem zurück an Ihren lokalen Datenspeicherort und löschen Sie Ihr FSx for Lustre-Dateisystem.

Datenrepository-Ereignisprotokolle

Sie können die Protokollierung in CloudWatch Logs aktivieren, um Informationen über Fehler beim Import oder Export von Dateien mithilfe von Import-, Export-, Datenrepository-Aufgaben und Wiederherstellungsereignissen zu protokollieren. Weitere Informationen finden Sie unter Protokollierung mit Amazon CloudWatch Logs.

> **Note**
>
> Wenn eine Datenrepository-Aufgabe fehlschlägt, schreibt Amazon FSx auch Fehlerinformationen in den Bericht zum Abschluss der Aufgabe. Weitere Informationen zu Fehlerinformationen in Abschlussberichten finden Sie unterBehebung von Fehlern bei Datenrepository-Aufgaben.

Themen

Ereignisse importieren

Fehlertyp	Protokoebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
Fehler beim Auflisten von Objekten	ERROR	Fehler beim Auflisten von S3-Objekten im S3-Bucket	Amazon FSx konnte S3-Objekte nicht im S3-Bucket	N/A

Fehlertyp	Protokoebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
		bucket_name mit Präfix*prefix*.	auflisten. Dies kann passieren, wenn die S3-Bucket-Richtlinie Amazon keine ausreichenden Berechtigungen gewährt FSx.	
Die S3-Speicherklasse wird nicht unterstützt	WARN	Das S3-Objekt mit dem Schlüssel konnte nicht *key_value* in den S3-Bucket importiert werden, *bucket_name* da sich ein S3-Objekt in einer nicht unterstützten Stufe befindet. *S3_tier_name*	Amazon FSx konnte ein S3-Objekt nicht importieren, da es sich in einer Amazon S3 S3-Speicherklasse befindet, die nicht unterstützt wird, wie z. B. S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive.	`S3ObjectInUnsupportedTier`

Fehlertyp	Protokoebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
Die Symlink-Speicherklasse wird nicht unterstützt	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht *key_value* in den S3-Bucket importiert werden, *bucket_name* da sich ein S3-Symlink-Objekt in einer nicht unterstützten Stufe befindet. *S3_tier_name*	Amazon FSx konnte ein Symlink-Objekt nicht importieren, da es sich in einer Amazon S3 S3-Speicherklasse befindet, die nicht unterstützt wird, wie z. B. S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive.	`S3SymlinkInUnsupportedTier`

Fehlertyp	Protokoebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3-Zugriff verweigert	ERROR	Das S3-Objekt mit dem Schlüssel *key_value* im S3-Bucket konnte nicht importiert werden*bucket_me* , da 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 FSx Amazon-Dateisystem über die Berechtigung verfügen, die `s3:GetObject` AND-Operationen für den `s3:HeadObject` Import aus einem verknüpften Daten-Repository auf S3 auszuführen. Wenn Ihr S3-Bucket für Importauf	`S3AccessDenied`

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

Fehlertyp	Protokoebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
Der Löschzugriff wurde verweigert	ERROR	Die lokale Datei für das S3-Objekt mit dem Schlüssel *key_value* im S3-Bucket konnte nicht gelöscht werden*bucket_me* , da der Zugriff auf das S3-Objekt verweigert wurde.	Dem automatischen Import wurde der Zugriff auf ein S3-Objekt verweigert.	N/A

Fehlertyp	Protokoebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
Nicht POSIX-konformes Objekt	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht *key_value* in den S3-Bucket importiert werden*bucket_me* , da das S3-Objekt nicht POSIX-konform ist.	Das Amazon S3 S3-Objekt ist vorhanden, kann aber nicht importiert werden, da es kein POSIX-kompatibles Objekt ist. Informationen zu unterstützten POSIX-Metadaten finden Sie unter. Unterstützung von POSIX-Metadaten für Datenrepositorys	`S3ObjectPathNotPosixCompliant`

Fehlertyp	Protokoebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
Der Objekttyp stimmt nicht überein	ERROR	Das S3-Objekt mit dem Schlüssel *key_value* im S3-Bucket konnte nicht importiert werden, *bucket_name* da bereits ein S3-Objekt mit demselben Namen in das Dateisystem importiert wurde.	Das importierte S3-Objekt ist von einem anderen Typ (Datei oder Verzeichnis) als ein vorhandenes Objekt mit demselben Namen im Dateisystem.	`S3ObjectTypeMismatch`
Aktualisierung der Verzeichnis-Metadaten fehlgeschlagen	ERROR	Die Metadaten des lokalen Verzeichnisses konnten aufgrund eines internen Fehlers nicht aktualisiert werden.	Verzeichnismetadaten konnten aufgrund eines internen Fehlers nicht importiert werden.	N/A

Fehlertyp	Protokoebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3-Objekt wurde nicht gefunden	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht importiert werden*key_val*, da 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`
S3-Bucket wurde nicht gefunden	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht *key_value* in den S3-Bucket importiert werden, *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.	N/A

Fehlertyp	Protokoebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
S3-Bucket wurde nicht gefunden	ERROR	Die lokale Datei für das S3-Objekt mit dem Schlüssel *key_value* im S3-Bucket konnte nicht gelöscht werden, *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.	N/A
Fehler beim Erstellen des Verzeichnisses	ERROR	Das lokale Verzeichnis konnte aufgrund eines internen Fehlers nicht erstellt werden.	Amazon FSx konnte eine Verzeichniserstellung aufgrund eines internen Fehlers nicht automatisch in das Dateisystem importieren.	N/A

Fehlertyp	Protokoll ebene	Nachricht protokollieren	Ursache	Fehlercode im Abschluss bericht
Der Festplattenspeicher ist voll	ERROR	Das S3-Objekt mit dem Schlüssel konnte nicht *key_value* in den S3-Bucket importiert werden*bucket_name* , da das Dateisystem voll ist.	Beim Erstellen der Datei oder des Verzeichnisses ist dem Dateisystem auf den Metadatenservern der Speicherplatz ausgegangen.	N/A

Ereignisse exportieren

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
Zugriff verweigert	ERROR	Die Datei konnte nicht exportiert werden, da der Zugriff auf das S3-Objekt mit dem Schlüssel *key_value* im S3-Bucket verweigert wurde*bucket_name* .	Der Zugriff auf Amazon S3 wurde für eine Datenrepository-Exportaufgabe verweigert. Für Exportaufgaben muss das FSx Amazon-Dateisystem über die Berechtigung verfügen, den `s3:PutObj`	`S3AccessDenied`

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
			`ect` Vorgang zum Exportieren in ein verknüpftes Datenrepository auf S3 auszuführen. Diese Berechtigung wird in der `AWSServiceRoleForFSxS3Access_` *`fs-0123456789abcdef0`* serviceverknüpften Rolle erteilt. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon FSx. Da die Exportaufgabe erfordert, dass Daten außerhalb der VPC eines Dateisystems fließen, kann dieser Fehler auftreten, wenn das Ziel-Repository über eine	

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
			Bucket-Richtlinie verfügt, die einen der globalen Bedingungsschlüssel `aws:SourceVpc` oder `aws:SourceVpce` IAM-Bedingungsschlüssel enthält. Wenn Ihr S3-Bucket Objekte enthält, die von einem anderen AWS-Konto als Ihrem mit dem Dateisystem verknüpften S3-Bucket-Konto hochgeladen wurden, können Sie sicherstellen, dass Ihre Datenrepository-Aufgaben unabhängig davon, welches Konto sie hochgeladen hat, S3-Metadaten ändern oder S3-Objekt	

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
			e überschre iben können. Wir empfehlen Ihnen, die Funktion S3-Objektbesitz für Ihren S3-Bucket zu aktivieren. Mit dieser Funktion können Sie die Verantwortung für neue Objekte übernehmen, die von anderen in Ihren Bucket AWS-Konten hochgeladen werden, indem Sie Uploads dazu zwingen, die gespeiche rte ACL `--acl bucket-ow ner-full-control` bereitzustellen. Sie aktiviere n S3 Object Ownership, indem Sie in Ihrem S3-Bucket die bevorzugt e Option des Bucket-Besitzers	

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
			auswählen. Weitere Informationen finden Sie unter Steuern des Eigentums an hochgeladenen Objekten mithilfe von S3 Object Ownership im Amazon S3 S3-Benutzerhandbuch.	
Der Exportpfad ist zu lang	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 maximale Länge des Objektschlüssels, die von S3 unterstützt wird, beträgt 1.024 Zeichen.	`PathSizeTooLong`

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
Die Datei ist zu groß	ERROR	Die Datei konnte nicht exportiert werden, da die Dateigröße die maximal unterstützte Größe von S3-Objekten überschreitet.	Die maximale Objektgröße, die von Amazon S3 unterstützt wird, beträgt 5 TiB.	`FileSizeTooLarge`

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

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
Ressource ausgelastet	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`
Datei veröffentlicht	WARN	Export übersprungen: Die lokale Datei befindet sich im Status „Freigegeben“ und ein verknüpftes S3-Objekt mit Schlüssel *`key_value`* wurde nicht im Bucket *`bucket_name`* gefunden.	Amazon FSx konnte die Datei nicht exportieren, da sie sich im Dateisystem in einem freigegebenen Zustand befand.	N/A

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
Der Pfad des Datenrepositorys stimmt nicht überein	WARN	Der Export wurde 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.	N/A
Internal failure (Interner Fehler)	ERROR	Beim automatischen Export ist beim Export eines Dateisystemobjekts ein interner Fehler aufgetreten	Der Export ist aufgrund eines internen Fehlers (Autoexport oder Lustrebene) fehlgeschlagen.	N/A
Fehler beim Hochladen des Abschlussberichts	ERROR	Der Abschlussbericht für die Aufgabe im Datenrepository konnte nicht hochgeladen werden *bucket_name*	Amazon FSx konnte den Abschlussbericht nicht hochladen.	N/A

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache	Fehlercode im Abschlussbericht
Fehler bei der Validierung des Abschluss berichts	ERROR	Der Abschluss bericht für die Datenrepo sitory-Aufgabe konnte nicht in den Bucket hochgelad en werden, *bucket_na me* da der Pfad des Abschluss berichts *report_pa th* nicht zu einem Datenrepo sitory gehört, das diesem Dateisyst em zugeordnet ist	Amazon FSx konnte den Abschluss bericht nicht hochladen, da der vom Kunden bereitgestellte S3-Pfad nicht zu einem verknüpft en Datenspei cher gehört.	N/A

HSM-Wiederherstellungsereignisse

Fehlertyp	Protokoll ebene	Nachricht protokoll ieren	Ursache
Zugriff verweigert	ERROR	Die Datei konnte nicht wiederher gestellt werden, da der Zugriff auf das S3-Objekt *object_na me* im S3-Bucket verweigert	Beim Versuch, eine Datei mithilfe von HSM-Befehlen wiederherzustellen , wurde der Zugriff auf Amazon S3 verweigert. Das Dateisystem muss

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache
		wurde*bucket_name* .	berechtigt sein, die `s3:GetObject` Operationen `s3:HeadObject` und zur Wiederherstellung aus dem verknüpften Daten-Repository auf S3 auszuführen.
Die S3-Speicherklasse wird nicht unterstützt	WARN	Die Datei konnte nicht wiederhergestellt werden, da sich das S3-Objekt *object_name* im Bucket in einem nicht unterstützten *S3_storage_class_name* Ordner *bucket_name* befand.	Amazon FSx konnte die Datei nicht wiederherstellen, da sich das entsprechende S3-Objekt in einer S3-Speicherklasse befindet, die nicht unterstützt wird, z. B. S3 Glacier Flexible Retrieval oder S3 Glacier Deep Archive. Sie müssen das Objekt zuerst aus der Glacier-Speicherklasse wiederherstellen, bevor Sie es verwenden können. `hsm_restore`

Fehlertyp	Protokollebene	Nachricht protokollieren	Ursache
S3-Objekt wurde nicht gefunden	ERROR	Die Datei konnte nicht wiederhergestellt werden, da das S3-Objekt mit dem Schlüssel nicht im S3-Bucket gefunden *key_value* wurde*bucket_name* .	Amazon FSx konnte die Datei nicht wiederherstellen, da das entsprechende S3-Objekt nicht im Daten-Repository existiert.
S3-Bucket wurde nicht gefunden	ERROR	Die Datei konnte nicht wiederhergestellt werden, da der S3-Bucket nicht *bucket_name* existiert.	Amazon FSx kann die Datei nicht wiederherstellen, da der verknüpfte S3-Bucket nicht mehr existiert.
Der Festplattenspeicher ist voll	ERROR	Die Datei konnte nicht wiederhergestellt werden, da im Dateisystem kein Speicherplatz verfügbar war.	Beim Versuch, die Dateidaten aus S3 wiederherzustellen, ging dem Dateisystem der verfügbare Speicherplatz aus. Erwägen Sie, die Speicherkapazität des Dateisystems zu erhöhen oder Dateien freizugeben, um Speicherplatz freizugeben.

Arbeiten mit älteren Bereitstellungstypen

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. Beachten Sie, dass der automatische Export und die Unterstützung mehrerer Datenrepositorys FSx für Lustre-Dateisysteme, die keine Datenrepository-Verknüpfungen verwenden, nicht verfügbar sind.

Themen

Verknüpfen Sie Ihr Dateisystem mit einem Amazon S3 S3-Bucket

Wenn Sie ein Amazon FSx for Lustre-Dateisystem erstellen, können Sie es mit einem dauerhaften Daten-Repository in Amazon S3 verknüpfen. Bevor Sie Ihr Dateisystem erstellen, stellen Sie sicher, dass Sie den Amazon S3 S3-Bucket, zu dem Sie verlinken, bereits erstellt haben. Im Assistenten zum Erstellen von Dateisystemen legen Sie im optionalen Bereich Datenrepository-Import/Export die folgenden Eigenschaften für die Datenrepository-Konfiguration fest.

- Wählen Sie aus, wie Amazon Ihre Datei- und Verzeichnisliste auf dem neuesten Stand FSx hält, wenn Sie Objekte in Ihrem S3-Bucket hinzufügen oder ändern, nachdem das Dateisystem erstellt wurde. 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.
- Importpräfix: Geben Sie ein optionales Importpräfix ein, wenn Sie nur einige Datei- und Verzeichnislisten von Daten in Ihrem S3-Bucket in Ihr Dateisystem importieren möchten. Das Importpräfix definiert, aus welcher Position in Ihrem S3-Bucket Daten importiert werden sollen.
- Exportpräfix: Definiert, wo Amazon den Inhalt Ihres Dateisystems in Ihren verknüpften S3-Bucket FSx exportiert.

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

- Wenn Sie ein Dateisystem mit der Konsole erstellen, wählen Sie die Option Präfix exportieren > Ein von Ihnen festgelegtes Präfix und lassen Sie das Präfixfeld leer.
- Wenn Sie ein Dateisystem mithilfe der AWS CLI oder API erstellen, geben Sie den Exportpfad als Namen des S3-Buckets ohne zusätzliche Präfixe an, z. B. `ExportPath=s3://amzn-s3-demo-bucket/`

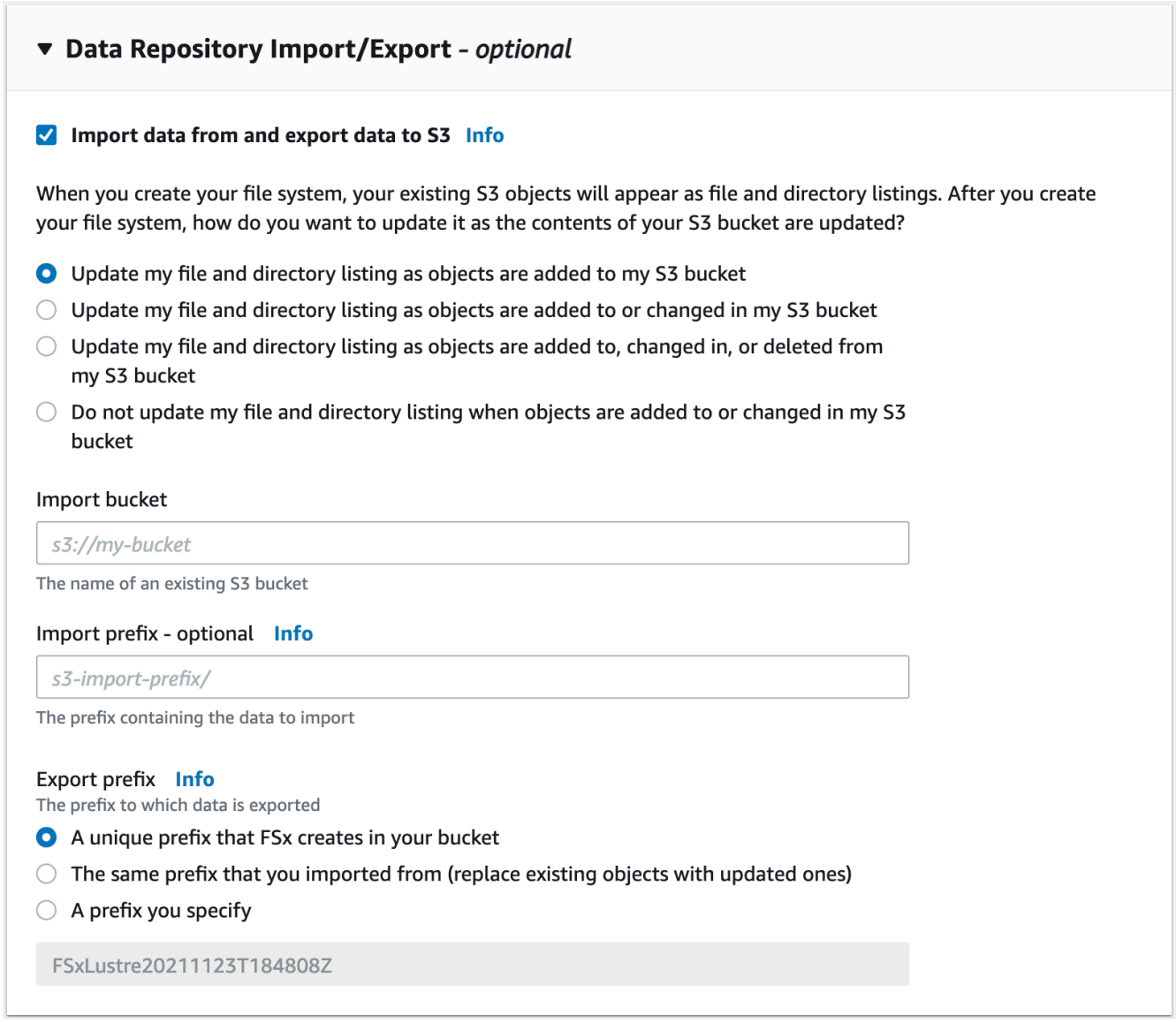
Mit dieser Methode können Sie bei der Angabe des Importpfads ein Importpräfix angeben, ohne dass sich dies auf eine 1:1 -Zuordnung für Exporte auswirkt.

Dateisysteme erstellen, die mit einem S3-Bucket verknüpft sind

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

Console

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Dashboard die Option Dateisystem erstellen aus.
3. Wählen Sie FSx als Dateisystemtyp Lustre und dann Weiter aus.
4. Geben Sie die Informationen ein, die für die Abschnitte Dateisystemdetails und Netzwerk und Sicherheit erforderlich sind. Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie Ihr FSx for Lustre-Dateisystem.
5. Sie verwenden den Bereich Daten-Repository-Import/Export, um ein verknüpftes Daten-Repository in Amazon S3 zu konfigurieren. Wählen Sie Daten aus S3 importieren und Daten nach S3 exportieren, um den Abschnitt Datenrepository-Import/Export zu erweitern und die Datenrepository-Einstellungen zu konfigurieren.



6. Wählen Sie aus, wie Amazon Ihre Datei- und Verzeichnisliste auf dem neuesten Stand FSx 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 aktualisiert FSx automatisch die Datei- und Verzeichnislisten aller neuen Objekte, die dem verknüpften S3-Bucket hinzugefügt wurden und derzeit nicht im FSx Dateisystem existieren. Amazon aktualisiert FSx keine Angebote für Objekte, die sich im S3-Bucket geändert haben. Amazon löscht FSx keine Angebote 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 API lautet`NONE`. Die Standardeinstellung für die Importeinstellungen bei Verwendung der Konsole lautet „Aktualisieren“ Lustre wenn dem S3-Bucket neue Objekte hinzugefügt werden.

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

7. Geben Sie ein optionales Importpräfix ein, wenn Sie nur einige der Datei- und Verzeichnislisten von Daten in Ihrem S3-Bucket in Ihr Dateisystem importieren möchten. Das Importpräfix definiert, aus welcher Position in Ihrem S3-Bucket Daten importiert werden sollen. Weitere Informationen finden Sie unter Automatischer Import von Updates aus Ihrem S3-Bucket.
8. Wählen Sie eine der verfügbaren Optionen für das Exportpräfix:

   - Ein eindeutiges Präfix, das Amazon in Ihrem Bucket FSx 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 (vorhandene Objekte durch aktualisierte ersetzen): Wählen Sie diese Option, um vorhandene Objekte durch aktualisierte zu ersetzen.
- Ein von Ihnen angegebenes Präfix: 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 eine 1:1 -Zuordnung zu erreichen, wählen Sie diese Option und lassen Sie das Präfixfeld leer. FSx exportiert Daten in dieselben Verzeichnisse, aus denen sie importiert wurden.

9. (Optional) Legen Sie die Wartungseinstellungen fest, oder verwenden Sie die Systemstandardwerte.
10. Wählen Sie Weiter und überprüfen Sie die Dateisystemeinstellungen. Nehmen Sie bei Bedarf Änderungen vor.
11. Wählen Sie Create file system (Dateisystem erstellen) aus.

AWS CLI

Das folgende Beispiel erstellt ein FSx Amazon-Dateisystem, das mit dem verknüpft istamzn-s3-demo-bucket, mit einer Importeinstellung, die alle neuen, geänderten und gelöschten Dateien in das verknüpfte Datenrepository importiert, nachdem das Dateisystem erstellt wurde.

> **Note**
>
> Die Standard-Importeinstellungen für den Import von Daten aus einem verknüpften S3-Bucket mithilfe der CLI und API sindNONE, was sich vom Standardverhalten bei Verwendung der Konsole unterscheidet.

Um ein FSx for Lustre-Dateisystem zu erstellen, verwenden Sie den Amazon FSx CLI-Befehl create-file-system, wie unten gezeigt. Die entsprechende API-Operation ist CreateFileSystem.

```
$ aws fsx create-file-system \
--client-request-token CRT1234 \
--file-system-type LUSTRE \
--file-system-type-version 2.10 \
```

```
--lustre-configuration
AutoImportPolicy=NEW_CHANGED_DELETED,DeploymentType=SCRATCH_1,ImportPath=s
3://amzn-s3-demo-bucket/,ExportPath=s3://amzn-s3-demo-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, FSx gibt Amazon 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://amzn-s3-demo-bucket/",
                    "ExportPath": "s3://amzn-s3-demo-bucket/export",
                    "ImportedFileChunkSize": 1024
                },
                "PerUnitStorageThroughput": 50
            }
        }
    ]
}
```

Den Exportpfad eines Dateisystems anzeigen

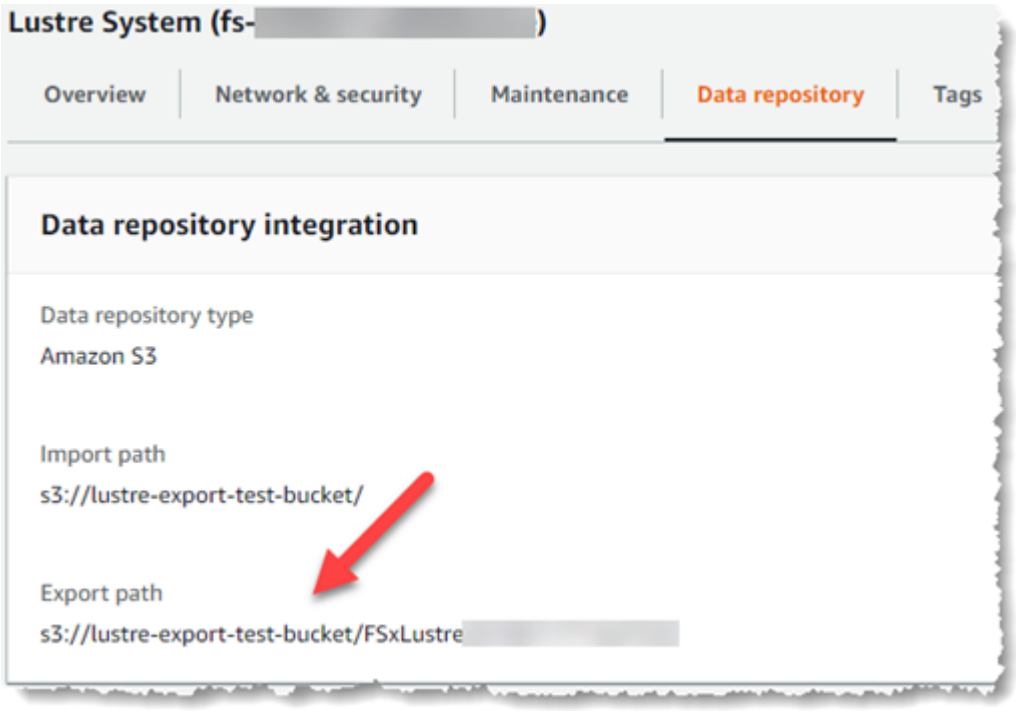
Sie können den Exportpfad eines Dateisystems mithilfe der FSx for Lustre-Konsole, der AWS CLI und der API anzeigen.

Console

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

   Die Seite mit den Dateisystemdetails für dieses Dateisystem wird angezeigt.
3. Wählen Sie die Registerkarte Daten-Repository.

   Das Datenrepository-Integrationsfenster mit den Import- und Exportpfaden wird angezeigt.



CLI

Verwenden Sie den `describe-file-systems` AWS CLI-Befehl, um den Exportpfad für Ihr Dateisystem zu ermitteln.

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

Suchen Sie `LustreConfiguration` in der Antwort nach der `ExportPath` Eigenschaft unter.

```
{
    "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://amzn-s3-demo-bucket/",
    "ExportPath": "s3://amzn-s3-demo-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 erstellt FSx die Datenrepository-Konfiguration zwischen dem Dateisystem und dem verknüpften Daten-Repository. Das Daten-Repository ist nicht verfügbar.
- Verfügbar: Das Datenrepository kann verwendet werden.
- Aktualisierung: Die Konfiguration des Datenrepositorys wird derzeit vom Kunden initiiert, was sich auf die Verfügbarkeit auswirken kann.
- 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 Daten-Repositorys mithilfe der FSx Amazon-Konsole, der AWS Befehlszeilenschnittstelle und der FSx Amazon-API anzeigen. In der FSx Amazon-

Konsole können Sie im Bereich Data Repository Integration der Registerkarte Data Repository für das Dateisystem auf den Lebenszyklusstatus des Daten-Repositorys zugreifen. Die `Lifecycle` Eigenschaft befindet sich im `DataRepositoryConfiguration` Objekt in der Antwort auf einen `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, FSx importiert Amazon standardmäßig die Dateimetadaten (Name, Besitz, Zeitstempel und Berechtigungen) von Objekten im verknüpften S3-Bucket bei der Erstellung des Dateisystems. Sie können Ihr FSx for Lustre-Dateisystem so konfigurieren, dass Metadaten von Objekten, die nach der Erstellung des Dateisystems zu Ihrem S3-Bucket hinzugefügt, dort geändert oder gelöscht wurden, automatisch importiert werden. 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 die Datei- und Verzeichnisliste eines geänderten Objekts FSx aktualisiert und das geänderte Objekt im S3-Bucket seine Metadaten nicht mehr enthält, FSx behält Amazon die aktuellen Metadatenwerte der Datei bei, anstatt Standardberechtigungen zu verwenden.

> **Note**
>
> Importeinstellungen sind FSx für Lustre-Dateisysteme 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 Einstellungen auf vorhandenen Dateisystemen mithilfe der FSx Managementkonsole, der AWS CLI und der AWS API aktualisieren. (Optional) Wenn Sie Ihr Dateisystem erstellen, werden Ihre vorhandenen S3-Objekte als Datei- und Verzeichnislisten angezeigt. Wie möchten Sie Ihr Dateisystem nach der Erstellung aktualisieren, wenn der Inhalt Ihres S3-Buckets aktualisiert wird? Ein Dateisystem kann eine der folgenden Importeinstellungen haben:

> **Note**
>
> Das FSx for Lustre-Dateisystem und der verknüpfte S3-Bucket müssen sich in derselben AWS Region befinden, damit Updates automatisch importiert werden können.

- Aktualisiere meine Datei- und Verzeichnisliste, wenn Objekte zu meinem S3-Bucket hinzugefügt werden: (Standard) Amazon aktualisiert FSx automatisch die Datei- und Verzeichnislisten aller neuen Objekte, die dem verknüpften S3-Bucket hinzugefügt wurden und derzeit nicht im FSx Dateisystem existieren. Amazon aktualisiert FSx keine Angebote für Objekte, die sich im S3-Bucket geändert haben. Amazon löscht FSx keine Angebote 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 API lautet`NONE`. Die Standardeinstellung für die Importeinstellungen bei Verwendung der Konsole lautet „Aktualisieren“ Lustre wenn dem S3-Bucket neue Objekte hinzugefügt werden.

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

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

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

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

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

Jede dieser Bedingungen führt dazu, dass der Lebenszyklusstatus des Daten-Repositorys falsch konfiguriert wird. Weitere Informationen finden Sie unter Status des Lebenszyklus des Datenrepositorys.

Voraussetzungen

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

- Das Dateisystem und der verknüpfte S3-Bucket müssen sich in derselben AWS Region befinden.
- 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 für den 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 Ordner-Metadaten
- Änderungen am Symlink-Ziel oder an den Metadaten

Importeinstellungen werden aktualisiert

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

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

Console

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Dashboard Dateisysteme aus.
3. Wählen Sie das Dateisystem aus, das Sie verwalten möchten, um die Dateisystemdetails anzuzeigen.
4. Wählen Sie Datenrepository, um die Datenrepository-Einstellungen anzuzeigen. Sie können die Importeinstellungen ändern, wenn der Lebenszyklusstatus VERFÜGBAR oder FALSCH KONFIGURIERT lautet. Weitere Informationen finden Sie unter Status des Lebenszyklus des Datenrepositorys.
5. Wählen Sie „Aktionen“ und anschließend „Importeinstellungen aktualisieren“, um das Dialogfeld „Importeinstellungen aktualisieren“ anzuzeigen.
6. Wählen Sie die neue Einstellung und anschließend „Aktualisieren“, um die Änderung vorzunehmen.

CLI

Verwenden Sie den `update-file-system`CLI-Befehl, um die Importeinstellungen zu aktualisieren. Die entsprechende API-Operation ist `UpdateFileSystem`.

Nachdem Sie das Dateisystem erfolgreich aktualisiert haben`AutoImportPolicy`, FSx gibt Amazon 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://amzn-s3-demo-bucket/",
                    "ExportPath": "s3://amzn-s3-demo-bucket/export",
                    "ImportedFileChunkSize": 1024
                }
                "PerUnitStorageThroughput": 50,
                "WeeklyMaintenanceStartTime": "2:04:30"
            }
        }
    ]
}
```

Leistung von Amazon FSx for Lustre

Dieses Kapitel enthält Leistungsthemen von Amazon FSx for Lustre, einschließlich einiger wichtiger Tipps und Empfehlungen zur Maximierung der Leistung Ihres Dateisystems.

Themen

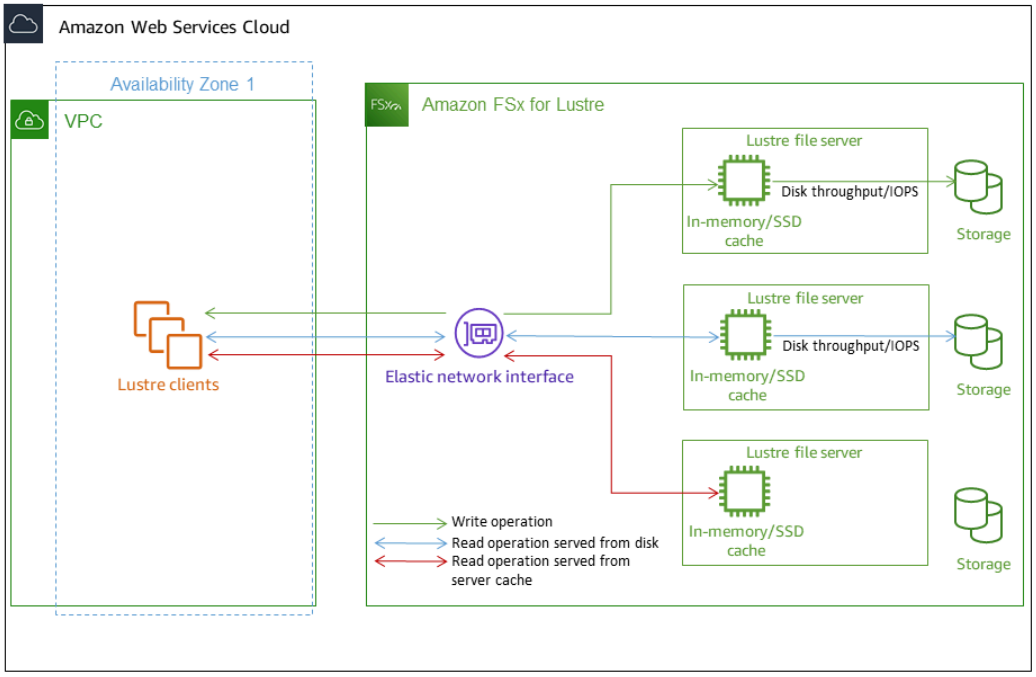
-Übersicht

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

Wie funktionieren FSx die Dateisysteme von For Lustre

Jedes Dateisystem FSx für Lustre besteht aus den Dateiservern, mit denen die Clients kommunizieren, und einem Satz von Festplatten, die an jeden Dateiserver angeschlossen sind und Ihre Daten speichern. Jeder Dateiserver verwendet einen schnellen In-Memory-Cache, um die Leistung der Daten zu verbessern, auf die am häufigsten zugegriffen wird. Je nach Speicherklasse kann Ihr Dateiserver mit einem optionalen SSD-Lesecache ausgestattet werden. Wenn ein Client auf

Daten zugreift, die im In-Memory- oder SSD-Cache gespeichert sind, muss der Dateiserver sie nicht von der Festplatte lesen, was die Latenz reduziert und den Gesamtdurchsatz erhöht, den Sie steuern können. Das folgende Diagramm zeigt die Pfade eines Schreibvorgangs, eines Lesevorgangs, der von der Festplatte aus ausgeführt wird, und eines Lesevorgangs, der über den Arbeitsspeicher oder den SSD-Cache ausgeführt wird.



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

Weitere Informationen über den Netzwerkdurchsatz, den Festplattendurchsatz und die IOPS-Eigenschaften von SSD- und HDD-Speicherklassen finden Sie unter Leistungsmerkmale der SSD- und HDD-Speicherklassen und. Leistungsmerkmale der Intelligent-Tiering-Speicherklasse

Leistung der Metadaten des Dateisystems

I/O-Operationen pro Sekunde (IOPS) für Dateisystem-Metadaten bestimmen die Anzahl der Dateien und Verzeichnisse, die Sie pro Sekunde erstellen, auflisten, lesen und löschen können.

Persistent 2-Dateisysteme ermöglichen es Ihnen, Metadaten-IOPS unabhängig von der Speicherkapazität bereitzustellen und bieten einen besseren Einblick in die Anzahl und Art der Metadaten-IOPS-Client-Instances, die in Ihrem Dateisystem ausgeführt werden. Bei SSD-Dateisystemen werden Metadaten-IOPS automatisch auf der Grundlage der von Ihnen bereitgestellten Speicherkapazität bereitgestellt. Der automatische Modus wird auf Intelligent-Tiering-Dateisystemen nicht unterstützt.

FSx Bei Lustre Persistent 2-Dateisystemen bestimmen die Anzahl der bereitgestellten Metadaten-IOPS und die Art des Metadatenvorgangs die Geschwindigkeit der Metadatenoperationen, die Ihr Dateisystem unterstützen kann. Die Ebene der von Ihnen bereitgestellten Metadaten-IOPS bestimmt die Anzahl der IOPS, die für die Metadaten-Festplatten Ihres Dateisystems bereitgestellt werden.

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

Für SSD-Dateisysteme können Sie festlegen, dass Metadaten-IOPS im automatischen Modus bereitgestellt werden soll. Im automatischen Modus stellt Amazon FSx automatisch Metadaten-IOPS basierend auf der Speicherkapazität Ihres Dateisystems gemäß der folgenden Tabelle bereit:

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

Speicherkapazität des Dateisystems	Inklusive Metadaten-IOPS im automatischen Modus
≥48000 GiB	12000 IOPS pro 24000 GiB

Im vom Benutzer bereitgestellten Modus können Sie optional die Anzahl der bereitzustellenden Metadaten-IOPS angeben. Gültige Werte sind:

- Für SSD-Dateisysteme sind die Werte`1500`,, `3000` `6000`–`12000`, und ein Vielfaches von `12000` bis zu einem Maximum von gültig. `192000`
- Für Intelligent-Tiering-Dateisysteme sind die gültigen Werte und. `6000` `12000`

Informationen zur Konfiguration von Metadaten-IOPS finden Sie unter. Verwaltung der Metadaten-Performance Beachten Sie, dass Sie für Metadaten-IOPS zahlen, die über der Standardanzahl an Metadaten-IOPS für Ihr Dateisystem bereitgestellt werden.

Durchsatz für einzelne Client-Instanzen

Wenn Sie ein Dateisystem mit einer Durchsatzkapazität GBps von über 10% erstellen, empfehlen wir, den Elastic Fabric Adapter (EFA) zu aktivieren, um den Durchsatz pro Client-Instance zu optimieren. Um den Durchsatz pro Client-Instance weiter zu optimieren, unterstützen EFA-fähige Dateisysteme auch GPUDirect Storage für EFA-fähige NVIDIA-GPU-basierte Client-Instances und ENA Express für ENA Express-fähige Client-Instances.

Der Durchsatz, den Sie einer einzelnen Client-Instance zuweisen können, hängt von der Wahl des Dateisystemtyps und der Netzwerkschnittstelle auf Ihrer Client-Instance ab.

Typ des Dateisystems	Netzwerkschnittstelle der Client-Instanz	Maximaler Durchsatz pro Client, Gbit/s
Nicht EFA-fähig	Beliebig	100 Gbit/s*
EFA-fähig	ENA	100 Gbit/s*
EFA-fähig	ENA Express	100 Gbit/s
EFA-fähig	EFA	700 Gbit/s

Typ des Dateisystems	Netzwerkschnittstelle der Client-Instanz	Maximaler Durchsatz pro Client, Gbit/s
EFA-fähig	EFA mit GDS	1200 Gbit/s

> **Note**
>
> * Der Datenverkehr zwischen einer einzelnen Client-Instance und einem individuellen Object Storage-Server FSx für Lustre ist auf 5 Gbit/s begrenzt. Die Anzahl der Objektspeicherserver, die Ihrem IP-Adressen für Dateisysteme for Lustre-Dateisystem zugrunde liegen, finden Sie FSx unter.

Speicherlayout des Dateisystems

Alle Lustre darin enthaltenen Dateidaten werden auf Speichervolumes gespeichert, die als Objektspeicherziele (OSTs) bezeichnet werden. Alle Dateimetadaten (einschließlich Dateinamen, Zeitstempel, Berechtigungen und mehr) werden auf Speichervolumes gespeichert, die als Metadatenziele (MDTs) bezeichnet werden. Amazon FSx for Lustre-Dateisysteme bestehen aus einem oder mehreren MDTs und mehreren OSTs. Amazon FSx for Lustre verteilt Ihre Dateidaten über das gesamte Dateisystem OSTs , um die Speicherkapazität mit dem Durchsatz und der IOPS-Auslastung in Einklang zu bringen.

Führen Sie den folgenden Befehl von einem Client aus, auf dem OSTs das Dateisystem installiert ist, um die Speichernutzung der MDTs und der Elemente Ihres Dateisystems zu überprüfen.

```
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
```

Striping von Daten in Ihrem Dateisystem

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

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

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

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

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

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

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

Ändern Sie Ihre Striping-Konfiguration

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

```
lfs setstripe filename --stripe-count number_of_OSTs
```

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

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

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

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

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

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

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

- Die Stripe-Größe beträgt standardmäßig 1 MiB. Das Einstellen eines Stripe-Offsets kann unter bestimmten Umständen nützlich sein, aber im Allgemeinen ist es am besten, ihn nicht anzugeben und die Standardeinstellung zu verwenden.

Progressive Datei-Layouts

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

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

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

Mit diesem Befehl werden vier Layoutkomponenten festgelegt:

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

> **Important**
>
> Durch das Anhängen von Daten an eine Datei, die mit einem PFL-Layout erstellt wurde, werden alle Layoutkomponenten aufgefüllt. Wenn Sie beispielsweise mit dem oben gezeigten 4-Komponenten-Befehl eine 1 MiB-Datei erstellen und dann Daten am Ende der Datei hinzufügen, wird das Layout der Datei auf eine Stripeanzahl von -1 erweitert, was bedeutet, dass alle Stripes im System vorhanden sind. OSTs Das bedeutet nicht, dass Daten in jedes

OST geschrieben werden, aber ein Vorgang wie das Lesen der Dateilänge sendet parallel zu jedem OST eine Anfrage, was das Dateisystem erheblich belastet.
Achten Sie daher darauf, die Anzahl der Stripes für Dateien mit kleiner oder mittlerer Länge zu begrenzen, an die anschließend Daten angehängt werden können. Da Protokolldateien normalerweise wachsen, wenn neue Datensätze angehängt werden, weist Amazon FSx for Lustre jeder im Anfügemodus erstellten Datei eine Standard-Stripe-Anzahl von 1 zu, unabhängig von der im übergeordneten Verzeichnis angegebenen Standard-Stripe-Konfiguration.

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

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

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

Überwachung von Leistung und Nutzung

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

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

Weitere Informationen zur Überwachung der Leistung Ihres Dateisystems finden Sie unterÜberwachung von Amazon FSx for Lustre-Dateisystemen.

Leistungsmerkmale der SSD- und HDD-Speicherklassen

Der Durchsatz, den ein FSx für Lustre mit SSD- oder HDD-Speicherklasse bereitgestelltes Dateisystem unterstützt, ist proportional zu seiner Speicherkapazität. Amazon FSx for Lustre-

Dateisysteme lassen sich auf ein Vielfaches TBps des Durchsatzes und Millionen von IOPS skalieren. Amazon FSx for Lustre unterstützt auch den gleichzeitigen Zugriff auf dieselbe Datei oder dasselbe Verzeichnis von Tausenden von Recheninstanzen aus. Dieser Zugriff ermöglicht ein schnelles Prüfen von Daten vom Anwendungsspeicher zum Speicher, was eine gängige Technik im Hochleistungsrechnen (HPC) ist. Sie können den Speicherplatz und die Durchsatzkapazität nach Bedarf jederzeit erhöhen, nachdem Sie das Dateisystem erstellt haben. Weitere Informationen finden Sie unter Verwaltung der Speicherkapazität.

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

Die folgenden Tabellen zeigen die Leistung, FSx für die die Bereitstellungsoptionen von Lustre mit SSD- und HDD-Speicherklassen konzipiert wurden.

Dateisystemleistung für SSD-Speicheroptionen

Art der Bereitstellung	Netzwerkdurchsatz (MBps/TiB des bereitgestellten Speichers)		Netzwerk-IOPS (IOPS/TiB des bereitgestellten Speichers)	Cache-Speicher (GiB RAM/TiB des bereitgestellten Speichers)	Festplattenlatenzen pro Dateivorgang (Millisekunden, P50)	Festplattendurchsatz (MBps/TiB bereitgestellter Speicher oder SSD-Cache)	
	Ausgangswert	Platzen				Grundlinie	Platzen
KRATZEN_2	200	1300	Zehntausende als Ausgangswert	6.7	Metadaten: Unter-MS Daten: Unter-Ms	200 (gelesen) 100 (schreiben)	-
HARTNÄCKIG-125	320	1300	Hunderttausende sind geplatzt	3.4		125	500
HARTNÄCKIG-250	640	1300		6.8		250	500
HARTNÄCKIG-500	1300	-		13,7		500	-
HARTNÄCKIG-1000	2600	-		27,3		1000	-

Dateisystemleistung für HDD-Speicheroptionen

Art der Bereitstellung	Netzwerkdurchsatz (MBps/TiB bereitgestellter Speicher oder SSD-Cache)		Netzwerk-IOPS (IOPS/TiB des bereitgestellten Speichers)	Cache-Speicher (GiB RAM/TiB des bereitgestellten Speichers)	Festplattenlatenzen pro Dateivorgang (Millisekunden, P50)	Festplattendurchsatz (MBps/TiB bereitgestellter Speicher oder SSD-Cache)	
	Ausgangswert	Platzen				Grundlinie	Platzen
HARTNÄCKIG-12							
HDD-Speicher	40	375*	Zehntausende als Ausgangswert Hunderttausende sind geplatzt	0.4 Speicher	Metadaten: Sub-MS Daten: einstellige ms	12	80 (gelesen) 50 (schreiben)
SSD-Lesecache	200	1.900		200 SSD-Cache	Daten: Sub-MS	200	-
PERSISTENT-40							
HDD-Speicher	150	1.300*	Zehntausende als Ausgangswert Hunderttausende sind geplatzt	1.5	Metadaten: Unter-MS Daten: einstellige ms	40	250 (gelesen) 150 (schreiben)
SSD-Lesecache	750	6500		200 SSD-Cache	Daten: Sub-MS	200	-

Leistung des Dateisystems für SSD-Speicheroptionen der vorherigen Generation

Art der Bereitstellung	Netzwerkdurchsatz (MBps pro TiB bereitgestellten Speichers)		Netzwerk-IOPS (IOPS pro TiB bereitgestellten Speichers)	Cache-Speicher (GiB pro TiB bereitgestellten Speichers)	Festplattenlatenzen pro Dateivorgang (Millisekunden, P50)	Festplattendurchsatz (MBps pro bereitgestelltem TiB Speicher oder SSD-Cache)	
	Ausgangswert	Platzen				Grundlinie	Platzen
HARTNÄCKIG-50	250	1.300*	Zehntausende als Ausgangswert	2,2 RAM	Metadaten: Unter-MS	50	240
PERSISTENT-100	500	1.300*		4,4 GRAMM	Daten: Unter-Ms	100	240
PERSISTENT-200	750	1.300*	Hunderttausende sind geplatzt	8,8 GRAMM		200	240

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

Beispiel: Aggregierter Baseline- und Burst-Durchsatz

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

Ein persistentes Dateisystem mit einer Speicherkapazität von 4,8 TiB und 50 MBps pro TiB Durchsatz pro Speichereinheit bietet einen aggregierten Basisdatenträgerdurchsatz von 240 MBps und einen Burst-Festplattendurchsatz von 1,152. GBps

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

Leistungsmerkmale der Intelligent-Tiering-Speicherklasse

Die Intelligent-Tiering-Speicherklasse von FSx for Lustre bietet elastischen, kostenoptimierten Speicher für Workloads, die traditionell auf HDD-basierten oder gemischten HDD-/SDD-basierten Hochleistungsdateisystemen ausgeführt werden. Dateisysteme, die die Intelligent-Tiering-Speicherklasse verwenden, verwenden vollständig elastischen, intelligent gestuften, regionalen Speicher, der automatisch wächst und schrumpft, um sich an Ihre Arbeitslast anzupassen, wenn sich diese ändert. Informationen zur Datenklassifizierung finden Sie unter. Wie die Intelligent-Tiering-Speicherklasse Daten einteilt

Der Durchsatz, den ein FSx for Lustre-Dateisystem mit Intelligent-Tiering-Speicherklasse unterstützt, ist unabhängig von seinem Speicher. Intelligent-Tiering-Dateisysteme lassen sich auf ein Vielfaches TBps des Durchsatzes und Millionen von IOPS skalieren. Dateisysteme, die die Intelligent-Tiering-Speicherklasse verwenden, bieten außerdem einen optionalen bereitgestellten SSD-Lesecache für den Zugriff auf häufig aufgerufene Daten mit geringer Latenz. Standardmäßig stellt Amazon FSx for Lustre einen SSD-Lese-Cache für häufig aufgerufene Metadaten bereit. Da die meisten Workloads in der Regel leseintensiv sind und zu einem bestimmten Zeitpunkt nur mit einem kleinen Teil des

Gesamtdatensatzes aktiv arbeiten, ermöglicht das Hybridmodell aus Intelligent-Tiering-Speicher und SSD-Lesecaches Dateisystemen, Speicher bereitzustellen, dessen Leistung mit SSD-Dateisystemen für die meisten Workloads vergleichbar ist, und gleichzeitig Speicherkosteneinsparungen im Vergleich zu den SSD- und HDD-Speicherklassen zu erzielen.

Beim Lesen und Schreiben von Daten in ein Intelligent-Tiering-Dateisystem, insbesondere bei Daten, auf die in letzter Zeit nicht oder nicht häufig genug zugegriffen wurde, um sich im In-Memory-Cache des Dateiservers zu befinden, hängt die Leistung von der Größe des SSD-Lesecaches ab. Der Datenzugriff über Intelligent-Tiering-Speicher hat time-to-first-byte Latenzen von etwa zehn Millisekunden sowie Kosten pro Anfrage, während Zugriffe aus dem SSD-Lesecache mit einer Latenz von unter einer Millisekunde und ohne Kosten pro Anfrage zurückgegeben werden.

Bei der Konfiguration der Größe des SSD-Lesecaches für Ihr Dateisystem sollten Sie sowohl die Größe Ihres häufig aufgerufenen Datensatzes innerhalb des Workloads als auch die Empfindlichkeit des Workloads gegenüber höheren Latenzen beim Lesen von Daten berücksichtigen, auf die seltener zugegriffen wird. Sie können nach der Erstellung Ihres Dateisystems zwischen den Modi für die Größe des SSD-Lesecaches wechseln und den Cache nach oben oder unten skalieren. Weitere Informationen zum Ändern Ihres SSD-Lesecaches finden Sie unterVerwaltung des bereitgestellten SSD-Lesecache.

Eine Schreibanforderung tritt auf, wenn FSx for Lustre einen Datenblock in den Intelligent-Tiering-Speicher schreibt. Wenn Sie Daten in das Dateisystem schreiben, werden Schreibanforderungen aggregiert und in den Intelligent-Tiering-Speicher geschrieben, wodurch der Durchsatz erhöht und die Anforderungskosten gesenkt werden. Lesevorgänge können aus dem In-Memory-Cache, dem SSD-Lesecache oder direkt aus dem Intelligent-Tiering-Speicher des Dateiservers bereitgestellt werden. Wenn ein Lesevorgang aus dem Intelligent-Tiering-Speicher bereitgestellt wird, erfolgt für jeden abgerufenen Datenblock eine Leseanforderung. Wenn Sie Daten sequentiell lesen, ruft FSx for Lustre Daten vorab ab, um die Leistung zu verbessern.

Daten aus dem In-Memory-Cache auf Dateisystemen, die die Intelligent-Tiering-Speicherklasse verwenden, werden dem anfragenden Client direkt als Netzwerk-I/O bereitgestellt. Wenn ein Client auf Daten zugreift, die sich nicht im In-Memory-Cache befinden, werden diese entweder aus dem SSD-Lesecache oder dem Intelligent-Tiering-Speicher als Festplatten-I/O gelesen und dem Client dann als Netzwerk-I/O bereitgestellt.

Dateisystemleistung für Intelligent-Tiering

Die folgende Tabelle zeigt die Leistung, FSx für die Intelligent-Tiering-Dateisysteme von Lustre konzipiert wurden.

Bereitgestellte Durchsatzkapazität () MBps	Netzwerkdurchsatz () MBps		Netzwerk-IOPS	In-Memory-Cache-Speicher (GB)	Maximaler SSD-Cache-Festplattendurchsatz () MBps	Maximaler SSD-Cache-Festplatten-IOPS	
	Basislinie	Platzen				Grundlinie	Platzen
Alle 4000	12500	-	Hunderttausende	76,8	4000	160000	-

Tipps zur Leistung

Beachten Sie bei der Verwendung von Amazon FSx for Lustre die folgenden Leistungstipps. Informationen zu Servicebeschränkungen finden Sie unterServicekontingente für Amazon FSx for Lustre.

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

  > **Note**
  >
  > Das von Ihnen gewählte Anforderungsmodell weist Kompromisse in Bezug auf Konsistenz (wenn Sie mehrere EC2 Amazon-Instances verwenden) und Geschwindigkeit auf.

- Verzeichnisgröße einschränken — Um eine optimale Metadaten-Performance auf den Dateisystemen Persistent 2 FSx for Lustre zu erreichen, beschränken Sie jedes Verzeichnis auf weniger als 100.000 Dateien. Durch die Begrenzung der Anzahl der Dateien in einem Verzeichnis wird die Zeit reduziert, die das Dateisystem benötigt, um das übergeordnete Verzeichnis zu sperren.
- EC2 Amazon-Instances — Anwendungen, die eine große Anzahl von Lese- und Schreibvorgängen ausführen, benötigen wahrscheinlich mehr Speicher oder Rechenkapazität als Anwendungen, die dies nicht tun. Wenn Sie Ihre EC2 Amazon-Instances für Ihre rechenintensive Arbeitslast starten, wählen Sie Instance-Typen aus, die über die Menge dieser Ressourcen verfügen, die Ihre Anwendung benötigt. Die Leistungsmerkmale von Amazon FSx for Lustre-Dateisystemen hängen nicht von der Verwendung von Amazon EBS-optimierten Instances ab.
- Empfohlenes Tuning von Client-Instances für optimale Leistung

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

```
sudo lctl set_param ldlm.namespaces.*.lru_max_age=600000
sudo lctl set_param ldlm.namespaces.*.lru_size=<100 * number_of_CPUs>
```

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

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

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

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

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

3. Um die Leistung für die Verzeichnisauflistung (ls) zu optimieren, muss die folgende Optimierung vorgenommen werden:

```
sudo lctl set_param llite.*.statahead_max=512
sudo lctl set_param llite.*.statahead_agl=1
if sudo lctl get_param llite.*.statahead_xattr > /dev/null 2>&1; then
    sudo lctl set_param llite.*.statahead_xattr=1
else
    echo "Warning: Xattr statahead is not supported on this Lustre client. Please
 upgrade to the latest Lustre 2.15 client to apply this tuning"
fi
```

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

- Workload-Balance OSTs — In einigen Fällen bestimmt Ihre Arbeitslast nicht den Gesamtdurchsatz, den Ihr Dateisystem bereitstellen kann (200 MBps pro TiB Speicher). Falls ja, können

Sie CloudWatch Metriken verwenden, um Fehler zu beheben, falls die Leistung durch ein Ungleichgewicht in den I/O Mustern Ihrer Workloads beeinträchtigt wird. Um herauszufinden, ob dies die Ursache ist, schauen Sie sich die CloudWatch Maximum-Metrik für Amazon FSx for Lustre an.

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

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

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

- LustreClient für Metadaten-IOPS — Wenn für Ihr Dateisystem eine Metadatenkonfiguration angegeben ist, empfehlen wir Ihnen, einen Lustre 2.15-Client oder einen Lustre 2.12-Client mit einer der folgenden Betriebssystemversionen zu installieren: Amazon Linux 2023; Amazon Linux 2; Red Hat/Rocky Linux 8.9, 8.10 oder 9.x; CentOS 8.9 oder 8.10; Ubuntu 22+ mit 6.2, 6.5 oder 6.8 Kernel; oder Ubuntu 20.

Überlegungen zur Leistung von Intelligent-Tiering

Im Folgenden finden Sie einige wichtige Überlegungen zur Leistung bei der Arbeit mit Dateisystemen, die die Intelligent-Tiering-Speicherklasse verwenden:

- Workloads, die Daten mit kleineren I/O Größen lesen, erfordern aufgrund der höheren Latenz der Intelligent-Tiering-Speicherstufen eine höhere Parallelität und verursachen höhere Anforderungskosten, um den gleichen Durchsatz zu erzielen wie Workloads, die große I/O Datenmengen verwenden. Wir empfehlen, Ihren SSD-Lesecache groß genug zu konfigurieren,

um die höhere Parallelität und den höheren Durchsatz bei der Arbeit mit kleineren I/O-Größen zu unterstützen.

- Die maximale Festplatten-IOPS, die Ihre Clients mit einem Intelligent-Tiering-Dateisystem erreichen können, hängt von den spezifischen Zugriffsmustern Ihres Workloads ab und davon, ob Sie einen SSD-Lesecache bereitgestellt haben. Bei Workloads mit wahlfreiem Zugriff können Clients in der Regel viel höhere IOPS erzielen, wenn die Daten im SSD-Lesecache zwischengespeichert werden, als wenn sich die Daten nicht im Cache befinden.
- Die Intelligent-Tiering-Speicherklasse unterstützt Read-Ahead, um die Leistung bei sequentiellen Leseanforderungen zu optimieren. Wir empfehlen, Ihr Datenzugriffsmuster nach Möglichkeit sequentiell zu konfigurieren, um Daten vorab abzurufen und eine höhere Leistung zu erzielen.

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. Direct Connect Sie können lokal auf Ihr FSx Amazon-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

LustreDateisystem- und Client-Kernel-Kompatibilität

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	Lustre-Clientversion	Lustre-Dateisystemversion		
					2.10	2,12	2,15
Amazon Linux 2023	6,12	*	*	2.15	Nein	Ja	Ja
	6.1	6.1.79-99,167	6,179-99,167+	2.15	Nein	Ja	Ja
Amazon Linux 2	5,10	5.10.144-127,601	5.10.144-127,601+	2.12	Ja	Ja	Ja
			<5.10.144-127,601	(2.10)	Ja	Ja	Nein
	5.4	5,4.214-120,368	5,4.214-120,368+	2.12	Ja	Ja	Ja
			<5,4,214-120,368	(2.10)	Ja	Ja	Nein
	4,14	4,14.294-220,533	4,14.294-220,533+	2.12	Ja	Ja	Ja
			<4,14,294-220,533	(2.10)	Ja	Ja	Nein

Ubuntu-Clients

Betriebssystem	Betriebssystemversion	Minimale Kernelversion	Maximale Kernelversion	Lustre-Clientversion	Lustre-Dateisystemversion		
					2.10	2,12	2,15
Ubuntu	24	6,14.0-1012	6,14,0*	2.15	Nein	Ja	Ja
		6,8,0-1024	6,8,0*	2.15	Nein	Ja	Ja
	22	6,8,0-1017	6,8,0*	2.15	Nein	Ja	Ja
		6,5,0-1023	6,5,0*	2.15	Nein	Ja	Ja
		6.2.0-1017	6.2,0*	2.15	Nein	Ja	Ja
		5.15.0-1015-aws	5.15.0-1051-aws	2.12	Ja	Ja	Ja
	20	5.15.0-1015-aws	5,15,0*	2.12	Ja	Ja	Ja
		5.4.0-1011-aws	5.13.0-1031-aws	(2.10)	Ja	Ja	Nein

RHEL/CentOS/RockyLinux-Kunden

Betriebssystem	Betriebssystemversion	Architektur	Minimale Kernelversion	Maximale Kernelversion	Lustre-Clientversion	Lustre-Dateisystemversion		
						2.10	2,12	2,15
RHEL/Rocky Linux	9.7	Arm + x86	5,14,0-61,5,1	5,14,0-61*	2.15	Nein	Ja	Ja
	9,6	Arm + x86	5,14,0-570,12,1	5,14,0-570*	2.15	Nein	Ja	Ja
	9,5	Arm + x86	5,14,0-503,19,1	5,14,0-503*	2.15	Nein	Ja	Ja
	9.4	Arm + x86	5,14,0-427,13,1	5,14,0-427*	2.15	Nein	Ja	Ja
	9,3	Arm + x86	5,14,0-362,18,1	5,14,0-362,18,1	2.15	Nein	Ja	Ja
	9.0	Arm + x86	5,14,0-70,13,1	5,14,0-70,30,1	2.15	Nein	Ja	Ja
RHEL/CentOS/RockyLinux	8.10	Arm + x86	4,18,0-553	4,18,0-553*	2.12	Ja	Ja	Ja
	8,9	Arm + x86	4,18,0-513*	4,18,0-513*	2.12	Ja	Ja	Ja
	8,8	Arm + x86	4,18,0-477*	4,18,0-477*	2.12	Ja	Ja	Ja

Betriebssystem	Betriebssystemversion	Architektur	Minimale Kernelversion	Maximale Kernelversion	Lustre-Clientversion	Lustre-Dateisystemversion		
	8,7	Arm + x86	4,18,0-42 5*	4,18,0-42 5*	2.12	Ja	Ja	Ja
	8,6	Arm + x86	4,18,0-37 2*	4,18,0-37 2*	2.12	Ja	Ja	Ja
	8,5	Arm + x86	4,18,0-34 8*	4,18,0-34 8*	2.12	Ja	Ja	Ja
	8,4	Arm + x86	4,18,0-30 5*	4,18,0-30 5*	2.12	Ja	Ja	Ja
RHEL/CentOS	8,3	Arm + x86	4,18,0-24 0*	4,18,0-24 0*	(2.10)	Ja	Ja	Nein
	8,2	Arm + x86	4,18,0-19 3*	4,18,0-19 3*	(2.10)	Ja	Ja	Nein
	7,9	86 x	3.10.0-1 60*	3.10.0-1 60*	2.12	Ja	Ja	Ja
	7.8	86 x	3.10.0-1 27*	3.10.0-1 27*	(2.10)	Ja	Ja	Nein
	7.7	86 x	3.10.0-10 62*	3.10.0-10 62*	(2.10)	Ja	Ja	Nein
CentOS	7,9	Arm	4,18,0-19 3*	4,18,0-19 3*	2.12	Ja	Ja	Ja
	7.8	Arm	4,18,0-14 7*	4,18,0-14 7*	2.12	Ja	Ja	Ja

Den Client installieren Lustre

Um Ihr Amazon FSx for Lustre-Dateisystem von einer Linux-Instance aus zu mounten, installieren Sie zunächst den Open-Source-ClientLustre. Verwenden Sie dann, abhängig von Ihrer Betriebssystemversion, eines der folgenden Verfahren. Informationen zur Kernel-Unterstützung finden Sie unterLustreDateisystem- und Client-Kernel-Kompatibilität.

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 im Lustre Wiki unter Kompilieren Lustre.

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:

   - 6.12 Kernel-Mindestanforderung — 6.12*
   - 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 Client. Lustre

   Wenn der Befehl ein Ergebnis zurückgibt, das unter den Kernel-Mindestanforderungen liegt, aktualisieren Sie den Kernel und starten Sie Ihre EC2 Amazon-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 Client. Lustre

   Wenn der Befehl ein Ergebnis zurückgibt, das unter den Kernel-Mindestanforderungen liegt, aktualisieren Sie den Kernel und starten Sie Ihre EC2 Amazon-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-Mindestanforderungen aktualisieren können, können Sie den Legacy-2.10-Client mit dem folgenden Befehl installieren.

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

Um den Lustre Client auf Amazon Linux zu installieren

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 EC2 Amazon-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 Red Hat und Rocky Linux 9.0 oder 9.3—9.7 zu installieren

Sie können Lustre Client-Pakete, die mit Red Hat Enterprise Linux (RHEL) und Rocky Linux kompatibel sind, aus dem Yum-Paket-Repository des FSx Lustre Amazon-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 FSx Lustre Amazon-Clients hinzu

1. Öffnen Sie ein Terminal auf Ihrem Client.

2. Installieren Sie den öffentlichen Amazon FSx RPM-Schlüssel 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 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 FSx Lustre des Amazon-Clients

Das Yum-Paket-Repository des FSx Lustre Amazon-Clients ist standardmäßig so konfiguriert, dass der Lustre Client installiert wird, der mit der Kernel-Version kompatibel ist, die ursprünglich mit der neuesten unterstützten Version von Rocky Linux und RHEL 9 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`5.14.0-611*`, müssen Sie die Repository-Konfiguration nicht ändern. Fahren Sie mit dem Verfahren So installieren Sie den Lustre Client fort.
   - Wenn der Befehl zurückkehrt`5.14.0-570*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre Client für die Versionen Rocky Linux und RHEL 9.6 verweist.

- Wenn der Befehl zurückkehrt`5.14.0-503*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre Client für die Versionen Rocky Linux und RHEL 9.5 verweist.
- Wenn der Befehl zurückkehrt`5.14.0-427*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre Client für die Versionen Rocky Linux und RHEL 9.4 verweist.
- Wenn der Befehl zurückkehrt`5.14.0-362.18.1`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre Client für die Versionen Rocky Linux und RHEL 9.3 verweist.
- Wenn der Befehl zurückkehrt`5.14.0-70*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre Client für die Versionen Rocky Linux und RHEL 9.0 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 9.6 zu verweisen, *`specific_RHEL_version`* ersetzen `9.6` Sie den Befehl durch, wie im folgenden Beispiel.

   ```
   sudo sed -i 's#9#9.6#' /etc/yum.repos.d/aws-fsx.repo
   ```

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

   ```
   sudo yum clean all
   ```

So installieren Sie den Lustre-Client

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

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

Zusätzliche Informationen (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 FSx Amazon-Dateisystem erforderlich sind. Das Repository enthält zusätzliche Lustre Pakete, z. B. ein Paket mit dem Quellcode und Pakete mit Tests, die Sie optional installieren können. 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—8.10 oder auf Rocky Linux 8.4—8.10 zu installieren

Sie können Lustre Client-Pakete, die mit Red Hat Enterprise Linux (RHEL), Rocky Linux und CentOS kompatibel sind, aus dem Yum-Paket-Repository des FSx Lustre Amazon-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 FSx Lustre Amazon-Clients hinzu

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Installieren Sie den öffentlichen Amazon FSx RPM-Schlüssel 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 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 FSx Lustre des Amazon-Clients

Das Yum-Paket-Repository des FSx Lustre Amazon-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-, Rocky Linux- und RHEL 8-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`4.18.0-553*`, müssen Sie die Repository-Konfiguration nicht ändern. Fahren Sie mit dem Verfahren So installieren Sie den Lustre Client fort.
   - Wenn der Befehl zurückkehrt`4.18.0-513*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre Client für die CentOS-, Rocky Linux- und RHEL 8.9-Versionen verweist.

- 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 Versionen CentOS, Rocky Linux und RHEL 8.7 verweist.
- Wenn der Befehl zurückkehrt`4.18.0-372*`, müssen Sie die Repository-Konfiguration so bearbeiten, dass sie auf den Lustre Client für die Versionen CentOS, Rocky Linux und RHEL 8.6 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 Versionen CentOS, Rocky Linux und RHEL 8.4 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 8.9 verweisen möchten, *specific_RHEL_version* ersetzen Sie `8.9` den Befehl durch.

```
sudo sed -i 's#8#8.9#' /etc/yum.repos.d/aws-fsx.repo
```

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

```
sudo yum clean all
```

So installieren Sie den Lustre-Client

- 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 FSx Amazon-Dateisystem erforderlich sind. Das Repository enthält zusätzliche Lustre Pakete, z. B. ein Paket mit dem Quellcode und Pakete mit Tests, die Sie optional installieren können. 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 FSx Lustre Amazon-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 FSx Lustre Amazon-Clients hinzu

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Installieren Sie den öffentlichen Amazon FSx RPM-Schlüssel 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 FSx Lustre des Amazon-Clients

Das Yum-Paket-Repository des FSx Lustre Amazon-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- 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-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#7#specific_RHEL_version#' /etc/yum.repos.d/aws-fsx.repo
```

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

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

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

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

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

```
sudo yum clean all
```

So installieren Sie den Lustre-Client

- 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 FSx Amazon-Dateisystem erforderlich sind. Das Repository enthält zusätzliche Lustre Pakete, z. B. ein Paket mit dem Quellcode und Pakete mit Tests, die Sie optional installieren können. 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 (ARM-basierte AWS Graviton-Instanzen)

Sie können Lustre Client-Pakete aus dem Yum-Paket-Repository des FSx Lustre Amazon-Clients installieren und aktualisieren, die mit CentOS 7 für AWS ARM-basierte Graviton-basierte Instances kompatibel sind. EC2 Diese Pakete sind signiert, um sicherzustellen, dass sie vor oder während des Herunterladens 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 FSx Lustre Amazon-Clients hinzu

1. Öffnen Sie ein Terminal auf Ihrem Client.
2. Installieren Sie den öffentlichen Amazon FSx RPM-Schlüssel 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 FSx Lustre des Amazon-Clients

Das Yum-Paket-Repository des FSx Lustre Amazon-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
```

So installieren Sie den Lustre-Client

- 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 Graviton-basierte Instances AWS) EC2

Mit den obigen Befehlen werden die beiden Pakete installiert, die für das Mounten und die Interaktion mit Ihrem FSx Amazon-Dateisystem erforderlich sind. Das Repository enthält zusätzliche Lustre Pakete, z. B. ein Paket mit dem Quellcode und Pakete mit Tests, die Sie optional installieren können. 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 18.04, 20.04, 22.04 oder 24.04 zu installieren

Sie können Lustre Pakete aus dem Amazon FSx Ubuntu-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 FSx Amazon-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 $(lsb_release -cs) 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. Eine Liste der erforderlichen Kernel für den Lustre Client auf Ubuntu sowohl für x86-basierte EC2 Instances als auch für ARM-basierte EC2 Instances, die mit Graviton-Prozessoren betrieben werden, finden Sie unter. AWS Ubuntu-Clients

   a. Führen Sie den folgenden Befehl aus, um festzustellen, welcher Kernel läuft.

   ```
   uname -r
   ```

   b. Führen Sie den folgenden Befehl aus, um auf den neuesten Ubuntu-Kernel und die neueste Lustre Version zu aktualisieren und dann den Computer neu zu starten.

```
sudo apt install -y linux-aws lustre-client-modules-aws && sudo reboot
```

Wenn Ihre Kernelversion höher ist als die Kernel-Mindestversion sowohl für x86-basierte EC2 Instances als auch für Graviton-basierte EC2 Instances und Sie nicht auf die neueste Kernel-Version aktualisieren möchten, können Sie mit dem folgenden Befehl Lustre für den aktuellen Kernel 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 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

Um den Lustre Client unter SUSE Linux 12 zu installieren SP3 SP4, oder SP5

Um den Lustre Client unter SUSE Linux 12 zu installieren SP3

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

   ```
   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 unter SUSE Linux 12 zu installieren SP4

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

```
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 zu migriert SP4 und zuvor das FSx Amazon-Repository für hinzugefügt haben SP3, 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
```

So installieren Sie den Lustre Client unter SUSE Linux 12 SP5

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

```
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 zu migriert SP5 und zuvor das FSx Amazon-Repository für hinzugefügt haben SP4, 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 EC2 Amazon-Instance aus mounten.

So mounten Sie Ihr Dateisystem von Amazon EC2

1. Connect zu Ihrer EC2 Amazon-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 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. Stellen Sie sicher, 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 FSx Amazon-Dateisystem, das auf /fsx gemountet ist.

Konfiguration von EFA-Clients

Gehen Sie wie folgt vor, um Ihren Lustre-Client für den Zugriff auf ein FSx for Lustre-Dateisystem über den Elastic Fabric Adapter (EFA) einzurichten.

EFA wird auf Lustre-Clients unterstützt, auf denen die folgenden Betriebssysteme ausgeführt werden:

- Amazon Linux 2023 (AL2023)
- Red Hat Enterprise Linux (RHEL) 9.5 oder neuer
- Ubuntu 22.04 oder neuer mit Kernel-Version 6.8+

EFA wird auf den unten aufgeführten Lustre-Clients unterstützt. Weitere Informationen finden Sie unter Den Client installieren Lustre.

EFA wird auf Nitro EC2 v4-Instances (oder höher) unterstützt, die EFA unterstützen, mit Ausnahme der trn2-Instance-Familie. Weitere Informationen finden Sie im EC2 Amazon-Benutzerhandbuch unter Unterstützte Instance-Typen.

Themen

- Schritt 1: Installieren Sie die erforderlichen Treiber
- Schritt 2: EFA für den Lustre-Client konfigurieren
- Schritt 3: EFA-Schnittstellen

Schritt 1: Installieren Sie die erforderlichen Treiber

> **Note**
>
> Wenn Sie ein Deep Learning-AMI verwenden, können Sie diesen Schritt überspringen, da sowohl der EFA-Treiber als auch der GPUDirect NVIDIA-Speichertreiber (GDS) vorinstalliert sind.

Installieren Sie den EFA-Treiber

Folgen Sie den Anweisungen in Schritt 3: Installation der EFA-Software im EC2 Amazon-Benutzerhandbuch.

Installieren Sie den GDS-Treiber (optional)

Dieser Schritt ist nur erforderlich, wenn Sie NVIDIA GPUDirect Storage (GDS) mit FSx for Lustre verwenden möchten.

Voraussetzungen:

- Amazon EC2 P5-, P5e-, P5en-, P6-B200- oder P6e-00-Instanz GB2
- NVIDIA GDS-Treiberversion 2.24.2 oder höher

Um den GPUDirect NVIDIA-Speichertreiber auf Ihrer Client-Instanz zu installieren

1. Klonen Sie das NVIDIA GDS-Repository:

```
git clone https://github.com/NVIDIA/gds-nvidia-fs.git
```

2. Erstellen und installieren Sie den Treiber:

```
cd gds-nvidia-fs/src/
export NVFS_MAX_PEER_DEVS=128
export NVFS_MAX_PCI_DEPTH=16
sudo -E make
sudo insmod nvidia-fs.ko
```

Schritt 2: EFA für den Lustre-Client konfigurieren

Um über eine EFA-Schnittstelle auf ein FSx for Lustre-Dateisystem zuzugreifen, müssen Sie die Lustre-EFA-Module installieren und EFA-Schnittstellen konfigurieren.

Quick Setup

Um Ihren Lustre-Client schnell zu konfigurieren

1. Connect zu Ihrer EC2 Amazon-Instance her.
2. Laden Sie die Datei mit dem Konfigurationsskript herunter und entpacken Sie sie:

   ```
   curl -O https://docs.aws.amazon.com/fsx/latest/LustreGuide/samples/configure-efa-fsx-lustre-client.zip
   unzip configure-efa-fsx-lustre-client.zip
   ```

3. Wechseln Sie in den `configure-efa-fsx-lustre-client` Ordner und führen Sie das Setup-Skript aus:

   ```
   cd configure-efa-fsx-lustre-client
   sudo ./setup.sh
   ```

   Das Skript führt automatisch Folgendes aus:

   - Importiert Lustre-Module
   - Konfiguriert TCP- und EFA-Schnittstellen
   - Erzeugt einen Systemd-Dienst für die automatische Konfiguration beim Neustart

   Eine Liste der Optionen und Anwendungsbeispiele, die Sie mit dem `setup.sh` Skript verwenden können, finden Sie in der `README.md` Datei in der ZIP-Datei.

Manuelles Verwalten des Systemd-Dienstes

Die Systemd-Dienstdatei wird unter/etc/systemd/system/configure- efa-fsx-lustre-client .service erstellt. Im Folgenden finden Sie einige hilfreiche Befehle im Zusammenhang mit Systemd:

```
# Check status
sudo systemctl status configure-efa-fsx-lustre-client.service
```

```
# View logs
sudo journalctl -u configure-efa-fsx-lustre-client.service
# View warnings/errors from dmesg
sudo dmesg
```

Weitere Informationen finden Sie in der `README.md` Datei in der ZIP-Datei.

Konfiguration für automatisches Mounten (optional)

Informationen zum automatischen Mounten Ihres Amazon FSx for Lustre-Dateisystems beim Systemstart finden Sie unterAutomatisches Mounten Ihres FSx Amazon-Dateisystems.

Schritt 3: EFA-Schnittstellen

Jedes Dateisystem FSx für Lustre hat ein maximales Limit von 1024 EFA-Verbindungen für alle Client-Instanzen.

Das `configure-efa-fsx-lustre-client.sh` Skript konfiguriert automatisch EFA-Schnittstellen auf der Grundlage des Instanztyps.

Instance-Typ	Standardanzahl von EFA-Schnittstellen
p6e-gb200.36xlarge	8
p6-b 200.48x groß	8
p5en.48x groß	8
p 5e. 48 x groß	8
p5.48xlarge	8
Andere Instanzen mit mehreren Netzwerkkarten	2
Andere Instanzen mit einer einzigen Netzwerkkarte	1

Jede konfigurierte EFA-Schnittstelle auf einer Client-Instance zählt als eine Verbindung im Hinblick auf das EFA-Verbindungslimit von 1024, wenn sie mit einem FSx for Lustre-Dateisystem verbunden ist.

Manuelles Verwalten von EFA-Schnittstellen

Instances mit mehr EFA-Schnittstellen unterstützen in der Regel einen höheren Durchsatz. Sie können die Anzahl der Schnittstellen anpassen, um die Leistung für Ihre spezifischen Workloads zu optimieren, solange Sie das gesamte EFA-Verbindungslimit einhalten.

Sie können EFA-Schnittstellen mit den folgenden Befehlen manuell verwalten:

1. Verfügbare EFA-Geräte anzeigen:

```
for interface in /sys/class/infiniband/*; do
    if [ ! -e "$interface/device/driver" ]; then continue; fi
    driver=$(basename "$(realpath "$interface/device/driver")")
    if [ "$driver" != "efa" ]; then continue; fi
    echo $(basename $interface)
done
```

2. Aktuell konfigurierte Schnittstellen anzeigen:

```
sudo lnetctl net show
```

3. Fügen Sie eine EFA-Schnittstelle hinzu:

```
sudo lnetctl net add --net efa --if device_name –peer-credits 32
```

   *device_name*Ersetzen Sie es durch einen tatsächlichen Gerätenamen aus der Liste in Schritt 1.

4. Entfernen Sie eine EFA-Schnittstelle:

```
sudo lnetctl net del --net efa --if device_name
```

   *device_name*Ersetzen Sie es durch einen tatsächlichen Gerätenamen aus der Liste in Schritt 2.

Montage über Amazon Elastic Container Service

Sie können über einen Docker-Container von Amazon Elastic Container Service (Amazon ECS) auf einer Amazon-Instance auf Ihr FSx for Lustre-Dateisystem zugreifen. EC2 Sie können dazu eine der folgenden Optionen verwenden:

1. Indem Sie Ihr FSx for Lustre-Dateisystem von der EC2 Amazon-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 EC2 Amazon-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 Montage FSx von Lustre auf einem AWS Fargate-Starttyp wird nicht unterstützt.

In den folgenden Abschnitten werden die Verfahren für die einzelnen Optionen zum Mounten Ihres FSx for Lustre-Dateisystems aus einem Amazon ECS-Container beschrieben.

Themen

- Mounten von einer EC2 Amazon-Instance aus, die Amazon ECS-Aufgaben hostet
- Mounten aus einem Docker-Container

Mounten von einer EC2 Amazon-Instance aus, die Amazon ECS-Aufgaben hostet

Dieses Verfahren zeigt, wie Sie eine Amazon EC2 ECS-On-Instance konfigurieren können, um Ihr FSx for Lustre-Dateisystem lokal zu mounten. Das Verfahren verwendet `volumes` Eigenschaften von `mountPoints` Containern, 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 Client installieren Lustre

So mounten Sie Ihr Dateisystem von Amazon ECS auf einer EC2 Instance

1. Wenn Sie Amazon ECS-Instances entweder manuell oder mithilfe einer Auto Scaling Scaling-Gruppe starten, fügen Sie die Zeilen im folgenden Codebeispiel am Ende des Benutzerdatenfeldes hinzu. Ersetzen Sie die folgenden Elemente im Beispiel:

   - *`file_system_dns_name`*Ersetzen Sie es durch den tatsächlichen DNS-Namen des Dateisystems.
   - *`mountname`*Ersetzen Sie durch den Mount-Namen des Dateisystems.
   - *`mountpoint`*Ersetzen Sie ihn durch den 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 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 durch den Mount-Namen des Dateisystems.
   - Ersetzen Sie *`mountpoint`* durch den Mountingpunkt des Dateisystems.

```
"command": [
  "/bin/sh -c \"amazon-linux-extras install -y lustre; mount -t
 lustre file_system_dns_name@tcp:/mountname mountpoint -o relatime,flock;\""
```

```
],
```

2. Fügen Sie Ihrem Container die `SYS_ADMIN` Möglichkeit hinzu, ihn mithilfe der Eigenschaft zum Mounten Ihres FSx for Lustre-Dateisystems zu autorisieren. `linuxParameters`

```
"linuxParameters": {
  "capabilities": {
      "add": [
        "SYS_ADMIN"
      ]
   }
}
```

Mounten von FSx Amazon-Dateisystemen vor Ort oder über eine Peering-Amazon-VPC

Sie können auf zwei Arten auf Ihr FSx Amazon-Dateisystem zugreifen. Eine stammt von EC2 Amazon-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 Direct Connect der VPC Ihres Dateisystems verbunden sind.

Sie verbinden die VPC des Kunden und die VPC Ihres FSx Amazon-Dateisystems entweder über eine VPC-Peering-Verbindung oder ein VPC-Transit-Gateway. Wenn Sie eine VPC-Peering-Verbindung oder ein Transit-Gateway für die Verbindung verwenden VPCs, können EC2 Amazon-Instances, die sich in einer VPC befinden, auf FSx Amazon-Dateisysteme in einer anderen VPC zugreifen, auch wenn sie zu unterschiedlichen Konten VPCs 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, über den Sie Ihre Netzwerke und Ihre VPCs lokalen 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 Dieser Verbindungstyp ermöglicht es Ihnen, den Verkehr zwischen ihnen mithilfe von privaten Internetprotokolladressen der Version 4 (IPv4) oder der Internetprotokollversion 6 (IPv6)

weiterzuleiten. Sie können VPC-Peering verwenden, um eine Verbindung VPCs innerhalb derselben AWS Region oder zwischen AWS Regionen herzustellen. 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 FSx Amazon-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
VPCs Mit VPC Peering gepeert oder AWS Transit Gateway	Clients mit IP-Adressen in einem privaten IP-Adressbereich nach RFC 1918:	✓
Peering-Netzwerke, die oder verwenden Direct Connect Site-to-Site VPN	• 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	✓

Wenn Sie mit einem nicht privaten IP-Adressbereich auf Ihr FSx Amazon-Dateisystem zugreifen müssen, das vor dem 17. Dezember 2020 erstellt wurde, können Sie ein neues Dateisystem erstellen, indem Sie eine Sicherungskopie des Dateisystems wiederherstellen. Weitere Informationen finden Sie unter Schützen Sie Ihre Daten mit Backups.

Um die IP-Adresse der primären Netzwerkschnittstelle für ein Dateisystem abzurufen

1. Öffnen Sie die FSx Amazon-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 EC2 Amazon-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 FSx Amazon-Dateisystem von außerhalb der VPC mounten, mit der es verknüpft ist.

Automatisches Mounten Ihres FSx Amazon-Dateisystems

Sie können die `/etc/fstab` Datei in Ihrer EC2 Amazon-Instance aktualisieren, nachdem Sie zum ersten Mal eine Verbindung mit der Instance hergestellt haben, sodass Ihr FSx Amazon-Dateisystem bei jedem Neustart bereitgestellt wird.

Automatisches Mounten für Lustre mithilfe von /etc/fstab FSx

Um Ihr FSx Amazon-Dateisystemverzeichnis beim Neustart der EC2 Amazon-Instance automatisch zu mounten, können Sie die `fstab` Datei verwenden. 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 FSx Amazon-Dateisystem bereits erstellt haben. Weitere Informationen finden Sie Schritt 1: Erstellen Sie Ihr FSx for Lustre-Dateisystem in der Übung Erste Schritte.
> - Für EFA-fähige Dateisysteme ist die Konfiguration von systemd eine Voraussetzung. Weitere Informationen finden Sie unter Quick Setup.

Um die Datei /etc/fstab in Ihrer Instanz zu aktualisieren EC2

1. Connect zu Ihrer EC2 Instance her und öffnen Sie die `/etc/fstab` Datei 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 FSx Amazon-Dateisystem mounten möchten.
   - *`file_system_dns_name`*Ersetzen Sie es durch den eigentlichen DNS-Namen des Dateisystems.
   - *`mountname`*Ersetzen Sie durch den Mount-Namen des Dateisystems. Dieser Mount-Name wird in der Antwort auf den `CreateFileSystem` API-Vorgang zurückgegeben. Er wird auch in der Antwort auf den describe-file-systems AWS CLI Befehl und in der `DescribeFileSystems` API-Operation zurückgegeben.

   Für Nicht-EFA-Dateisysteme:

   ```
   file_system_dns_name@tcp:/mountname /fsx lustre defaults,relatime,flock,_netdev,x-systemd.automount,x-systemd.requires=network.service 0 0
   ```

   Für EFA-fähige Dateisysteme:

   ```
   file_system_dns_name@tcp:/mountname /fsx lustre defaults,relatime,flock,_netdev,x-systemd.automount,x-systemd.requires=configure-efa-fsx-lustre-client.service,x-systemd.after=configure-efa-fsx-lustre-client.service 0 0
   ```

   > **Warning**
   >
   > Verwenden Sie beim automatischen Mounting Ihres Dateisystems die Option `_netdev`, um es als Netzwerkdateisystem zu identifizieren. Falls `_netdev` fehlt, reagiert Ihre EC2 Instance möglicherweise nicht mehr. Der Grund dafür ist, dass zuerst das Netzwerk auf der Datenverarbeitungs-Instance gestartet worden sein muss. Die Netzwerkdateisysteme müssen danach initialisiert werden. Weitere Informationen finden Sie unter Automatisches Mounting schlägt fehl und die Instance reagiert nicht.

3. Speichern Sie die Änderungen an der Datei.

Ihre EC2 Instance ist jetzt so konfiguriert, dass sie das FSx Amazon-Dateisystem bei jedem Neustart mountet.

> **Note**
>
> In einigen Fällen muss Ihre EC2 Amazon-Instance möglicherweise unabhängig vom Status Ihres bereitgestellten FSx Amazon-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	Description
file_system_dns_name `@tcp:/`	Der DNS-Name für Ihr FSx Amazon-Dateisystem, der das Dateisystem identifiziert. Sie können diesen Namen von der Konsole oder programmgesteuert aus dem AWS CLI oder einem AWS SDK abrufen.
mountname	Der Mount-Name für das Dateisystem. Sie können diesen Namen von der Konsole oder programmgesteuert AWS CLI mithilfe des describe-file-systems Befehls oder der AWS API oder des SDK mithilfe des `DescribeFileSystems` Vorgangs abrufen.
/fsx	Der Bereitstellungspunkt für das FSx Amazon-Dateisystem auf Ihrer EC2 Instance.
`lustre`	Der Typ des Dateisystems, Amazon FSx.
`mount options`	Einhängeoptionen für das Dateisystem, dargestellt als kommagetrennte 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-Zugriffszeiten), jedoch nicht für jeden Dateizugriff. Wenn diese Option aktiviert

Feld	Description
	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.
`x-systemd .automount,x- systemd.requir es=networ k.service`	Diese Optionen für Nicht-EFA-Dateisysteme stellen sicher, dass der Auto Mounter erst ausgeführt wird, wenn die Netzwerkverbindung online ist. **Note** Verwenden Sie für Amazon Linux 2023 und Ubuntu 22.04 und höher die `x-systemd.requires=systemd-networkd- wait-online.service` Option anstelle der `x-systemd .requires=network.service` Option.

Feld	Description
`x-systemd .automount,x- systemd.requir es=configure- efa-fsx-lustre- client.service,x- systemd.a fter=configure- efa-fsx-lustre- client.service`	Diese Optionen für EFA-fähige Dateisysteme stellen sicher, dass der Auto Mounter erst nach Abschluss der EFA-Client-Konfiguration ausgeführt wird.
`0`	Ein Wert, der angibt, ob das Dateisystem von gesichert werden soll. `dump` Für Amazon FSx sollte dieser Wert sein`0`.
`0`	Ein Wert, der die Reihenfolge angibt, in der Dateisysteme beim Booten `fsck` überprüft werden. Für FSx Amazon-Dateisysteme sollte dieser Wert angeben`0`, dass sie beim Start nicht ausgeführt werden `fsck` sollen.

Mounten bestimmter Dateisätze

Mithilfe der Lustre Dateisatzfunktion können Sie nur eine Teilmenge des Dateisystem-Namespaces einhängen, 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 Dateisatz ein Lustre

1. Angenommen, Sie haben ein FSx for Lustre-Dateisystem mit den folgenden Verzeichnissen:

```
team1/dataset1/
team2/dataset2/
```

2. Sie mounten nur den `team1/dataset1` Dateisatz, sodass nur dieser Teil des Dateisystems lokal auf dem Client sichtbar ist. Verwenden Sie den folgenden Befehl und ersetzen Sie die folgenden Elemente:

   - *`file_system_dns_name`*Ersetzen Sie es durch den tatsächlichen DNS-Namen des Dateisystems.
   - *`mountname`*Ersetzen Sie durch den Mount-Namen des Dateisystems. Dieser Mount-Name wird in der Antwort auf den `CreateFileSystem` API-Vorgang zurückgegeben. Er wird auch in der Antwort auf den describe-file-systems AWS CLI Befehl und in der 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 Verwaltungsbefehle, die Zugriff auf das `.lustre/` Verzeichnis erfordern, möglicherweise nicht, 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 Dokumentationswebsite. Lustre

Aufheben des Mountings von Dateisystemen

Bevor Sie ein FSx for Lustre-Dateisystem löschen, stellen Sie sicher, dass es von allen EC2 Amazon-Instances, die es bereitgestellt haben, getrennt ist, und stellen Sie vor dem Herunterfahren oder Beenden einer EC2 Amazon-Instance sicher, dass alle FSx für Lustre-Dateisysteme von dieser Instance gemountet werden.

FSx für Lustre gewähren Server den Clients während des I/O Betriebs temporäre Datei- und Verzeichnissperren, und Clients müssen umgehend reagieren, wenn Server Clients auffordern, ihre Sperren aufzuheben, um Operationen zu entsperren. I/O operations from other clients. If clients become non-responsive, they may be forcefully evicted after several minutes to allow other clients to proceed with their requested I/O Um diese Wartezeiten zu vermeiden, sollten Sie das Dateisystem immer von den Client-Instances trennen, bevor Sie sie herunterfahren oder beenden und bei Lustre-Dateisystemen vor dem Löschen FSx .

Sie können ein Dateisystem auf Ihrer EC2 Amazon-Instance unmounten, indem Sie den `umount` Befehl auf der Instance selbst ausführen. Sie können ein FSx Amazon-Dateisystem nicht über das AWS CLI AWS-Managementkonsole, das oder über eines der AWS SDKs. Um ein FSx Amazon-Dateisystem auszuhängen, das mit einer EC2 Amazon-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 FSx Amazon-Dateisystem unmountet wurde, indem Sie den `df` Befehl ausführen. Dieser Befehl zeigt die Festplattennutzungsstatistiken für die Dateisysteme an, die derzeit auf Ihrer Linux-basierten EC2 Amazon-Instance gemountet sind. Wenn das FSx Amazon-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 FSx Amazon-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 EC2 Amazon-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 übersteigt, wenn die Nachfrage nach Spot-Instances steigt oder wenn das Angebot an Spot-Instances sinkt.

Wenn Amazon eine Spot-Instance EC2 unterbricht, wird eine Benachrichtigung zur Unterbrechung der Spot-Instance angezeigt, sodass die Instance zwei Minuten lang gewarnt wird, bevor Amazon sie EC2 unterbricht. Weitere Informationen finden Sie unter Spot-Instances im EC2 Amazon-Benutzerhandbuch.

Um sicherzustellen, dass FSx Amazon-Dateisysteme nicht von EC2 Spot-Instance-Unterbrechungen betroffen sind, empfehlen wir, die Bereitstellung von FSx Amazon-Dateisystemen aufzuheben, bevor Spot-Instances beendet oder in den Ruhezustand versetzt werden. EC2 Weitere Informationen finden Sie unter Aufheben des Mountings von Dateisystemen.

Umgang mit Amazon EC2 Spot-Instance-Unterbrechungen

FSx for Lustre ist ein verteiltes Dateisystem, in dem Server- und Client-Instances zusammenarbeiten, um ein leistungsstarkes und zuverlässiges Dateisystem bereitzustellen. Sie sorgen für einen verteilten und kohärenten Zustand auf Client- und Serverinstanzen. FSx für Lustre delegieren Server temporäre Zugriffsberechtigungen an Clients, während sie aktiv Dateisystemdaten I/O bearbeiten und zwischenspeichern. Von Clients wird erwartet, dass sie innerhalb kurzer Zeit antworten, wenn Server sie auffordern, ihre temporären Zugriffsberechtigungen zu widerrufen. Um das Dateisystem vor fehlerhaften Clients zu schützen, können Server Clients, die nach einigen Minuten Lustre 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 Spot-Instances beenden. EC2

EC2 Spot sendet Kündigungsmitteilungen 2 Minuten im Voraus, bevor eine Instance heruntergefahren wird. Wir empfehlen Ihnen, vor dem EC2 Beenden von Spot-Instances den Vorgang des sauberen Aushängens der Lustre Clients zu automatisieren.

Example — Skript zum sauberen Aushängen terminierender Spot-Instances EC2

Dieses Beispielskript macht die Bereitstellung terminierter Spot-Instances sauber rückgängig, indem EC2 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/spot/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/spot/instance-action
    echo

    # Gracefully stop applications accessing the filesystem
    #
    # TODO*: Replace with the proper command to stop your application if possible*

    # Kill every process still accessing Lustre filesystem
    echo "Kill every process still accessing Lustre filesystem..."
    fuser -kMm -TERM "${FSXPATH}"; sleep 2
    fuser -kMm -KILL "${FSXPATH}"; sleep 2

    # Unmount FSx For Lustre filesystem
    if ! umount -c "${FSXPATH}"; then
        echo "Error unmounting '$FSXPATH'. Processes accessing it:" >&2
        lsof "${FSXPATH}"

        echo "Retrying..."
        continue
    fi

    # Start a graceful shutdown of the host
    shutdown now

done
```

Verwaltung von Dateisystemen

FSx for Lustre bietet eine Reihe von Funktionen, die die Ausführung Ihrer Verwaltungsaufgaben 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), Amazon FSx API oder verwalten. AWS SDKs

Themen

Arbeiten mit EFA-fähigen Dateisystemen

Wenn Sie ein Dateisystem mit einer Durchsatzkapazität GBps von über 10% erstellen, empfehlen wir, den Elastic Fabric Adapter (EFA) zu aktivieren, um den Durchsatz pro Client-Instance zu optimieren. EFA ist eine leistungsstarke Netzwerkschnittstelle, die zur Leistungssteigerung eine maßgeschneiderte Technik zur Umgehung des Betriebssystems und das Netzwerkprotokoll AWS Scalable Reliable Datagram (SRD) verwendet. Informationen zu EFA finden Sie unter Elastic Fabric Adapter für AI/ML und HPC-Workloads bei Amazon EC2 im EC2 Amazon-Benutzerhandbuch.

EFA-fähige Dateisysteme unterstützen zwei zusätzliche Leistungsmerkmale: GPUDirect Storage (GDS) und ENA Express. Die GDS-Unterstützung baut auf EFA auf, um die Leistung weiter zu verbessern, indem sie die direkte Datenübertragung zwischen dem Dateisystem und dem GPU-Speicher unter Umgehung der CPU ermöglicht. Dieser direkte Pfad macht redundante Speicherkopien und die Beteiligung der CPU an den Datenübertragungsvorgängen überflüssig. Mit EFA- und GDS-Unterstützung können Sie einen höheren Durchsatz für einzelne EFA-fähige Client-Instances erzielen. ENA Express bietet optimierte Netzwerkkommunikation für EC2 Amazon-Instances mithilfe eines fortschrittlichen Pfadauswahlalgorithmus und eines verbesserten Mechanismus zur Überlastungskontrolle. Mit der ENA Express-Unterstützung können Sie einen höheren Durchsatz für einzelne ENA Express-fähige Client-Instances erzielen. Informationen zu ENA Express finden Sie unter Verbessern der Netzwerkleistung zwischen EC2 Instances mit ENA Express im EC2 Amazon-Benutzerhandbuch.

Themen

Überlegungen bei der Verwendung von EFA-fähigen Dateisystemen

Hier sind einige wichtige Punkte, die Sie bei der Erstellung von EFA-fähigen Dateisystemen berücksichtigen sollten:

- Mehrere Konnektivitätsoptionen: EFA-fähige Dateisysteme können mithilfe von ENA, ENA Express und EFA mit Client-Instances kommunizieren.
- Bereitstellungstyp: EFA wird auf Persistent 2-Dateisystemen mit einer angegebenen Metadatenkonfiguration unterstützt, einschließlich Dateisystemen, die die Intelligent-Tiering-Speicherklasse verwenden.
- Aktualisierung der EFA-Einstellung: Sie können EFA aktivieren, wenn Sie ein neues Dateisystem erstellen, aber Sie können EFA nicht in einem vorhandenen Dateisystem aktivieren oder deaktivieren.
- Skalierung des Durchsatzes anhand der Speicherkapazität: Sie können die Speicherkapazität auf einem EFA-fähigen SSD-basierten Dateisystem skalieren, um die Durchsatzkapazität zu erhöhen, aber Sie können die Durchsatzstufe eines EFA-fähigen Dateisystems nicht ändern.
- AWS-Regionen: Eine Liste der unterstützten EFA-fähigen AWS-Regionen Persistent 2-Dateisysteme finden Sie unter. Art der Bereitstellung, Verfügbarkeit

Voraussetzungen für die Verwendung von EFA-fähigen Dateisystemen

Im Folgenden sind die Voraussetzungen für die Verwendung von EFA-fähigen Dateisystemen aufgeführt:

So erstellen Sie Ihr EFA-fähiges Dateisystem:

- Verwenden Sie eine EFA-fähige Sicherheitsgruppe. Weitere Informationen finden Sie unter EFA-fähige Sicherheitsgruppen.
- Verwenden Sie dieselbe Availability Zone und /16 CIDR wie Ihre EFA-fähigen Client-Instances in Ihrer Amazon VPC.
- Auf Intelligent-Tiering-Dateisystemen wird EFA nur mit einer Durchsatzkapazität von 4.000 oder Schritten von 4.000 unterstützt. MBps MBps

So greifen Sie mit dem Elastic Fabric Adapter (EFA) auf Ihr Dateisystem zu:

- Verwenden Sie Nitro EC2 v4-Instances (oder höher), die EFA unterstützen, mit Ausnahme der trn2-Instance-Familie. Weitere Informationen finden Sie im EC2 Amazon-Benutzerhandbuch unter Unterstützte Instance-Typen.
- Führen Sie AL2 023, RHEL 9.5 und neuer oder Ubuntu 22+ mit Kernelversion 6.8 und neuer aus. Weitere Informationen finden Sie unter Den Client installieren Lustre.
- Installieren Sie die EFA-Module und konfigurieren Sie EFA-Schnittstellen auf Ihren Client-Instances. Weitere Informationen finden Sie unter Konfiguration von EFA-Clients.

So greifen Sie mit GPUDirect Storage (GDS) auf Ihr Dateisystem zu:

- Verwenden Sie eine Amazon EC2 P5-, P5e-, P5en-, P6-B200- oder P6e-00-Client-Instance. GB2
- Installieren Sie das NVIDIA Compute Unified Device Architecture (CUDA) -Paket, den Open-Source-NVIDIA-Treiber und den NVIDIA-Speichertreiber auf Ihrer Client-Instance. GPUDirect Weitere Informationen finden Sie unter Installieren Sie den GDS-Treiber (optional).

So greifen Sie mit ENA Express auf Ihr Dateisystem zu:

- Verwenden Sie EC2 Amazon-Instances, die ENA Express unterstützen. Weitere Informationen finden Sie unter Unterstützte Instance-Typen für ENA Express im EC2 Amazon-Benutzerhandbuch.

- Aktualisieren Sie die Einstellungen für Ihre Linux-Instance. Weitere Informationen finden Sie unter Voraussetzungen für Linux-Instances im EC2 Amazon-Benutzerhandbuch.
- Aktivieren Sie ENA Express auf Netzwerkschnittstellen für Ihre Client-Instances. Einzelheiten finden Sie unter Überprüfen der ENA Express-Einstellungen für Ihre EC2 Instance im EC2 Amazon-Benutzerhandbuch.

Ein EFA-fähiges Dateisystem erstellen

Dieser Abschnitt enthält Anweisungen zum Erstellen eines FSx für Lustre EFA-fähigen Dateisystems mit dem. AWS CLI Informationen zum Erstellen eines EFA-fähigen Dateisystems mithilfe der FSx Amazon-Konsole finden Sie unter. Schritt 1: Erstellen Sie Ihr FSx for Lustre-Dateisystem

So erstellen Sie ein EFA-fähiges Dateisystem (CLI)

Verwenden Sie den create-file-systemCLI-Befehl (oder die entsprechende CreateFileSystemAPI-Operation). Im folgenden Beispiel wird ein EFA-fähiges Dateisystem FSx für Lustre mit einem `PERSISTENT_2` Bereitstellungstyp erstellt.

```
aws fsx create-file-system\
   --storage-capacity 4800 \
   --storage-type SSD \
   --file-system-type LUSTRE \
   --file-system-type-version 2.15 \
   --subnet-ids subnet-01234567890 \
   --security-group-ids sg-0123456789abcdefg \
   --lustre-configuration '{"DeploymentType": "PERSISTENT_2", "EfaSupport": true}'
```

Nach erfolgreicher Erstellung des Dateisystems FSx gibt Amazon die Beschreibung des Dateisystems im JSON-Format zurück.

Die Verwendung von Lustre Speicherkontingente

Sie können Speicherkontingente für Benutzer, Gruppen und Projekte auf FSx Lustre-Dateisystemen erstellen. Mit Speicherkontingenten können Sie den Speicherplatz und die Anzahl der Dateien, die ein Benutzer, eine Gruppe oder ein Projekt verbrauchen kann, einschränken. Speicherkontingente verfolgen automatisch die Nutzung auf Benutzer-, Gruppen- und Projektebene, sodass Sie den Verbrauch überwachen können, unabhängig davon, ob Sie Speicherlimits festlegen oder nicht.

Amazon FSx setzt Kontingente durch und verhindert, dass Benutzer, die diese überschritten haben, auf den Speicherplatz schreiben. Wenn Benutzer ihre Kontingente überschreiten, müssen sie genügend Dateien löschen, um die Kontingentgrenzen zu überschreiten, sodass sie wieder in das Dateisystem schreiben können.

Themen

Durchsetzung von Kontingenten

Die Durchsetzung von Benutzer-, Gruppen- und Projektkontingenten wird automatisch auf allen Dateisystemen FSx für Lustre aktiviert. Die Durchsetzung von Kontingenten kann nicht deaktiviert werden.

Arten von Kontingenten

Systemadministratoren mit AWS Root-Benutzeranmeldedaten können die folgenden Arten von Kontingenten erstellen:

- Ein Benutzerkontingent gilt für einen einzelnen Benutzer. Ein Benutzerkontingent für einen bestimmten Benutzer kann sich von den Kontingenten anderer Benutzer unterscheiden.
- Ein Gruppenkontingent gilt für alle Benutzer, die Mitglieder einer bestimmten Gruppe sind.
- Ein Projektkontingent gilt für alle Dateien oder Verzeichnisse, die einem Projekt zugeordnet sind. Ein Projekt kann mehrere Verzeichnisse oder einzelne Dateien enthalten, die sich in verschiedenen Verzeichnissen innerhalb eines Dateisystems befinden.

> **Note**
>
> Projektkontingente werden nur unterstützt auf Lustre Version 2.15 auf FSx für Lustre-Dateisysteme.

- Ein Blockkontingent begrenzt den Speicherplatz, den ein Benutzer, eine Gruppe oder ein Projekt belegen kann. Sie konfigurieren die Speichergröße in Kilobyte.
- Ein Inode-Kontingent begrenzt die Anzahl der Dateien oder Verzeichnisse, die ein Benutzer, eine Gruppe oder ein Projekt erstellen kann. Sie konfigurieren die maximale Anzahl von Inodes als Ganzzahl.

> **Note**
>
> Standardkontingente werden nicht unterstützt.

Wenn Sie Kontingente für einen bestimmten Benutzer und eine Gruppe festlegen und der Benutzer Mitglied dieser Gruppe ist, gilt die Datennutzung des Benutzers für beide Kontingente. Es ist auch durch beide Kontingente begrenzt. Wenn eine der Kontingentgrenzen erreicht wird, wird der Benutzer daran gehindert, in das Dateisystem zu schreiben.

> **Note**
>
> Für den Root-Benutzer festgelegte Kontingente werden nicht durchgesetzt. In ähnlicher Weise umgeht das Schreiben von Daten als Root-Benutzer mithilfe des `sudo` Befehls die Durchsetzung des Kontingents.

Kontingentgrenzen und Übergangsfristen

Amazon FSx setzt Nutzer-, Gruppen- und Projektkontingente als festes Limit oder als Soft-Limit mit konfigurierbarem Kulanzzeitraum durch.

Das harte Limit ist das absolute Limit. Wenn Benutzer ihr festes Limit überschreiten, schlägt eine Block- oder Inode-Zuweisung fehl und es wird eine Meldung angezeigt, dass das Festplattenkontingent überschritten wurde. Benutzer, die ihr festes Kontingentlimit erreicht haben, müssen genügend Dateien oder Verzeichnisse löschen, um das Kontingentlimit zu unterschreiten, bevor sie wieder in das Dateisystem schreiben können. Wenn ein Kulanzzeitraum festgelegt ist, können Benutzer das Soft-Limit innerhalb des Kulanzzeitraums überschreiten, wenn das Hard-Limit unterschritten wird.

Für Soft-Limits konfigurieren Sie eine Kulanzzeit in Sekunden. Das Soft-Limit muss kleiner als das Hard-Limit sein.

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

Wenn Benutzer ein Soft-Limit überschreiten, FSx erlaubt Amazon ihnen, ihr Kontingent weiter zu überschreiten, bis die Karenzzeit abgelaufen ist oder bis das harte Limit erreicht ist. Nach Ablauf der Karenzzeit wird das weiche Limit in ein festes Limit umgewandelt, und Benutzer werden für weitere Schreibvorgänge gesperrt, bis ihre Speichernutzung wieder unter die definierten Block- oder Inode-Kontingentgrenzen fällt. Benutzer erhalten keine Benachrichtigung oder Warnung, wenn die Kulanzfrist beginnt.

Kontingente festlegen und anzeigen

Sie legen Speicherkontingente fest mit Lustre `lfs`Dateisystembefehle in Ihrem Linux-Terminal. Der `lfs setquota` Befehl legt Kontingentgrenzen fest und der `lfs quota` Befehl zeigt Kontingentinformationen an.

Weitere Informationen zur Lustre Quota-Befehle finden Sie im Lustre-Betriebshandbuch auf der Lustre Website zur Dokumentation.

Festlegung von Benutzer-, Gruppen- und Projektkontingenten

Die Syntax des `setquota` Befehls zum Festlegen von Benutzer-, Gruppen- oder Projektkontingenten lautet wie folgt.

```
lfs setquota {-u|--user|-g|--group|-p|--project} username|groupname|projectid
             [-b block_softlimit] [-B block_hardlimit]
             [-i inode_softlimit] [-I inode_hardlimit]
             /mount_point
```

Wobei gilt:

- `-u`oder `--user` gibt einen Benutzer an, für den ein Kontingent festgelegt werden soll.
- `-g`oder `--group` gibt eine Gruppe an, für die ein Kontingent festgelegt werden soll.
- `-p`oder `--project` gibt ein Projekt an, für das ein Kontingent festgelegt werden soll.

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

Beispiel für ein Benutzerkontingent: Mit dem folgenden Befehl wird ein Softblock-Limit von 5.000 KB, ein Hardblock-Limit von 8.000 KB, ein Soft-Inode-Limit von 2.000 KB und ein Hard-Inode-Limit von 3.000 KB für das Dateisystem festgelegt, `user1` auf das gemountet ist. `/mnt/fsx`

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

Beispiel für ein Gruppenkontingent: Mit dem folgenden Befehl wird ein Hardblock-Limit von 100.000 KB für die Gruppe festgelegt, die auf dem Dateisystem benannt ist, `group1` auf das gemountet wurde. `/mnt/fsx`

```
sudo lfs setquota -g group1 -B 100000 /mnt/fsx
```

Beispiel für ein Projektkontingent: Stellen Sie zunächst sicher, dass Sie den `project` Befehl verwendet haben, um die gewünschten Dateien und Verzeichnisse dem Projekt zuzuordnen. Mit dem folgenden Befehl werden beispielsweise alle Dateien und Unterverzeichnisse des `/mnt/fsxfs/dir1` Verzeichnisses dem Projekt zugeordnet, dessen Projekt-ID lautet`100`.

```
sudo lfs project -p 100 -r -s /mnt/fsxfs/dir1
```

Verwenden Sie dann den `setquota` Befehl, um das Projektkontingent festzulegen. Mit dem folgenden Befehl wird ein Softblock-Limit von 307.200 KB, ein Hardblock-Limit von 309.200 KB, ein Soft-Inode-Limit von 10.000 KB und ein Hard-Inode-Limit von 11.000 KB für das Projekt `250` auf dem Dateisystem festgelegt, auf das gemountet ist. `/mnt/fsx`

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

Kulanzfristen festlegen

Die Standard-Nachfrist beträgt eine Woche. Sie können den Standard-Kulanzzeitraum für Benutzer, Gruppen oder Projekte mithilfe der folgenden Syntax anpassen.

```
lfs setquota -t {-u|-g|-p}
             [-b block_grace]
             [-i inode_grace]
             /mount_point
```

Wobei gilt:

- `-t`gibt an, dass ein Kulanzzeitraum festgelegt wird.
- `-u`legt eine Übergangsfrist für alle Benutzer fest.
- `-g`legt eine Übergangsfrist für alle Gruppen fest.
- `-p`legt eine Übergangsfrist für alle Projekte fest.
- `-b`legt eine Übergangsfrist für Blockkontingente fest. `-i`legt eine Übergangsfrist für Inode-Kontingente fest. *`block_grace`*Sowohl als auch *`inode_grace`* werden in ganzzahligen Sekunden oder im `XXwXXdXXhXXmXXs` Format ausgedrückt.
- *`mount_point`*ist das Verzeichnis, in dem das Dateisystem eingehängt wurde.

Mit dem folgenden Befehl werden Übergangsfristen von 1.000 Sekunden für Benutzerblockkontingente und von 1 Woche und 4 Tagen für Benutzer-Inode-Kontingente festgelegt.

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

Kontingente anzeigen

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

Befehl „Quota anzeigen“	Kontingentinformationen werden angezeigt
`lfs quota /`*`mount_point`*	Allgemeine Kontingentinformationen (Festplattennutzung und Grenzwerte) für den Benutzer,

Befehl „Quota anzeigen“	Kontingentinformationen werden angezeigt
	der den Befehl ausführt, und für die primäre Gruppe des Benutzers.
`lfs quota -u username /mount_point`	Allgemeine Kontingentinformationen für einen bestimmten Benutzer. Benutzer mit AWS Root-Benutzeranmeldedaten können diesen Befehl für jeden Benutzer ausführen, Benutzer ohne Root-Rechte können diesen Befehl jedoch nicht ausführen, um Kontingentinformationen über andere Benutzer abzurufen.
`lfs quota -u username -v /mount_point`	Allgemeine Kontingentinformationen für einen bestimmten Benutzer und detaillierte Kontingentstatistiken für jedes Object Storage-Ziel (OST) und Metadatenziel (MDT). Benutzer mit AWS Root-Benutzeranmeldedaten können diesen Befehl für jeden Benutzer ausführen, Benutzer ohne Root-Rechte können diesen Befehl jedoch nicht ausführen, um Kontingentinformationen über andere Benutzer abzurufen.

Befehl „Quota anzeigen“	Kontingentinformationen werden angezeigt
`lfs quota -g groupname /mount_point`	Allgemeine Kontingentinformationen für eine bestimmte Gruppe.
`lfs quota -p projectid /mount_point`	Allgemeine Quoteninformationen für ein bestimmtes Projekt.
`lfs quota -t -u /mount_point`	Übergangszeiten für Benutzerkontingente beim Blockieren und Inoden.
`lfs quota -t -g /mount_point`	Block- und Inode-Übergangszeiten für Gruppenkontingente.
`lfs quota -t -p /mount_point`	Block- und Inode-Übergangszeiten für Projektkontingente.

Kontingente und mit Amazon S3 verknüpfte Buckets

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

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

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

Wenn ein Benutzer eine Datei `hsm_restore` verzögert oder verzögert lädt, wird die volle Größe der Datei auf das Blockkontingent angerechnet, das dem Eigentümer der Datei zugewiesen ist. Wenn Benutzer A beispielsweise eine Datei verzögert lädt, deren Eigentümer Benutzer B ist, werden der Speicherplatz und die Inode-Nutzung auf das Kontingent von Benutzer B angerechnet. Wenn ein Benutzer die FSx Amazon-API verwendet, um eine Datei freizugeben, werden die Daten ebenfalls von den Blockquoten des Benutzers oder der Gruppe befreit, der die Datei gehört.

Da HSM-Wiederherstellungen und verzögertes Laden mit Root-Zugriff ausgeführt werden, umgehen sie die Quotendurchsetzung. Sobald Daten importiert wurden, werden sie auf der Grundlage der in S3 festgelegten Eigentumsrechte dem Benutzer oder der Gruppe angerechnet, was dazu führen kann, dass Benutzer oder Gruppen ihre Blocklimits überschreiten. In diesem Fall müssen sie Dateien freigeben, um wieder in das Dateisystem schreiben zu können.

In ähnlicher Weise erstellen Dateisysteme mit aktiviertem automatischem Import automatisch neue Inodes für Objekte, die zu S3 hinzugefügt wurden. Diese neuen Inodes werden mit Root-Zugriff erstellt und umgehen die Einhaltung von Kontingenten, während sie erstellt werden. Diese neuen Inodes werden auf die Benutzer und Gruppen angerechnet, je nachdem, wem das Objekt in S3 gehört. Wenn diese Benutzer und Gruppen aufgrund der automatischen Importaktivität ihre Inode-Kontingente überschreiten, müssen sie Dateien löschen, um zusätzliche Kapazität freizugeben und ihre Kontingentgrenzen zu unterschreiten.

Kontingente und Wiederherstellung von Backups

Wenn Sie ein Backup wiederherstellen, werden die Kontingenteinstellungen des ursprünglichen Dateisystems im wiederhergestellten Dateisystem implementiert. Wenn beispielsweise Kontingente in Dateisystem A festgelegt sind und Dateisystem B aus einer Sicherung von Dateisystem A erstellt wird, werden die Kontingente von Dateisystem A in Dateisystem B durchgesetzt.

Verwaltung der Speicherkapazität

Sie können die SSD- oder HDD-Speicherkapazität erhöhen, die auf Ihrem FSx for Lustre-Dateisystem konfiguriert ist, wenn Sie zusätzlichen Speicherplatz und Durchsatz benötigen. Da der Durchsatz eines FSx for Lustre-Dateisystems linear mit der Speicherkapazität skaliert, erzielen Sie auch eine vergleichbare Steigerung der Durchsatzkapazität. Um die Speicherkapazität zu erhöhen, können Sie die FSx Amazon-Konsole, die AWS Command Line Interface (AWS CLI) oder die FSx Amazon-API verwenden.

Wenn Sie eine Aktualisierung der Speicherkapazität Ihres Dateisystems anfordern, fügt Amazon FSx automatisch neue Netzwerk-Dateiserver hinzu und skaliert Ihren Metadatenserver. Während

der Skalierung der Speicherkapazität ist das Dateisystem möglicherweise für einige Minuten nicht verfügbar. Dateioperationen, die von Clients ausgeführt werden, während das Dateisystem nicht verfügbar ist, werden auf transparente Weise wiederholt und sind schließlich erfolgreich, nachdem die Speicherskalierung abgeschlossen ist. Während der Zeit, in der das Dateisystem nicht verfügbar ist, wird der Dateisystemstatus auf gesetzt. `UPDATING` Sobald die Speicherskalierung abgeschlossen ist, wird der Dateisystemstatus auf gesetzt`AVAILABLE`.

Amazon führt FSx dann einen Speicheroptimierungsprozess durch, der die Daten auf transparente Weise auf die vorhandenen und neu hinzugefügten Dateiserver verteilt. Der Rebalancing wird im Hintergrund durchgeführt, ohne dass sich dies auf die Verfügbarkeit des Dateisystems auswirkt. Beim Rebalancing kann es zu einer verminderten Leistung des Dateisystems kommen, da Ressourcen für die Datenverschiebung verbraucht werden. Bei den meisten Dateisystemen dauert die Speicheroptimierung einige Stunden bis zu einigen Tagen. Während der Optimierungsphase können Sie auf Ihr Dateisystem zugreifen und es verwenden.

Sie können den Fortschritt der Speicheroptimierung jederzeit über die FSx Amazon-Konsole, CLI und API verfolgen. Weitere Informationen finden Sie unter Überwachung: Die Speicherkapazität steigt.

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.
- Inkremente erhöhen — Wenn Sie die Speicherkapazität erhöhen, verwenden Sie die im Dialogfeld Speicherkapazität erhöhen aufgeführten Stufen.
- Zeit zwischen Erhöhungen — Sie können die Speicherkapazität in einem Dateisystem erst 6 Stunden, nachdem die letzte Erhöhung angefordert wurde, weiter erhöhen.

- Durchsatzkapazität — Sie erhöhen automatisch die Durchsatzkapazität, wenn Sie die Speicherkapazität erhöhen. Bei persistenten HDD-Dateisystemen mit SSD-Cache wird die Lese-Cache-Speicherkapazität ebenfalls erhöht, um einen SSD-Cache aufrechtzuerhalten, der auf 20 Prozent der Festplattenspeicherkapazität ausgelegt ist. Amazon FSx berechnet die neuen Werte für die Lager- und Durchsatzkapazitätseinheiten und listet sie im Dialogfeld Speicherkapazität erhöhen auf.

  > **Note**
  >
  > Sie können die Durchsatzkapazität eines persistenten SSD-basierten Dateisystems unabhängig ändern, ohne die Speicherkapazität des Dateisystems aktualisieren zu müssen. Weitere Informationen finden Sie unter Verwaltung der bereitgestellten Durchsatzkapazität.

- Bereitstellungstyp — Sie können die Speicherkapazität aller Bereitstellungstypen mit Ausnahme von Scratch-1-Dateisystemen erhöhen.

Wann sollte die Speicherkapazität erhöht werden

Erhöhen Sie die Speicherkapazität Ihres Dateisystems, wenn die freie Speicherkapazität knapp wird. Verwenden Sie die `FreeStorageCapacity` CloudWatch Metrik, um die Menge an freiem Speicherplatz zu überwachen, der im Dateisystem verfügbar ist. Sie können einen CloudWatch Amazon-Alarm für diese Metrik erstellen und sich benachrichtigen lassen, wenn sie einen bestimmten Schwellenwert unterschreitet. Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch.

Sie können CloudWatch Metriken verwenden, um die laufende Durchsatznutzung Ihres Dateisystems zu überwachen. Wenn Sie feststellen, dass Ihr Dateisystem eine höhere Durchsatzkapazität benötigt, können Sie anhand der Metrikinformationen entscheiden, um wie viel die Speicherkapazität erhöht werden soll. Informationen darüber, wie Sie den aktuellen Durchsatz Ihres Dateisystems ermitteln können, finden Sie unterSo verwenden Sie Amazon FSx for Lustre-Metriken CloudWatch . Informationen darüber, wie sich die Speicherkapazität auf die Durchsatzkapazität auswirkt, finden Sie unterLeistung von Amazon FSx for Lustre.

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

Wie werden gleichzeitige Speicherskalierungs- und Backup-Anfragen behandelt

Sie können ein Backup anfordern, kurz bevor ein Speicherskalierungs-Workflow beginnt oder während dieser ausgeführt wird. Die Reihenfolge, in der Amazon die beiden Anfragen FSx bearbeitet, ist wie folgt:

- Wenn ein Speicherskalierungs-Workflow läuft (Speicherskalierungsstatus ist `IN_PROGRESS` und Dateisystemstatus ist`UPDATING`) und Sie ein Backup anfordern, wird die Backup-Anfrage in die Warteschlange gestellt. Die Backup-Aufgabe wird gestartet, wenn sich die Speicherskalierung in der Speicheroptimierungsphase befindet (der Speicherskalierungsstatus ist `UPDATED_OPTIMIZING` und der Dateisystemstatus ist`AVAILABLE`).
- Wenn das Backup gerade läuft (Backup-Status ist`CREATING`) und Sie eine Speicherskalierung anfordern, wird die Speicherskalierungsanforderung in die Warteschlange gestellt. Der Speicherskalierungs-Workflow wird gestartet, wenn Amazon FSx das Backup auf Amazon S3 überträgt (Backup-Status ist`TRANSFERRING`).

Wenn eine Speicherskalierungsanforderung aussteht und auch eine Dateisystem-Backup-Anfrage aussteht, hat die Backup-Aufgabe eine höhere Priorität. Die Speicherskalierungsaufgabe wird erst gestartet, wenn die Sicherungsaufgabe abgeschlossen ist.

Erhöhung der Speicherkapazität

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

Um die Speicherkapazität für ein Dateisystem (Konsole) zu erhöhen

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Navigieren Sie zu Dateisysteme und wählen Sie das Lustre Dateisystem aus, für das Sie die Speicherkapazität erhöhen möchten.
3. Wählen Sie unter Aktionen die Option Speicherkapazität aktualisieren aus. Oder wählen Sie im Übersichtsbereich neben der Speicherkapazität des Dateisystems die Option Aktualisieren aus, um das Dialogfeld „Speicherkapazität erhöhen“ anzuzeigen.
4. Geben Sie für Gewünschte Speicherkapazität eine neue Speicherkapazität in GiB an, die größer ist als die aktuelle Speicherkapazität des Dateisystems:

- Für ein persistentes SSD- oder Scratch-2-Dateisystem muss dieser Wert ein Vielfaches von 2400 GiB sein.
- Für ein persistentes HDD-Dateisystem muss dieser Wert ein Vielfaches von 6000 GiB für 12 MBps /TiB-Dateisysteme und ein Vielfaches von 1800 GiB für 40 MBps /TiB-Dateisysteme sein.
- Für ein EFA-fähiges Dateisystem muss dieser Wert ein Vielfaches von 38400 GiB für MBps 125-/TiB-Dateisysteme, ein Vielfaches von 19200 GiB für 250-/TiB-Dateisysteme, ein Vielfaches von 9600 MBps GiB für 500/TiB-Dateisysteme und ein Vielfaches von 4800 GiB für MBps 1000/TiB-Dateisysteme sein. MBps

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

5. Wählen Sie Update, um die Aktualisierung der Speicherkapazität zu starten.
6. Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme auf der Registerkarte Updates überwachen.

Um die Speicherkapazität für ein Dateisystem (CLI) zu erhöhen

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

   Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.

   Auf `--storage-capacity` einen ganzzahligen Wert gesetzt, der den Betrag der Erhöhung der Speicherkapazität in GiB angibt. Für ein persistentes SSD- oder Scratch-2-Dateisystem muss dieser Wert ein Vielfaches von 2400 sein. Für ein persistentes HDD-Dateisystem muss dieser Wert ein Vielfaches von 6000 für MBps 12-TiB-Dateisysteme und ein Vielfaches von 1800 für MBps 40-TiB-Dateisysteme sein. Der neue Zielwert muss größer als die aktuelle Speicherkapazität des Dateisystems sein.

   Dieser Befehl gibt einen Zielwert für die Speicherkapazität von 9600 GiB für ein persistentes SSD- oder Scratch-2-Dateisystem an.

   ```
   $ aws fsx update-file-system \
   ```

```
    --file-system-id fs-0123456789abcdef0 \
    --storage-capacity 9600
```

2. Sie können den Fortschritt des Updates mithilfe des AWS CLI Befehls describe-file-systemsüberwachen. Suchen Sie `administrative-actions` in der Ausgabe nach dem.

   Weitere Informationen finden Sie unter AdministrativeAction.

Überwachung: Die Speicherkapazität steigt

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

Überwachung von Zunahmen in der Konsole

Auf der Registerkarte Updates auf der Seite mit den Dateisystemdetails können Sie die 10 neuesten Updates für jeden Updatetyp einsehen.

Sie können die folgenden Informationen einsehen:

Art der Aktualisierung

Unterstützte Typen sind Speicherkapazität und Speicheroptimierung.

Zielwert

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

Status

Der aktuelle Status der Speicherkapazität wird aktualisiert. Die möglichen Werte lauten wie folgt:

- Ausstehend — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.
- In Bearbeitung — Amazon bearbeitet FSx die Aktualisierungsanfrage.
- Aktualisiert; Optimierung — Amazon FSx hat die Speicherkapazität des Dateisystems erhöht. Bei der Speicheroptimierung werden nun die Daten auf den Dateiservern neu verteilt.
- Abgeschlossen — Die Erhöhung der Speicherkapazität wurde erfolgreich abgeschlossen.
- Fehlgeschlagen — Die Erhöhung der Speicherkapazität ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Informationen darüber zu erhalten, warum das Speicherupdate fehlgeschlagen ist.

Fortschritt%

Zeigt den Fortschritt des Speicheroptimierungsprozesses in Prozent als abgeschlossen an.

Uhrzeit der Anfrage

Der Zeitpunkt, zu dem Amazon die Anfrage zur Aktualisierungsaktion FSx erhalten hat.

Die Überwachung nimmt mit der API AWS CLI und zu

Mithilfe des describe-file-systems AWS CLI Befehls und der DescribeFileSystemsAPI-Aktion können Sie Anfragen zur Erhöhung der Speicherkapazität des Dateisystems anzeigen und überwachen. Das `AdministrativeActions` Array listet die 10 letzten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die Speicherkapazität eines Dateisystems erhöhen, `AdministrativeActions` werden zwei generiert: eine Aktion `FILE_SYSTEM_UPDATE` und eine `STORAGE_OPTIMIZATION` Aktion.

Das folgende Beispiel zeigt einen Auszug der Antwort auf einen describe-file-systems CLI-Befehl. Das Dateisystem hat eine Speicherkapazität von 4800 GB, und eine Verwaltungsmaßnahme zur Erhöhung der Speicherkapazität auf 9600 GB steht noch aus.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 4800,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 9600
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "PENDING",
```

```
            }
        ]
```

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

Die `ProgressPercent` Eigenschaft zeigt den Fortschritt des Speicheroptimierungsprozesses an. Nachdem der Speicheroptimierungsprozess erfolgreich abgeschlossen wurde, ändert sich der Status der `FILE_SYSTEM_UPDATE` Aktion in`COMPLETED`, und die `STORAGE_OPTIMIZATION` Aktion wird nicht mehr angezeigt.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 9600,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 9600
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

Wenn die Erhöhung der Speicherkapazität fehlschlägt, ändert sich der Status der `FILE_SYSTEM_UPDATE` Aktion in`FAILED`. Die `FailureDetails` Eigenschaft enthält Informationen über den Fehler, wie im folgenden Beispiel dargestellt.

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

Verwaltung des bereitgestellten SSD-Lesecache

Wenn Sie ein Dateisystem mit der Intelligent-Tiering-Speicherklasse erstellen, haben Sie die Möglichkeit, auch einen SSD-basierten Lesecache bereitzustellen, der SSD-Latenzen für Lesevorgänge Ihrer häufig aufgerufenen Daten bietet, bis zu 3 IOPS pro GiB.

Sie können Ihren SSD-Lesecache für Daten, auf die häufig zugegriffen wird, mit einer der folgenden Optionen für den Größenmodus konfigurieren:

- Automatisch (proportional zur Durchsatzkapazität). Mit Automatisch wählt Amazon FSx for Lustre automatisch eine SSD-Datenlese-Cachegröße auf der Grundlage der bereitgestellten Durchsatzkapazität aus.
- Benutzerdefiniert (vom Benutzer bereitgestellt). Mit Benutzerdefiniert können Sie die Größe Ihres SSD-Lesecaches anpassen und ihn je nach den Anforderungen Ihres Workloads jederzeit nach oben oder unten skalieren.

- Wählen Sie Kein Cache, wenn Sie in Ihrem Dateisystem keinen SSD-Datenlese-Cache verwenden möchten.

Im Modus Automatisch (proportional zur Durchsatzkapazität) stellt Amazon FSx automatisch die folgende Standard-Lese-Cache-Größe bereit, die auf der Durchsatzkapazität Ihres Dateisystems basiert.

Bereitgestellte Durchsatzkapazität () MBps	SSD-Lesecache im automatischen Modus (proportional zur Durchsatzkapazität) (GiB)	Unterstützte SSD-Lesecache-Größe	
		mindestens (GiB)	maximal (GiB)
Alle 4000	20000	32	131072

Nachdem Ihr Dateisystem erstellt wurde, können Sie den Größenmodus und die Speicherkapazität Ihres Lesecaches jederzeit ändern.

Themen

Überlegungen bei der Aktualisierung des SSD-Lesecaches

Hier sind einige wichtige Überlegungen bei der Änderung Ihres SSD-Datenlesecaches:

- Jedes Mal, wenn Sie den SSD-Lesecache ändern, wird sein gesamter Inhalt gelöscht. Dies bedeutet, dass die Leistung möglicherweise abnimmt, bis der SSD-Lesecache wieder aufgefüllt ist.
- Sie können die Kapazität eines SSD-Lesecaches erhöhen oder verringern. Sie können dies jedoch nur einmal alle sechs Stunden tun. Es gibt keine zeitliche Beschränkung beim Hinzufügen oder Entfernen eines SSD-Lesecaches zu Ihrem Dateisystem.
- Sie müssen die Größe Ihres SSD-Lesecaches bei jeder Änderung um mindestens 10% erhöhen oder verringern.

Aktualisierung eines bereitgestellten SSD-Lesecaches

Sie können Ihren SSD-Datenlese-Cache mithilfe der FSx Amazon-Konsole AWS CLI, der oder der FSx Amazon-API aktualisieren.

Um den SSD-Lesecache für ein Intelligent-Tiering-Dateisystem (Konsole) zu aktualisieren

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich die Option Dateisysteme aus. Wählen Sie in der Liste Dateisysteme das FSx for Lustre-Dateisystem aus, für das Sie den SSD-Lesecache aktualisieren möchten.
3. SSD Wählen Sie im Übersichtsbereich neben dem SSD-Lesecache-Wert des Dateisystems die Option Aktualisieren aus.

   Das Dialogfeld „SSD-Lesecache aktualisieren“ wird angezeigt.

4. Wählen Sie den neuen Größenmodus, den Sie für Ihren Datenlesecache verwenden möchten, wie folgt aus:

   - Wählen Sie Automatisch (proportional zur Durchsatzkapazität), damit Ihr Datenlese-Cache automatisch an Ihre Durchsatzkapazität angepasst wird.
   - Wählen Sie Benutzerdefiniert (vom Benutzer bereitgestellt), wenn Sie die ungefähre Größe Ihres Datensatzes kennen und Ihren Datenlese-Cache anpassen möchten. Wenn Sie Benutzerdefiniert wählen, müssen Sie auch die gewünschte Lese-Cache-Kapazität in GiB angeben.
   - Wählen Sie Keine aus, wenn Sie keinen SSD-Datenlesecache mit Ihrem Intelligent-Tiering-Dateisystem verwenden möchten.

5. Wählen Sie Aktualisieren.

So aktualisieren Sie den SSD-Lesecache für ein Intelligent-Tiering-Dateisystem (CLI)

Verwenden Sie den AWS CLI Befehl update-file-systemoder die entsprechende API-Aktion, um den SSD-Datenlesecache für ein Intelligent-Tiering-Dateisystem zu aktualisieren. UpdateFileSystem Legen Sie die folgenden Parameter fest:

- Geben Sie `--file-system-id` die ID des Dateisystems ein, das Sie aktualisieren.
- Verwenden Sie die `--lustre-configuration DataReadCacheConfiguration` Eigenschaft, um Ihren SSD-Lesecache zu ändern. Diese Eigenschaft hat zwei Parameter `SizeGiB` und`SizingMode`:
  - SizeGiB - Legt die Größe Ihres SSD-Lesecaches in GiB fest, wenn Sie `USER_PROVISIONED` den Modus verwenden.
  - SizingMode- Legt den Größenmodus Ihres SSD-Lesecaches fest.
    - Stellen Sie diese `NO_CACHE` Option ein, wenn Sie keinen SSD-Lesecache mit Ihrem Intelligent-Tiering-Dateisystem verwenden möchten.
    - Stellen Sie auf ein`USER_PROVISIONED`, um die genaue Größe Ihres SSD-Lesecaches anzugeben.
    - Stellen Sie ein`PROPORTIONAL_TO_THROUGHPUT_CAPACITY`, dass Ihr SSD-Datenlese-Cache automatisch auf der Grundlage Ihrer Durchsatzkapazität dimensioniert wird.

Im folgenden Beispiel wird der SSD-Lesecache auf `USER_PROVISIONED` Modus aktualisiert und die Größe auf 524288 GiB festgelegt.

```
aws fsx update-file-system \
   --file-system-id fs-0123456789abcdef0 \
   --lustre-configuration
 'DataReadCacheConfiguration={SizeGiB=524288,SizingMode=USER_PROVISIONED}'
```

Verwenden Sie den Befehl, um den Fortschritt des Updates zu überwachen. describe-file-systems AWS CLI Suchen Sie in der Ausgabe nach dem `AdministrativeActions` Abschnitt.

Weitere Informationen finden Sie AdministrativeActionin der Amazon FSx API-Referenz.

Überwachung von SSD-Lese-Cache-Updates

Sie können den Fortschritt eines SSD-Lese-Cache-Updates mithilfe der FSx Amazon-Konsole, der API oder der überwachen AWS CLI.

Updates in der Konsole überwachen

Sie können Dateisystemupdates auf der Registerkarte Updates auf der Seite mit den Dateisystemdetails überwachen.

Für SSD-Lesecache-Updates können Sie die folgenden Informationen einsehen:

Art des Updates

Unterstützte Typen sind der SSD-Lesecache-Größenmodus und die SSD-Lesecache-Größe.

Zielwert

Der aktualisierte Wert für den SSD-Lesecache-Größenmodus oder die SSD-Lesecache-Größe des Dateisystems.

Status

Der aktuelle Status des Updates. Die möglichen Werte lauten wie folgt:

- Ausstehend — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.
- In Bearbeitung — Amazon bearbeitet FSx die Aktualisierungsanfrage.
- Abgeschlossen — Das Update wurde erfolgreich abgeschlossen.
- Fehlgeschlagen — Die Aktualisierungsanforderung ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Details darüber zu sehen, warum die Anfrage fehlgeschlagen ist.

Uhrzeit der Anfrage

Der Zeitpunkt, zu dem Amazon die Anfrage zur Aktualisierungsaktion FSx erhalten hat.

Überwachung von SSD-Lese-Cache-Updates mit der AWS CLI AND-API

Mithilfe des describe-file-systems AWS CLI Befehls und der DescribeFileSystemsAPI-Operation können Sie SSD-Lesecache-Aktualisierungsanforderungen des Dateisystems anzeigen und überwachen. Das `AdministrativeActions` Array listet die 10 neuesten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie den SSD-Lesecache eines Dateisystems aktualisieren, `FILE_SYSTEM_UPDATE` `AdministrativeActions` wird ein generiert.

Das folgende Beispiel zeigt einen Auszug der Antwort auf einen `describe-file-systems` CLI-Befehl. Im Dateisystem steht eine administrative Aktion zur Änderung des SSD-Lesecache-Größenmodus auf `USER_PROVISIONED` und der SSD-Lesecachegröße auf 524288 aus.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "LustreConfiguration": {
                "DataReadCacheConfiguration": {
                     "SizingMode": "USER_PROVISIONED"
                     "SizeGiB": 524288,
                }
            }
        }
    }
]
```

Wenn die neue SSD-Lesecache-Konfiguration für das Dateisystem verfügbar ist, ändert sich der `FILE_SYSTEM_UPDATE` Status in. `COMPLETED` Wenn die Aktualisierungsanforderung für den SSD-Lesecache fehlschlägt, ändert sich der Status der `FILE_SYSTEM_UPDATE` Aktion in`FAILED`.

Verwaltung der Metadaten-Performance

Sie können die Metadatenkonfiguration Ihres FSx for Lustre-Dateisystems aktualisieren, ohne dass Ihre Endbenutzer oder Anwendungen gestört werden, indem Sie die FSx Amazon-

Konsole, die FSx Amazon-API oder AWS Command Line Interface (AWS CLI) verwenden. Das Aktualisierungsverfahren erhöht die Anzahl der bereitgestellten Metadaten-IOPS für Ihr Dateisystem.

> **Note**
>
> Verbesserte Metadaten sind nur für 2.15-Dateisysteme verfügbar. Sie können die Leistung von Metadaten nur FSx für Lustre-Dateisysteme erhöhen, die mit dem Bereitstellungstyp Persistent 2 und einer angegebenen Metadatenkonfiguration erstellt wurden. Sie können die Metadatenkonfiguration für ein FSx for Lustre-Dateisystem nicht hinzufügen oder aktualisieren, wenn die Metadatenkonfiguration bei der Erstellung des Dateisystems nicht angegeben wurde. Dies gilt auch für Dateisysteme, die aus Backups von 2.12-Dateisystemen wiederhergestellt wurden, die keine verbesserte Metadaten-Performance unterstützten, oder aus 2.15-Dateisystemen, für die keine Metadatenkonfiguration angegeben war.

Die erhöhte Metadaten-Performance Ihres Dateisystems ist innerhalb weniger Minuten einsatzbereit. Sie können die Leistung der Metadaten jederzeit aktualisieren, sofern die Anfragen zur Steigerung der Metadatenleistung mindestens 6 Stunden auseinander liegen. Während der Skalierung der Metadatenleistung ist das Dateisystem möglicherweise für einige Minuten nicht verfügbar. Dateioperationen, die von Clients ausgeführt werden, während das Dateisystem nicht verfügbar ist, werden auf transparente Weise wiederholt und sind schließlich erfolgreich, wenn die Skalierung der Metadaten-Leistung abgeschlossen ist. Die Leistungssteigerung der neuen Metadaten wird Ihnen in Rechnung gestellt, sobald sie Ihnen zur Verfügung steht.

Sie können den Fortschritt einer Leistungssteigerung bei Metadaten jederzeit mithilfe der FSx Amazon-Konsole, CLI und API verfolgen. Weitere Informationen finden Sie unter Überwachung von Aktualisierungen der Metadaten-Konfiguration.

Themen

LustreKonfiguration der Metadaten-Leistung

Die Anzahl der bereitgestellten Metadaten-IOPS bestimmt die maximale Rate von Metadatenoperationen, die vom Dateisystem unterstützt werden können.

Wenn Sie das Dateisystem erstellen, wählen Sie einen Metadaten-Konfigurationsmodus:

- Für SSD-Dateisysteme können Sie den Modus Automatisch wählen, wenn Amazon FSx die Metadaten-IOPS auf Ihrem Dateisystem basierend auf der Speicherkapazität Ihres Dateisystems automatisch bereitstellen und skalieren soll. Beachten Sie, dass Intelligent-Tiering-Dateisysteme den automatischen Modus nicht unterstützen.
- Für SSD-Dateisysteme können Sie vom Benutzer bereitgestellt wählen, wenn Sie die Anzahl der Metadaten-IOPS angeben möchten, die für Ihr Dateisystem bereitgestellt werden sollen.
- Für Intelligent-Tiering-Dateisysteme müssen Sie den Modus Benutzerbereitgestellt wählen. Im vom Benutzer bereitgestellten Modus können Sie die Anzahl der Metadaten-IOPS angeben, die für Ihr Dateisystem bereitgestellt werden sollen.

Auf SSD-Dateisystemen können Sie jederzeit vom automatischen Modus in den vom Benutzer bereitgestellten Modus wechseln. Sie können auch vom Modus „Benutzerbereitgestellt“ in den Modus „Automatisch“ wechseln, wenn die Anzahl der auf Ihrem Dateisystem bereitgestellten Metadaten-IOPS der Standardanzahl der im automatischen Modus bereitgestellten Metadaten-IOPS entspricht. Intelligent-Tiering-Dateisysteme unterstützen nur den vom Benutzer bereitgestellten Modus, sodass Sie nicht zwischen den Konfigurationsmodi für Metadaten wechseln können.

Gültige IOPS-Werte für Metadaten lauten wie folgt:

- Für SSD-Dateisysteme sind gültige Metadaten-IOPS-Werte 1500, 3000, 6000 und Vielfache von 12000 bis zu einem Maximum von 192000 gültig.
- Für Intelligent-Tiering-Dateisysteme sind die gültigen Metadaten-IOPS-Werte 6000 und 12000 gültig.

Wenn die Metadaten-Performance Ihres Workloads die Anzahl der im automatischen Modus bereitgestellten Metadaten-IOPS übersteigt, können Sie den vom Benutzer bereitgestellten Modus verwenden, um den Metadaten-IOPS-Wert für Ihr Dateisystem zu erhöhen.

Sie können den aktuellen Wert der Metadatenserverkonfiguration des Dateisystems wie folgt anzeigen:

- Mithilfe der Konsole — Im Bereich Zusammenfassung der Seite mit den Dateisystemdetails werden im Feld Metadaten-IOPS der aktuelle Wert der bereitgestellten Metadaten-IOPS und der aktuelle Metadaten-Konfigurationsmodus des Dateisystems angezeigt.
- Verwenden der CLI oder API — Verwenden Sie den describe-file-systemsCLI-Befehl oder die DescribeFileSystemsAPI-Operation und suchen Sie nach der `MetadataConfiguration` Eigenschaft.

Überlegungen zur Steigerung der Metadaten-Performance

Im Folgenden sind einige wichtige Überlegungen zur Steigerung der Leistung Ihrer Metadaten aufgeführt:

- Nur Steigerung der Metadaten-Performance — Sie können nur die Anzahl der Metadaten-IOPS für ein Dateisystem erhöhen; Sie können die Anzahl der Metadaten-IOPS nicht verringern.
- Die Angabe von Metadaten-IOPS im Automatikmodus wird nicht unterstützt — Sie können die Anzahl der Metadaten-IOPS in einem Dateisystem, das sich im automatischen Modus befindet, nicht angeben. Sie müssen in den vom Benutzer bereitgestellten Modus wechseln und dann die Anfrage stellen. Weitere Informationen finden Sie unter Ändern des Metadaten-Konfigurationsmodus.
- Metadaten-IOPS für Daten, die vor der Skalierung geschrieben wurden — Wenn Metadaten-IOPS auf über 12000 skaliert werden, fügt FSx for Lustre Ihrem Dateisystem neue Metadatenserver hinzu. Neue Metadaten werden automatisch auf alle Server verteilt, um die Leistung zu verbessern. Vorhandene Metadaten und Unterverzeichnisse, die vor der Skalierung erstellt wurden, verbleiben jedoch auf den Originalservern, ohne dass sich die Metadaten-IOPS erhöhen.
- Zeit zwischen Erhöhungen — Sie können die Leistung von Metadaten in einem Dateisystem erst 6 Stunden, nachdem die letzte Erhöhung angefordert wurde, weiter erhöhen.
- Gleichzeitige Erhöhung der Metadatenleistung und Erhöhung des SSD-Speichers — Sie können die Metadatenleistung und die Speicherkapazität des Dateisystems nicht gleichzeitig skalieren.

Wann sollte die Leistung von Metadaten erhöht werden

Erhöhen Sie die Anzahl der Metadaten-IOPS, wenn Sie Workloads ausführen müssen, die eine höhere Metadaten-Performance erfordern als die, die standardmäßig in Ihrem Dateisystem bereitgestellt wird. Sie können die Leistung Ihrer Metadaten auf dem überwachen, AWS-Managementkonsole indem Sie das `Metadata IOPS Utilization` Diagramm verwenden,

das den Prozentsatz der Leistung des bereitgestellten Metadatenservers angibt, den Sie in Ihrem Dateisystem verbrauchen.

Sie können die Leistung Ihrer Metadaten auch anhand CloudWatch detaillierterer Messwerte überwachen. CloudWatch Zu den Metriken gehören `DiskRead0perations` und`DiskWrite0perations`, die das Volumen der Metadaten-Serveroperationen angeben, für die Festplatten-E/A erforderlich ist, sowie detaillierte Metriken für Metadatenvorgänge, einschließlich Datei- und Verzeichniserstellung, Statistiken, Lese- und Löschvorgänge. Weitere Informationen finden Sie unter FSx für Lustre-Metadatenmetriken.

Steigerung der Leistung von Metadaten

Sie können die Metadaten-Performance eines Dateisystems erhöhen, indem Sie die FSx Amazon-Konsole AWS CLI, die oder die FSx Amazon-API verwenden.

Um die Metadaten-Performance für ein Dateisystem (Konsole) zu erhöhen

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich die Option Dateisysteme aus. Wählen Sie in der Liste Dateisysteme das FSx for Lustre-Dateisystem aus, für das Sie die Metadaten-Performance erhöhen möchten.
3. Wählen Sie für Aktionen die Option Metadaten aktualisieren IOPS aus. Oder wählen Sie im Übersichtsbereich neben dem Feld Metadaten-IOPS des Dateisystems die Option Aktualisieren aus.

   Das Dialogfeld „Metadaten-IOPS aktualisieren“ wird angezeigt.
4. Wählen Sie Vom Benutzer bereitgestellt aus.
5. Wählen Sie für Desired Metadata IOPS den neuen Metadaten-IOPS-Wert aus. Der von Ihnen eingegebene Wert muss größer oder gleich dem aktuellen IOPS-Wert für Metadaten sein.

   - Für SSD-Dateisysteme sind die Werte`1500`,, `3000` `600012000`, und ein Vielfaches von `12000` bis zu einem Maximum von gültig. `192000`
   - Für Intelligent-Tiering-Dateisysteme sind die gültigen Werte und. `6000` `12000`
6. Wählen Sie Aktualisieren.

Um die Metadatenleistung für ein Dateisystem (CLI) zu erhöhen

Um die Metadaten-Performance für ein FSx for Lustre-Dateisystem zu erhöhen, verwenden Sie den AWS CLI Befehl update-file-system(UpdateFileSystem entspricht der API-Aktion). Legen Sie die folgenden Parameter fest:

- Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.
- Verwenden Sie die `--lustre-configuration MetadataConfiguration` Eigenschaft, um die Leistung Ihrer Metadaten zu erhöhen. Diese Eigenschaft hat zwei Parameter `Mode` und`Iops`.
  1. Wenn sich Ihr Dateisystem im Modus USER_PROVISIONED befindet, `Mode` ist die Verwendung optional (falls verwendet, auf gesetzt`Mode`). `USER_PROVISIONED`

     Wenn sich Ihr SSD-Dateisystem im AUTOMATIC-Modus befindet, legen Sie den Wert `Mode` auf fest `USER_PROVISIONED` (wodurch der Dateisystemmodus auf USER_PROVISIONED umgeschaltet wird und zusätzlich der IOPS-Wert für Metadaten erhöht wird).
  2. Legen Sie `Iops` für SSD-Dateisysteme einen Wert von`1500`,, `3000` `600012000`, oder ein Vielfaches von `12000` bis zu einem Maximum von fest. `192000` Legen Sie für Intelligent-Tiering-Dateisysteme den Wert auf oder fest. `Iops` `6000` `12000` Der eingegebene Wert muss größer oder gleich dem aktuellen IOPS-Wert für Metadaten sein.

Im folgenden Beispiel werden die bereitgestellten Metadaten-IOPS auf 12000 aktualisiert.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration 'MetadataConfiguration={Mode=USER_PROVISIONED,Iops=12000}'
```

Ändern des Metadaten-Konfigurationsmodus

Für SSD-basierte Dateisysteme können Sie den Metadaten-Konfigurationsmodus eines vorhandenen Dateisystems mithilfe der AWS Konsole und der CLI ändern, wie in den folgenden Verfahren erläutert.

Wenn Sie vom automatischen Modus in den vom Benutzer bereitgestellten Modus wechseln, müssen Sie einen Metadaten-IOPS-Wert angeben, der größer oder gleich dem aktuellen IOPS-Wert für Metadaten des Dateisystems ist.

Wenn Sie vom Modus „Benutzerbereitgestellt“ in den Modus „Automatisch“ wechseln möchten und der aktuelle Metadaten-IOPS-Wert höher als der automatisierte Standardwert ist, FSx lehnt

Amazon die Anfrage ab, da das Herunterskalieren von Metadaten-IOPS nicht unterstützt wird. Um die Blockierung des Moduswechsels aufzuheben, müssen Sie die Speicherkapazität so erhöhen, dass sie Ihren aktuellen Metadaten-IOPS im Automatikmodus entspricht, um den Moduswechsel wieder zu aktivieren.

Sie können den Metadaten-Konfigurationsmodus eines Dateisystems ändern, indem Sie die FSx Amazon-Konsole AWS CLI, die oder die FSx Amazon-API verwenden.

Um den Metadaten-Konfigurationsmodus für ein Dateisystem (Konsole) zu ändern

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im linken Navigationsbereich die Option Dateisysteme aus. Wählen Sie in der Liste Dateisysteme das FSx for Lustre-Dateisystem aus, für das Sie den Metadaten-Konfigurationsmodus ändern möchten.
3. Wählen Sie für Aktionen die Option Metadaten aktualisieren IOPS aus. Oder wählen Sie im Übersichtsbereich neben dem Feld Metadaten-IOPS des Dateisystems die Option Aktualisieren aus.

   Das Dialogfeld „Metadaten-IOPS aktualisieren“ wird angezeigt.
4. Führen Sie eine der folgenden Aufgaben aus.

   - Um vom vom Benutzer bereitgestellten Modus in den automatischen Modus zu wechseln, wählen Sie Automatisch.
   - Um vom automatischen Modus in den vom Benutzer bereitgestellten Modus zu wechseln, wählen Sie Benutzerbereitgestellt. Geben Sie dann für Desired Metadata IOPS einen Metadaten-IOPS-Wert an, der größer oder gleich dem aktuellen IOPS-Wert für Metadaten im Dateisystem ist.
5. Wählen Sie Aktualisieren.

So ändern Sie den Metadaten-Konfigurationsmodus für ein SSD-Dateisystem (CLI)

Um den Metadaten-Konfigurationsmodus für ein SSD FSx for Lustre-Dateisystem zu ändern, verwenden Sie den AWS CLI Befehl update-file-system(UpdateFileSystem entspricht der API-Aktion). Legen Sie die folgenden Parameter fest:

- Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.

- Verwenden Sie die Eigenschaft, um den Metadaten-Konfigurationsmodus auf SSD-basierten Dateisystemen zu ändern. `--lustre-configuration MetadataConfiguration` Diese Eigenschaft hat zwei Parameter und`Mode`. `Iops`
  - Um Ihr SSD-Dateisystem vom AUTOMATIC-Modus in den USER_PROVISIONED-Modus umzuschalten, legen Sie `Mode` einen Metadaten-IOPS-Wert fest, der größer oder gleich dem aktuellen IOPS-Wert für Metadaten des Dateisystems ist. `USER_PROVISIONED` `Iops` Zum Beispiel:

    ```
    aws fsx update-file-system \
        --file-system-id fs-0123456789abcdef0 \
        --lustre-configuration
     'MetadataConfiguration={Mode=USER_PROVISIONED,Iops=96000}'
    ```

  - Um vom Modus USER_PROVISIONED in den Modus AUTOMATIC zu wechseln, stellen Sie den Parameter auf ein und verwenden Sie `Mode` ihn nicht. `AUTOMATIC` `Iops` Zum Beispiel:

    ```
    aws fsx update-file-system \
        --file-system-id fs-0123456789abcdef0 \
        --lustre-configuration 'MetadataConfiguration={Mode=AUTOMATIC}'
    ```

Überwachung von Aktualisierungen der Metadaten-Konfiguration

Sie können den Fortschritt der Aktualisierungen der Metadaten-Konfiguration mithilfe der FSx Amazon-Konsole, der API oder der überwachen AWS CLI.

Überwachung der Aktualisierungen der Metadaten-Konfiguration (Konsole)

Sie können Aktualisierungen der Metadatenkonfiguration auf der Registerkarte Updates auf der Seite mit den Dateisystemdetails überwachen.

Für Aktualisierungen der Metadaten-Konfiguration können Sie die folgenden Informationen einsehen:

Art des Updates

Unterstützte Typen sind Metadaten-IOPS und Metadaten-Konfigurationsmodus.

Zielwert

Der aktualisierte Wert für den Metadaten-IOPS- oder Metadaten-Konfigurationsmodus des Dateisystems.

Status

Der aktuelle Status des Updates. Die möglichen Werte lauten wie folgt:

- Ausstehend — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.
- In Bearbeitung — Amazon bearbeitet FSx die Aktualisierungsanfrage.
- Abgeschlossen — Das Update wurde erfolgreich abgeschlossen.
- Fehlgeschlagen — Die Aktualisierungsanforderung ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Details darüber zu sehen, warum die Anfrage fehlgeschlagen ist.

Uhrzeit der Anfrage

Der Zeitpunkt, zu dem Amazon die Anfrage zur Aktualisierungsaktion FSx erhalten hat.

Überwachung von Metadaten-Konfigurationsupdates (CLI)

Sie können Anfragen zur Aktualisierung der Metadatenkonfiguration mithilfe des describe-file-systems AWS CLI Befehls und der DescribeFileSystemsAPI-Operation anzeigen und überwachen. Das `AdministrativeActions` Array listet die 10 neuesten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die Metadaten-Performance oder den Metadaten-Konfigurationsmodus eines Dateisystems aktualisieren, `FILE_SYSTEM_UPDATE` `AdministrativeActions` wird ein generiert.

Das folgende Beispiel zeigt einen Auszug der Antwort auf einen `describe-file-systems` CLI-Befehl. Im Dateisystem steht eine Verwaltungsaktion zur Erhöhung der Metadaten-IOPS auf 96000 und des Metadaten-Konfigurationsmodus auf USER_PROVISIONED aus.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1678840205.853,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "LustreConfiguration": {
                "MetadataConfiguration": {
                    "Iops": 96000,
                    "Mode": USER_PROVISIONED
                }
            }
```

```
        }
    }
]
```

Amazon FSx verarbeitet die `FILE_SYSTEM_UPDATE` Aktion und ändert die Metadaten-IOPS und den Metadaten-Konfigurationsmodus des Dateisystems. Wenn die neuen Metadatenressourcen für das Dateisystem verfügbar sind, ändert sich der `FILE_SYSTEM_UPDATE` Status in`COMPLETED`.

Wenn die Anforderung zur Aktualisierung der Metadatenkonfiguration fehlschlägt, ändert sich der Status der `FILE_SYSTEM_UPDATE` Aktion auf`FAILED`, wie im folgenden Beispiel gezeigt. Die `FailureDetails` Eigenschaft stellt Informationen über den Fehler bereit.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1678840205.853,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "LustreConfiguration": {
                "MetadataConfiguration": {
                    "Iops": 96000,
                    "Mode": USER_PROVISIONED
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

Verwaltung der bereitgestellten Durchsatzkapazität

Jedes FSx for Lustre-Dateisystem hat eine Durchsatzkapazität, die bei der Erstellung des Dateisystems konfiguriert wird. Bei Dateisystemen, die SSD- oder HDD-Speicher verwenden, wird die Durchsatzkapazität in Megabyte pro Sekunde pro Tebibyte (MBps/TiB). For file systems using Intelligent-Tiering storage, the throughput capacity is measured in megabytes per second (MBps) for the file system. Throughput capacity is one factor that determines the speed at which the file server hosting the file system can serve file data. Higher levels of throughput capacity also come with higher levels of I/OOperationen pro Sekunde (IOPS)) und mehr Speicher für das Zwischenspeichern von

Daten auf dem Dateiserver gemessen. Weitere Informationen finden Sie unter Leistung von Amazon FSx for Lustre.

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

- Für Bereitstellungstypen auf der Basis von Persistent 1 SSD sind die gültigen Werte 50, 100 und 200 /TiB. MBps
- Für Bereitstellungstypen auf Basis von Persistent 2 SSD sind die gültigen Werte 125, 250, 500 und 1000 /TiB. MBps

Sie können die Durchsatzkapazität eines Intelligent-Tiering-Dateisystems ändern, indem Sie den Wert der Gesamtdurchsatzkapazität für das Dateisystem erhöhen. Gültige Werte sind 4.000 MBps oder Stufen von 4.000 MBps bis zu einem Höchstwert von 2.000.000. MBps

Sie können den aktuellen Wert der Durchsatzkapazität des Dateisystems wie folgt anzeigen:

- Mithilfe der Konsole — Im Bereich Zusammenfassung der Dateisystemdetailseite zeigt das Feld Durchsatz pro Speichereinheit den aktuellen Wert für SSD-basierte Dateisysteme, während das Feld Durchsatzkapazität den aktuellen Wert für Intelligent-Tiering-Dateisysteme anzeigt.
- Verwenden der CLI oder API — Verwenden Sie den describe-file-systemsCLI-Befehl oder die DescribeFileSystemsAPI-Operation und suchen Sie nach der `PerUnitStorageThroughput` Eigenschaft.

Wenn Sie die Durchsatzkapazität Ihres Dateisystems ändern, FSx schaltet Amazon hinter den Kulissen die Dateiserver des Dateisystems auf SSD-Dateisystemen aus oder fügt neue Dateiserver auf Intelligent-Tiering-Dateisystemen hinzu. Ihr Dateisystem wird während der Skalierung der Durchsatzkapazität für einige Minuten nicht verfügbar sein. Die neue Menge an Durchsatzkapazität wird Ihnen in Rechnung gestellt, sobald sie für Ihr Dateisystem verfügbar ist.

Themen

Überlegungen zur Aktualisierung der Durchsatzkapazität

Hier sind einige wichtige Punkte, die Sie bei der Aktualisierung der Durchsatzkapazität berücksichtigen sollten:

- Erhöhen oder verringern — Sie können die Durchsatzkapazität für ein SSD-basiertes Dateisystem erhöhen oder verringern. Sie können die Durchsatzkapazität nur für ein Intelligent-Tiering-Dateisystem erhöhen.
- Inkremente aktualisieren — Wenn Sie die Durchsatzkapazität ändern, verwenden Sie die Inkremente, die im Dialogfeld Durchsatzstufe aktualisieren für SSD-basierte Dateisysteme oder im Dialogfeld Durchsatzkapazität aktualisieren für Intelligent-Tiering-Dateisysteme aufgeführt sind.
- Zeit zwischen Erhöhungen — Weitere Änderungen der Durchsatzkapazität in einem Dateisystem können Sie erst 6 Stunden nach der letzten Anforderung oder bis zum Abschluss der Durchsatzoptimierung vornehmen, je nachdem, welcher Zeitraum länger ist.
- Automatische Skalierung des SSD-Lesecaches — Für den SSD-Lesecache-Standardmodus (proportional zur Durchsatzkapazität) FSx stellt Amazon automatisch 5 GiB Datenspeicher für jede MBps von Ihnen bereitgestellte Durchsatzkapazität bereit. Wenn Sie die Durchsatzkapazität Ihres Dateisystems skalieren, skaliert Amazon FSx automatisch Ihren SSD-Datencache, indem es zusätzlichen Cache-Speicher an alle neu hinzugefügten Dateiserver anhängt.
- Bereitstellungstyp — Sie können die Durchsatzkapazität nur bei Bereitstellungstypen aktualisieren, die auf persistenten SSDs oder Intelligent-Tiering basieren. Sie können die Durchsatzkapazität von EFA-fähigen SSD-basierten Dateisystemen nicht ändern.

Wann muss die Durchsatzkapazität geändert werden

Amazon ist in Amazon FSx integriert CloudWatch, sodass Sie die laufende Durchsatznutzung Ihres Dateisystems überwachen können. Die Leistung (Durchsatz und IOPS), die Sie über Ihr Dateisystem erzielen können, hängt von den Eigenschaften Ihres spezifischen Workloads sowie von der Durchsatzkapazität, Speicherkapazität und Speicherklasse Ihres Dateisystems ab. Informationen darüber, wie Sie den aktuellen Durchsatz Ihres Dateisystems ermitteln können, finden Sie unterSo verwenden Sie Amazon FSx for Lustre-Metriken CloudWatch . Informationen zu CloudWatch Metriken finden Sie unterÜberwachung mit Amazon CloudWatch.

Änderung der Durchsatzkapazität

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

Um die Durchsatzkapazität eines SSD-Dateisystems zu ändern (Konsole)

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Navigieren Sie zu Dateisysteme und wählen Sie das FSx for Lustre-Dateisystem aus, für das Sie die Durchsatzkapazität ändern möchten.
3. Wählen Sie für Aktionen die Option Durchsatzstufe aktualisieren aus. Oder wählen Sie im Bereich „Zusammenfassung“ neben „Durchsatz pro Speichereinheit“ des Dateisystems die Option „Aktualisieren“ aus.

   Das Fenster „Durchsatzstufe aktualisieren“ wird angezeigt.
4. Wählen Sie den neuen Wert für Gewünschter Durchsatz pro Speichereinheit aus der Liste aus.
5. Wählen Sie „Aktualisieren“, um die Aktualisierung der Durchsatzkapazität zu starten.

> **Note**
>
> Ihr Dateisystem kann während des Updates für einen sehr kurzen Zeitraum nicht verfügbar sein.

So ändern Sie die Durchsatzkapazität (CLI) eines SSD-Dateisystems

- Verwenden Sie den update-file-systemCLI-Befehl (oder die entsprechende UpdateFileSystemAPI-Operation), um die Durchsatzkapazität eines Dateisystems zu ändern. Legen Sie die folgenden Parameter fest:
  - Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.
  - Legen Sie `--lustre-configuration PerUnitStorageThroughput` den Wert auf `50100`, oder `200` MBps/TiB für Persistent 1-SSD-Dateisysteme oder auf einen Wert von`125`, `250500`, oder `1000` MBps/TiB für Persistent 2-SSD-Dateisysteme fest.

  Dieser Befehl gibt an, dass die Durchsatzkapazität für das Dateisystem auf 1000 MBps /TiB festgelegt wird.

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

Um die Durchsatzkapazität eines Intelligent-Tiering-Dateisystems zu ändern (Konsole)

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Navigieren Sie zu Dateisysteme und wählen Sie das FSx for Lustre-Dateisystem aus, für das Sie die Durchsatzkapazität ändern möchten.
3. Wählen Sie für Aktionen die Option Durchsatzkapazität aktualisieren aus. Oder wählen Sie im Übersichtsbereich neben der Durchsatzkapazität des Dateisystems die Option Aktualisieren aus.

   Das Dialogfeld „Durchsatzkapazität aktualisieren“ wird angezeigt.
4. Wählen Sie den neuen Wert für Gewünschte Durchsatzkapazität aus der Liste aus.

   Amazon skaliert Ihren Datenlese-Cache automatisch, um zu vermeiden, dass der Cache-Inhalt gelöscht FSx wird.
5. Wählen Sie Update, um die Aktualisierung der Durchsatzkapazität zu starten.

> **Note**
>
> Ihr Dateisystem kann während des Updates für einen sehr kurzen Zeitraum nicht verfügbar sein.

So ändern Sie die Durchsatzkapazität (CLI) eines Intelligent-Tiering-Dateisystems

- Verwenden Sie den update-file-systemCLI-Befehl (oder die entsprechende UpdateFileSystemAPI-Operation), um die Durchsatzkapazität eines Dateisystems zu ändern. Legen Sie die folgenden Parameter fest:
  - Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.
  - Wenn Ihr Datenlese-Cache proportional zum Durchsatzkapazitätsmodus konfiguriert ist, legen Sie `--lustre-configuration ThroughputCapacity` einen Durchsatz in Schritten von `4000` MBps bis zu einem Maximum von `2000000` MBps fest.

    Wenn Ihr Datenlese-Cache im vom Benutzer bereitgestellten Modus konfiguriert ist, müssen Sie die `--lustre-configuration DataReadCacheConfiguration` Eigenschaft auch verwenden, um den Datenlese-Cache anzugeben. Sie müssen das gleiche Verhältnis von Cache-Speicher pro Server beibehalten und das neue SizeGi B angeben, andernfalls wird die Anfrage abgelehnt.

Dieser Befehl gibt an, dass die Durchsatzkapazität MBps für ein Dateisystem, das einen Lesecache verwendet, der proportional zum Durchsatzkapazitätsmodus konfiguriert ist, auf 8000 festgelegt wird.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration '{
      "ThroughputCapacity": 8000
      }'
```

Dieser Befehl gibt an, dass die Durchsatzkapazität MBps für ein Dateisystem, das einen im vom Benutzer bereitgestellten Modus konfigurierten Lesecache verwendet, auf 8000 festgelegt wird.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration {
        "ThroughputCapacity": 8000,
        "DataReadCacheConfiguration": '{
             "SizingMode":"USER_PROVISIONED"
             "SizeGiB":1000
             # New size should be cache storage allocated per server multiplied by
 number of file servers
         }
}'
```

Überwachung von Änderungen der Durchsatzkapazität

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

Überwachung von Änderungen der Durchsatzkapazität (Konsole)

- Auf der Registerkarte Updates auf der Seite mit den Dateisystemdetails können Sie die 10 neuesten Aktualisierungsaktionen für jeden Aktualisierungsaktionstyp anzeigen.

  Zu den Aktionen zur Aktualisierung der Durchsatzkapazität können Sie sich die folgenden Informationen ansehen.

Art der Aktualisierung

Der unterstützte Typ ist Speicherdurchsatz pro Einheit.

Zielwert

Der gewünschte Wert, auf den der Durchsatz des Dateisystems pro Speichereinheit geändert werden soll.

Status

Der aktuelle Status des Updates. Für Aktualisierungen der Durchsatzkapazität sind die folgenden Werte möglich:

- Ausstehend — Amazon FSx hat die Aktualisierungsanfrage erhalten, aber noch nicht mit der Bearbeitung begonnen.
- In Bearbeitung — Amazon bearbeitet FSx die Aktualisierungsanfrage.
- Aktualisiert; Optimierung — Amazon FSx hat die I/O, CPU, and memory resources. The new disk I/O performance level is available for write operations. Your read operations will see disk I/O Netzwerkleistung des Dateisystems zwischen der vorherigen und der neuen Stufe aktualisiert, bis sich Ihr Dateisystem nicht mehr in diesem Zustand befindet.
- Abgeschlossen — Die Aktualisierung der Durchsatzkapazität wurde erfolgreich abgeschlossen.
- Fehlgeschlagen — Die Aktualisierung der Durchsatzkapazität ist fehlgeschlagen. Wählen Sie das Fragezeichen (?), um Einzelheiten darüber zu erhalten, warum die Durchsatzaktualisierung fehlgeschlagen ist.

Uhrzeit der Anfrage

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

Überwachung von Dateisystem-Updates (CLI)

- Sie können Anfragen zur Änderung der Kapazität des Dateisystemdurchsatzes mithilfe des describe-file-systemsCLI-Befehls und der DescribeFileSystemsAPI-Aktion anzeigen und überwachen. Das `AdministrativeActions` Array listet die 10 neuesten Aktualisierungsaktionen für jeden administrativen Aktionstyp auf. Wenn Sie die Durchsatzkapazität eines Dateisystems ändern, wird eine `FILE_SYSTEM_UPDATE` Verwaltungsaktion generiert.

Das folgende Beispiel zeigt den Antwortausschnitt eines `describe-file-systems` CLI-Befehls. Das Dateisystem hat einen Zieldurchsatz pro Speichereinheit von 500 MBps /TiB.

```
.
.
.
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "LustreConfiguration": {
            "PerUnitStorageThroughput": 500
          }
        }
    }
]
```

Wenn Amazon die Aktion erfolgreich FSx verarbeitet hat, 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.

LustreDatenkomprimierung

Sie können die Lustre Datenkomprimierungsfunktion verwenden, um Kosteneinsparungen bei Ihren leistungsstarken Amazon FSx for Lustre-Dateisystemen und Backup-Speichern zu erzielen. Wenn die Datenkomprimierung aktiviert ist, komprimiert Amazon FSx for Lustre neu geschriebene Dateien automatisch, bevor sie auf die Festplatte geschrieben werden, und dekomprimiert sie automatisch, wenn sie gelesen werden.

Die Datenkomprimierung verwendet den LZ4 Algorithmus, der für ein hohes Maß an Komprimierung optimiert ist, ohne die Leistung des Dateisystems zu beeinträchtigen. LZ4 ist ein von der Lustre Community anerkannter und leistungsorientierter Algorithmus, der für ein ausgewogenes Verhältnis zwischen Komprimierungsgeschwindigkeit und komprimierter Dateigröße sorgt. Die Aktivierung der Datenkomprimierung hat in der Regel keine messbaren Auswirkungen auf die Latenz.

Die Datenkomprimierung reduziert die Datenmenge, die zwischen Amazon FSx for Lustre-Dateiservern und Speicher übertragen wird. Wenn Sie noch keine komprimierten Dateiformate verwenden, werden Sie bei Verwendung der Datenkomprimierung einen Anstieg der Gesamtdurchsatzkapazität des Dateisystems feststellen. Erhöhungen der Durchsatzkapazität im Zusammenhang mit der Datenkomprimierung werden begrenzt, wenn Sie Ihre Front-End-Netzwerkschnittstellenkarten voll ausgelastet haben.

Wenn es sich bei Ihrem Dateisystem beispielsweise um einen PERSISTENT-50-SSD-Bereitstellungstyp handelt, hat Ihr Netzwerkdurchsatz einen Basiswert von 250 MBps pro TiB Speicher. Ihr Festplattendurchsatz hat einen Basiswert von 50 MBps pro TiB. Mit der Datenkomprimierung könnte Ihr Festplattendurchsatz von 50 MBps pro TiB auf maximal 250 MBps pro TiB steigen, was der Basisgrenzwert für den Netzwerkdurchsatz ist. Weitere Informationen zu den Netzwerk- und Festplattendurchsatzgrenzen finden Sie in den Leistungstabellen für Dateisysteme unter. Leistungsmerkmale der SSD- und HDD-Speicherklassen Weitere Informationen zur Leistung bei der Datenkomprimierung finden Sie im Beitrag Weniger ausgeben und gleichzeitig die Leistung durch Amazon FSx for Lustre Datenkomprimierung erhöhen im AWS Speicher-Blog.

Themen

- Verwaltung der Datenkomprimierung
- Komprimieren zuvor geschriebener Dateien
- Dateigrößen anzeigen
- Verwenden von Metriken CloudWatch

Verwaltung der Datenkomprimierung

Sie können die Datenkomprimierung ein- oder ausschalten, wenn Sie ein neues Amazon FSx for Lustre-Dateisystem erstellen. Die Datenkomprimierung ist standardmäßig deaktiviert, wenn Sie ein Amazon FSx for Lustre-Dateisystem über die Konsole oder API erstellen. AWS CLI

Um die Datenkomprimierung beim Erstellen eines Dateisystems (Konsole) zu aktivieren

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, das Schritt 1: Erstellen Sie Ihr FSx for Lustre-Dateisystem im Abschnitt Erste Schritte beschrieben ist.
3. Wählen Sie im Abschnitt Dateisystemdetails für Datenkomprimierungstyp die Option LZ4.

4. Führen Sie den Assistenten genauso aus, wie Sie es beim Erstellen eines neuen Dateisystems tun.
5. Wählen Sie Review and create.
6. Überprüfen Sie die Einstellungen, die Sie für Ihr Amazon FSx for Lustre-Dateisystem ausgewählt haben, und wählen Sie dann Dateisystem erstellen.

Wenn das Dateisystem verfügbar ist, ist die Datenkomprimierung aktiviert.

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

- Um ein FSx for Lustre-Dateisystem mit aktivierter Datenkomprimierung zu erstellen, verwenden Sie den Amazon FSx CLI-Befehl `create-file-system`mit dem `DataCompressionType` Parameter, wie unten gezeigt. Die entsprechende API-Operation ist CreateFileSystem.

```
$ aws fsx create-file-system \
      --client-request-token CRT1234 \
      --file-system-type LUSTRE \
      --file-system-type-version 2.12 \
      --lustre-configuration
 DeploymentType=PERSISTENT_1,PerUnitStorageThroughput=50,DataCompressionType=LZ4 \
      --storage-capacity 3600 \
      --subnet-ids subnet-123456 \
      --tags Key=Name,Value=Lustre-TEST-1 \
      --region us-east-2
```

Nach erfolgreicher Erstellung des Dateisystems FSx gibt Amazon die Dateisystembeschreibung als JSON zurück, wie im folgenden Beispiel gezeigt.

```
{

    "FileSystems": [
        {
            "OwnerId": "111122223333",
            "CreationTime": 1549310341.483,
            "FileSystemId": "fs-0123456789abcdef0",
            "FileSystemType": "LUSTRE",
            "FileSystemTypeVersion": "2.12",
            "Lifecycle": "CREATING",
            "StorageCapacity": 3600,
```

```
            "VpcId": "vpc-123456",
            "SubnetIds": [
                "subnet-123456"
            ],
            "NetworkInterfaceIds": [
                "eni-039fcf55123456789"
            ],
            "DNSName": "fs-0123456789abcdef0.fsx.us-east-2.amazonaws.com",
            "ResourceARN": "arn:aws:fsx:us-east-2:123456:file-system/
fs-0123456789abcdef0",
            "Tags": [
                {
                    "Key": "Name",
                    "Value": "Lustre-TEST-1"
                }
            ],
            "LustreConfiguration": {
                "DeploymentType": "PERSISTENT_1",
                "DataCompressionType": "LZ4",
                "PerUnitStorageThroughput": 50
            }
        }
    ]
}
```

Sie können auch die Datenkomprimierungskonfiguration Ihrer vorhandenen Dateisysteme ändern. Wenn Sie die Datenkomprimierung für ein vorhandenes Dateisystem aktivieren, werden nur neu geschriebene Dateien komprimiert und vorhandene Dateien werden nicht komprimiert. Weitere Informationen finden Sie unter Komprimieren zuvor geschriebener Dateien.

Um die Datenkomprimierung auf einem vorhandenen Dateisystem (Konsole) zu aktualisieren

1. Öffnen Sie die FSx Amazon-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 unter Aktionen die Option Datenkomprimierungstyp aktualisieren aus.
4. Wählen Sie im Dialogfeld Datenkomprimierungstyp aktualisieren aus, ob LZ4die Datenkomprimierung aktiviert werden soll, oder wählen Sie KEINE, um sie zu deaktivieren.
5. Wählen Sie Aktualisieren.

6. Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme auf der Registerkarte Updates überwachen.

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

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

- Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.
- Legt fest`--lustre-configuration DataCompressionType`, `NONE` ob die Datenkomprimierung ausgeschaltet oder `LZ4` die Datenkomprimierung mit dem LZ4 Algorithmus aktiviert werden soll.

Dieser Befehl gibt an, dass die Datenkomprimierung mit dem LZ4 Algorithmus aktiviert ist.

```
$ aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration DataCompressionType=LZ4
```

Konfiguration der Datenkomprimierung beim Erstellen eines Dateisystems aus einer Sicherungskopie

Sie können ein verfügbares Backup verwenden, um ein neues Amazon FSx for Lustre-Dateisystem zu erstellen. Wenn Sie aus einer Sicherungskopie ein neues Dateisystem erstellen, müssen Sie das `DataCompressionType` nicht angeben. Die Einstellung wird anhand der `DataCompressionType` Backup-Einstellung angewendet. Wenn Sie `DataCompressionType` bei der Erstellung aus einer Sicherungskopie die angeben, muss der Wert mit der `DataCompressionType` Einstellung der Sicherung übereinstimmen.

Um die Einstellungen eines Backups einzusehen, wählen Sie es auf der Registerkarte Backups der FSx Amazon-Konsole aus. Die Details des Backups werden auf der Übersichtsseite des Backups aufgeführt. Sie können den `describe-backups` AWS CLI Befehl auch ausführen (die entsprechende API-Aktion ist `DescribeBackups`).

Komprimieren zuvor geschriebener Dateien

Dateien sind unkomprimiert, wenn sie erstellt wurden, als die Datenkomprimierung im Amazon FSx for Lustre-Dateisystem ausgeschaltet war. Wenn Sie die Datenkomprimierung aktivieren, werden Ihre vorhandenen unkomprimierten Daten nicht automatisch komprimiert.

Sie können den `lfs_migrate` Befehl verwenden, der als Teil der Lustre Client-Installation installiert ist, um vorhandene Dateien zu komprimieren. Ein Beispiel finden Sie unter FSxL-Compression, verfügbar unter GitHub.

Dateigrößen anzeigen

Sie können die folgenden Befehle verwenden, um die unkomprimierten und komprimierten Größen Ihrer Dateien und Verzeichnisse anzuzeigen.

- `du` zeigt komprimierte Größen an.
- `du --apparent-size` zeigt unkomprimierte Größen an.
- `ls -l` zeigt unkomprimierte Größen an.

Die folgenden Beispiele zeigen die Ausgabe der einzelnen Befehle mit derselben Datei.

```
$ du -sh samplefile
272M samplefile
$ du -sh --apparent-size samplefile
1.0G samplefile
$ ls -lh samplefile
-rw-r--r-- 1 root root 1.0G May 10 21:16 samplefile
```

Die `-h` Option ist für diese Befehle nützlich, da sie Größen in einem für Menschen lesbaren Format ausgibt.

Verwenden von Metriken CloudWatch

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

Sie können das Komprimierungsverhältnis Ihres Dateisystems ermitteln, indem Sie den Wert `Sum` der `LogicalDiskUsage` Statistik durch den Wert `Sum` der `PhysicalDiskUsage` Statistik dividieren.

Weitere Informationen zur Überwachung der Leistung Ihres Dateisystems finden Sie unter. Überwachung von Amazon FSx for Lustre-Dateisystemen

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 FSx für Lustre-Dateisysteme. 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
- Wurzelkürbis verwalten

Wie funktioniert Root Squash

Die Root-Squash-Funktion funktioniert, indem sie die Benutzer-ID (UID) und Gruppen-ID (GID) des Root-Benutzers einer UID und GID neu zuordnet, die von Lustre Systemadministrator. Mit der Root-Squash-Funktion können Sie optional auch eine Gruppe von Clients angeben, für die eine UID/GID-Neuzuweisung nicht gilt.

Wenn Sie ein neues Dateisystem FSx für Lustre erstellen, ist Root-Squash standardmäßig deaktiviert. Sie aktivieren Root-Squash, indem Sie eine UID- und GID-Root-Squash-Einstellung für Ihr for Lustre-Dateisystem konfigurieren. FSx 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 FSx Amazon-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 NIDs von Clients angeben, für die Root Squash nicht gilt. Eine Client-NID ist ein 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 beschrieben Lustre NID-Format durch Angabe der IP-Adresse des Clients gefolgt von Lustre Netzwerk-ID (zum Beispiel`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 keinen Client angeben NIDs, gibt es keine Ausnahmen für Root Squash.

Wenn Sie Ihr Dateisystem erstellen oder aktualisieren, können Sie die Eigenschaft Exceptions to Root Squash in der FSx Amazon-Konsole verwenden, um die Liste der Clients NIDs bereitzustellen. Verwenden Sie in der API AWS CLI oder den `NoSquashNids` Parameter. Weitere Informationen finden Sie in den Verfahren unterWurzelkürbis verwalten.

Wurzelkürbis 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 FSx Amazon-Konsole oder API AWS CLI erstellen.

Um Root Squash beim Erstellen eines Dateisystems (Konsole) zu aktivieren

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Folgen Sie dem Verfahren zum Erstellen eines neuen Dateisystems, das Schritt 1: 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 den Benutzer und die Gruppe an, IDs 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 wie beim Erstellen eines neuen Dateisystems aus.
7. Wählen Sie Review and create.
8. Überprüfen Sie die Einstellungen, die Sie für Ihr Amazon FSx for Lustre-Dateisystem ausgewählt haben, und wählen Sie dann Dateisystem erstellen.

Wenn das Dateisystem verfügbar ist, ist Root-Squash aktiviert.

So aktivieren Sie Root Squash beim Erstellen eines Dateisystems (CLI)

- Um ein FSx for Lustre-Dateisystem mit aktiviertem Root-Squash zu erstellen, verwenden Sie den Amazon FSx CLI-Befehl `create-file-system`mit dem `RootSquashConfiguration` Parameter. 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, für die Root Squash nicht gilt. Informationen zum Client-NID-Format finden Sie unter. Wie funktioniert Root Squash

Im folgenden Beispiel wird ein FSx for Lustre-Dateisystem mit aktiviertem Root-Squash erstellt:

```
$ 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 FSx gibt Amazon 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 FSx Amazon-Konsole oder API aktualisieren. AWS CLI Sie können beispielsweise die Root-Squash-UID- und GID-Werte ändern, Clients hinzufügen oder entfernen oder Root-Squash NIDs deaktivieren.

Um die Root-Squash-Einstellungen auf einem vorhandenen Dateisystem (Konsole) zu aktualisieren

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Navigieren Sie zu Dateisysteme und wählen Sie Lustre Dateisystem, 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 den Benutzer und die Gruppe, IDs mit denen der Root-Benutzer auf das Dateisystem zugreifen kann. Sie können eine beliebige ganze Zahl im Bereich von `0` — `4294967294` angeben. Um Root Squash zu deaktivieren, geben Sie `0` (Null) für beide IDs an.

    1. Geben Sie unter Benutzer-ID die Benutzer-ID an, die der Root-Benutzer verwenden soll.

2. Geben Sie unter Gruppen-ID die Gruppen-ID an, die der Root-Benutzer verwenden soll.

5. Gehen Sie für Ausnahmen von Root Squash wie folgt vor:

   1. Wählen Sie Kundenadresse hinzufügen.
   2. Geben Sie im Feld Client-Adressen die IP-Adresse eines Clients an, für den Root Squash nicht gilt.
   3. Wiederholen Sie den Vorgang nach Bedarf, um weitere Client-IP-Adressen hinzuzufügen.

6. Wählen Sie Aktualisieren.

> **Note**
>
> Wenn Root Squash aktiviert ist und Sie es deaktivieren möchten, wählen Sie Deaktivieren, anstatt die Schritte 4-6 auszuführen.

Sie können den Aktualisierungsfortschritt auf der Detailseite der Dateisysteme auf der Registerkarte Updates überwachen.

So aktualisieren Sie die Root-Squash-Einstellungen auf einem vorhandenen Dateisystem (CLI)

Verwenden Sie den Befehl, um die Root-Squash-Einstellungen für ein vorhandenes FSx for Lustre-Dateisystem zu aktualisieren. AWS CLI update-file-system Die entsprechende API-Operation ist. UpdateFileSystem

Legen Sie die folgenden Parameter fest:

- Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.
- Stellen Sie die `--lustre-configuration RootSquashConfiguration` Optionen wie folgt ein:
  - `RootSquash`— Legt die durch Doppelpunkte getrennten UID:GID-Werte fest, die die Benutzer-ID und Gruppen-ID angeben, die der Root-Benutzer verwenden soll. Sie können für jede ID eine ganze Zahl im Bereich von `0` — `4294967294` (0 ist Stamm) angeben. Um Root-Squash zu deaktivieren, geben Sie `0:0` für die UID:GID-Werte an.
  - `NoSquashNids`— Geben Sie die an Lustre Netzwerkkennungen (NIDs) von Clients, für die Root Squash nicht gilt. Wird verwendet`[]`, um alle Clients zu entfernen NIDs, 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 FSx Amazon-Konsole oder in der Antwort auf einen `describe-file-systems`CLI-Befehl (die entsprechende API-Aktion ist `DescribeFileSystems`) einsehen.

FSx für den Status des Lustre-Dateisystems

Sie können den Status eines FSx Amazon-Dateisystems mithilfe der FSx Amazon-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 erstellt FSx ein neues Dateisystem.
WIRD GELÖSCHT	Amazon löscht FSx 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:

Status des Dateisystems	Beschreibung
	• Das Dateisystem ist ausgefallen und Amazon FSx kann es nicht wiederherstellen. • Beim Erstellen eines neuen Dateisystems FSx konnte Amazon das Dateisystem nicht erstellen.

Taggen Sie Ihre Amazon FSx for Lustre-Ressourcen

Um Ihnen bei der Verwaltung Ihrer Dateisysteme und anderer Amazon FSx for Lustre-Ressourcen zu helfen, können Sie jeder Ressource Ihre eigenen Metadaten in Form von Tags zuweisen. Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Dies ist nützlich, wenn Sie viele Ressourcen desselben Typs haben — In diesem Fall können Sie schnell bestimmte Ressourcen basierend auf den zugewiesenen Tags (Markierungen) bestimmen. In diesem Thema werden Tags (Markierungen) und deren Erstellung beschrieben.

Themen

Grundlagen zu Tags (Markierungen)

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

Mithilfe von Tags können Sie Ihre AWS Ressourcen auf unterschiedliche Weise kategorisieren, z. B. nach Zweck, Eigentümer oder Umgebung. Sie könnten beispielsweise eine Reihe von Tags für die Amazon FSx for Lustre-Dateisysteme Ihres Kontos definieren, mit deren Hilfe Sie den Besitzer und die Stack-Ebene jeder Instance verfolgen können.

Wir empfehlen die Verwendung von Tag (Markierung)-Schlüsseln, die die Anforderungen der jeweiligen Ressourcentypen erfüllen. Die Verwendung einheitlicher Tag-Schlüssel vereinfacht das

Verwalten der -Ressourcen. Sie können die Ressourcen auf Grundlage der hinzugefügten Tags (Markierungen) filtern und danach suchen.

Tags haben für Amazon keine semantische Bedeutung FSx und werden ausschließlich als Zeichenfolge interpretiert. Außerdem werden Tags (Markierungen) nicht automatisch Ihren Ressourcen zugewiesen. Sie können Tag (Markierung)-Schlüssel und -Werte bearbeiten und Tags (Markierungen) jederzeit von einer Ressource entfernen. Sie können den Wert eines Tags (Markierung) zwar auf eine leere Zeichenfolge, jedoch nicht null festlegen. Wenn Sie ein Tag (Markierung) mit demselben Schlüssel wie ein vorhandener Tag (Markierung) für die Ressource hinzufügen, wird der alte Wert mit dem neuen überschrieben. Wenn Sie eine Ressource löschen, werden alle Tags (Markierungen) der Ressource ebenfalls gelöscht.

Wenn Sie die Amazon FSx for Lustre-API, die AWS CLI oder ein AWS SDK verwenden, können Sie die `TagResource` API-Aktion verwenden, um Tags auf vorhandene Ressourcen anzuwenden. Zudem können Sie mit einigen Aktionen zur Ressourcenerstellung Tags beim Erstellen einer Ressource angeben. Wenn Tags (Markierungen) nicht während der Ressourcenerstellung angewendet werden können, wird die Ressourcenerstellung rückgängig gemacht. Auf diese Weise werden Ressourcen entweder mit Tags (Markierungen) oder überhaupt nicht erstellt und keine Ressourcen verbleiben ohne Tags (Markierungen). Indem Sie Ressourcen zum Erstellungszeitpunkt markieren, müssen Sie anschließend keine benutzerdefinierten Skripts ausführen. Weitere Informationen darüber, wie Sie Benutzern ermöglichen, Ressourcen bei der Erstellung zu markieren, finden Sie unter Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung.

Markieren Ihrer -Ressourcen

Sie können Amazon FSx for Lustre-Ressourcen, die in Ihrem Konto vorhanden sind, taggen. Wenn Sie die FSx Amazon-Konsole verwenden, können Sie Tags auf Ressourcen anwenden, indem Sie die Registerkarte Tags auf dem entsprechenden Ressourcenbildschirm verwenden. Wenn Sie Ressourcen erstellen, können Sie den Namensschlüssel mit einem Wert angeben, und Sie können Tags Ihrer Wahl anwenden, wenn Sie ein neues Dateisystem erstellen. Die Konsole kann Ressourcen nach dem Name-Tag organisieren, aber dieses Tag hat für den Amazon FSx for Lustre-Service keine semantische Bedeutung.

Sie können tagbasierte Berechtigungen auf Ressourcenebene in Ihren IAM-Richtlinien auf Amazon FSx for Lustre-API-Aktionen anwenden, die das Tagging bei der Erstellung unterstützen, um eine detaillierte Kontrolle über die Benutzer und Gruppen zu implementieren, die Ressourcen bei der Erstellung taggen können. Ihre Ressourcen sind ab Erstellung ordnungsgemäß geschützt. Tags (Markierungen) werden direkt auf Ihre Ressourcen angewendet. Daher treten alle Tag (Markierung)-

basierten Berechtigungen auf Ressourcenebene, die die Verwendung von Ressourcen steuern, direkt in Kraft. Ihre Ressourcen können nachverfolgt und genauer erfasst werden. Sie können das Markieren neuer Ressourcen gewährleisten und steuern, welche Tag (Markierung)-Schlüssel und Werte für Ihre Ressourcen festgelegt sind.

Sie können auch Berechtigungen auf Ressourcenebene auf die API-Aktionen `TagResource` und `UntagResource` Amazon FSx for Lustre-API-Aktionen in Ihren IAM-Richtlinien anwenden, um zu kontrollieren, welche Tag-Schlüssel und -Werte für Ihre vorhandenen Ressourcen festgelegt werden.

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

Tag-Einschränkungen

Die folgenden grundlegenden Einschränkungen gelten für Tags (Markierungen):

- Maximale Anzahl von Tags (Markierungen) pro Ressource: 50
- Jeder Tag (Markierung) muss für jede Ressource eindeutig sein. Jeder Tag (Markierung) kann nur einen Wert haben.
- Maximale Schlüssellänge: 128 Unicode-Zeichen in UTF-8
- Maximale Wertlänge: 256 Unicode-Zeichen in UTF-8
- Die zulässigen Zeichen für Amazon FSx for Lustre-Tags sind: Buchstaben, Zahlen und Leerzeichen, die in UTF-8 dargestellt werden können, sowie die folgenden Zeichen: + - =. _:/@.
- Bei Tag-Schlüsseln und -Werten wird zwischen Groß- und Kleinschreibung unterschieden.
- Das `aws:` Präfix ist für die Verwendung reserviert. AWS Wenn der Tag (Markierung) über einen Tag (Markierung)-Schlüssel mit diesem Präfix verfügt, können Sie den Schlüssel oder Wert des Tags (Markierung) nicht bearbeiten oder löschen. Tags (Markierungen) mit dem Präfix `aws:` werden nicht als Ihre Tags (Markierungen) pro Ressourcenlimit angerechnet.

Sie können eine Ressource nicht ausschließlich anhand ihrer Tags löschen. Sie müssen die Ressourcen-ID angeben. Um beispielsweise ein Dateisystem zu löschen, das Sie mit einem Tag-Schlüssel namens gekennzeichnet haben`DeleteMe`, müssen Sie die `DeleteFileSystem` Aktion mit der Dateisystem-Ressourcen-ID verwenden, z. B. fs-1234567890abcdef0.

Wenn Sie öffentliche oder gemeinsam genutzte Ressourcen taggen, sind die von Ihnen zugewiesenen Tags nur für Sie verfügbar. Andere haben keinen Zugriff auf diese Tags AWS-Konto. AWS-Konto Für die Tag-basierte Zugriffskontrolle auf gemeinsam genutzte Ressourcen AWS-Konto

muss jede Ressource ihren eigenen Satz von Tags zuweisen, um den Zugriff auf die Ressource zu kontrollieren.

Berechtigungen und Tag

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

Wartungsfenster FSx von Amazon for Lustre

Amazon FSx for Lustre führt routinemäßige Software-Patches für die von ihm verwaltete Lustre Software durch. Patches erfolgen selten, in der Regel einmal alle paar Wochen. Das Wartungsfenster bietet Ihnen die Möglichkeit, zu kontrollieren, an welchem Wochentag und zu welcher Uhrzeit das Software-Patching erfolgt. Das Wartungsfenster wählen Sie bei der Erstellung des Dateisystems aus. Wenn Sie keine Zeitpräferenz haben, wird ein Standardfenster von 30 Minuten zugewiesen.

Das Patchen sollte nur einen Bruchteil Ihres 30-minütigen Wartungsfensters in Anspruch nehmen. Während dieser wenigen Minuten ist Ihr Dateisystem vorübergehend nicht verfügbar. Dateioperationen, die von Clients ausgeführt werden, während das Dateisystem nicht verfügbar ist, werden auf transparente Weise wiederholt und sind schließlich nach Abschluss der Wartung erfolgreich. Beachten Sie, dass der In-Memory-Cache während der Wartung gelöscht wird, was zu höheren Latenzen führt, bis die Wartung abgeschlossen ist.

FSx for Lustre ermöglicht es Ihnen, Ihr Wartungsfenster nach Bedarf an Ihre Arbeitslast und Ihre betrieblichen Anforderungen anzupassen. Sie können Ihr Wartungsfenster beliebig oft verschieben, vorausgesetzt, dass mindestens einmal alle 14 Tage ein Wartungsfenster geplant ist. Wenn ein Patch veröffentlicht wird und Sie innerhalb von 14 Tagen kein Wartungsfenster geplant haben, wird FSx for Lustre mit der Wartung des Dateisystems fortfahren, um dessen Sicherheit und Zuverlässigkeit zu gewährleisten.

Sie können die Amazon FSx Management Console AWS CLI, AWS API oder eine davon verwenden, AWS SDKs um das Wartungsfenster für Ihre Dateisysteme zu ändern.

Um das Wartungsfenster mithilfe der Konsole zu ändern

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.

2. Wählen Sie im Navigationsbereich Dateisysteme aus.
3. Wählen Sie das Dateisystem aus, für das Sie das Wartungsfenster ändern möchten. Die Seite mit den Dateisystemdetails wird angezeigt.
4. Wählen Sie die Registerkarte Wartung. Das Fenster „Einstellungen“ des Wartungsfensters wird angezeigt.
5. Wählen Sie Bearbeiten und geben Sie den neuen Tag und die Uhrzeit ein, an dem das Wartungsfenster beginnen soll.
6. Wählen Sie Speichern, um Ihre Änderungen zu speichern. Die neue Startzeit der Wartung wird im Bereich Einstellungen angezeigt.

Sie können das Wartungsfenster für Ihr Dateisystem mit dem update-file-systemCLI-Befehl ändern. Führen Sie den folgenden Befehl aus und ersetzen Sie dabei die Dateisystem-ID durch die ID für Ihr Dateisystem und das Datum und die Uhrzeit, zu der Sie das Fenster starten möchten.

```
aws fsx update-file-system --file-system-id fs-01234567890123456 --lustre-configuration
 WeeklyMaintenanceStartTime=1:01:30
```

Verwaltung von Lustre-Versionen

FSx for Lustre unterstützt derzeit mehrere Lustre-Versionen mit langfristigem Support (LTS), die von der Lustre-Community veröffentlicht wurden. Neuere LTS-Versionen bieten Vorteile wie Leistungsverbesserungen, neue Funktionen und Unterstützung für die neuesten Linux-Kernelversionen für Ihre Client-Instances. Mit dem, oder können Sie Ihre Dateisysteme innerhalb weniger Minuten auf neuere Lustre-Versionen aktualisieren. AWS-Managementkonsole AWS CLI AWS SDKs

FSx for Lustre unterstützt derzeit die Lustre LTS-Versionen 2.10, 2.12 und 2.15. Sie können die LTS-Version Ihres FSx for Lustre-Dateisystems mithilfe des Befehls oder mithilfe des Befehls ermitteln. AWS-Managementkonsole describe-file-systems AWS CLI

Bevor Sie ein Lustre-Versionsupgrade durchführen, empfehlen wir Ihnen, die unter beschriebenen Schritte zu befolgen. Bewährte Methoden für Lustre-Versionsupgrades

Themen

Bewährte Methoden für Lustre-Versionsupgrades

Wir empfehlen, diese bewährten Methoden zu befolgen, bevor Sie die Lustre-Version Ihres FSx for Lustre-Dateisystems aktualisieren:

- Testen Sie in einer Nicht-Produktionsumgebung: Testen Sie ein Lustre-Versionsupgrade auf einem Duplikat Ihres Produktionsdateisystems, bevor Sie Ihr Produktionsdateisystem aktualisieren. Dadurch wird ein reibungsloser Upgrade-Prozess für Ihre Produktions-Workloads gewährleistet.
- Stellen Sie die Client-Kompatibilität sicher: Stellen Sie sicher, dass die Linux-Kernel-Versionen, die auf Ihren Client-Instances ausgeführt werden, mit der Lustre-Version kompatibel sind, auf die Sie aktualisieren möchten. Details dazu finden Sie unter LustreDateisystem- und Client-Kernel-Kompatibilität.
- Erstellen Sie eine Sicherungskopie Ihrer Daten:
  - Für Dateisysteme, die nicht mit S3 verknüpft sind: Wir empfehlen Ihnen, vor dem Upgrade der Lustre-Version eine FSx Sicherungskopie zu erstellen, damit Sie über einen bekannten Wiederherstellungspunkt für Ihr Dateisystem verfügen. Wenn automatische tägliche Backups auf Ihrem Dateisystem aktiviert sind, erstellt Amazon vor dem Upgrade FSx automatisch eine Sicherungskopie Ihres Dateisystems.
  - Für Dateisysteme, die mit S3 verknüpft sind, empfehlen wir, vor dem Upgrade sicherzustellen, dass alle Änderungen nach S3 exportiert wurden. Wenn Sie den automatischen Export aktiviert haben, überprüfen Sie, ob die `AgeOfOldestQueuedMessage` AutoExportMetrik Null ist, um sicherzustellen, dass alle Änderungen erfolgreich nach S3 exportiert wurden. Wenn Sie den automatischen Export nicht aktiviert haben, können Sie vor dem Upgrade einen manuellen DRT-Export (Data Repository Task) ausführen, um Ihr Dateisystem mit dem S3-Bucket zu synchronisieren.

Durchführung des Upgrades

Gehen Sie wie folgt vor, um Ihr FSx for Lustre-Dateisystem auf eine neuere Version zu aktualisieren:

1. Alle Clients aushängen: Bevor Sie das Upgrade starten, müssen Sie das Dateisystem von allen Client-Instanzen trennen, die auf Ihr Dateisystem zugreifen. Sie können anhand der `ClientConnections` Metrik auf Amazon überprüfen, ob alle Clients erfolgreich unmountet wurden. CloudWatch Diese Metrik sollte keine Verbindungen anzeigen. Der Upgrade-Vorgang wird nicht fortgesetzt, wenn noch Clients mit dem Dateisystem verbunden sind.

Sie können die Liste der Client-Netzwerkkennungen (NIDs), die mit dem Dateisystem verbunden sind, in der `.fsx/clientConnections` Datei einsehen, die im Stammverzeichnis Ihres Dateisystems gespeichert ist. Diese Datei wird alle 5 Minuten aktualisiert. Sie können den `cat` Befehl verwenden, um den Inhalt der Datei anzuzeigen, wie in diesem Beispiel:

```
cat /test/.fsx/clientConnections
```

2. Aktualisieren Sie die Lustre-Version: Sie können die Lustre-Version Ihres FSx for Lustre-Dateisystems mithilfe der FSx Amazon-Konsole, der oder der AWS CLI Amazon-API aktualisieren. FSx Wir empfehlen, Ihre Dateisysteme auf die neueste Lustre-Version zu aktualisieren, die von for Lustre unterstützt wird. FSx

   Um die Lustre-Version eines Dateisystems (Konsole) zu aktualisieren

   a. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.

   b. Wählen Sie im linken Navigationsbereich die Option Dateisysteme aus. Wählen Sie in der Liste Dateisysteme das FSx for Lustre-Dateisystem aus, für das Sie die Lustre-Version aktualisieren möchten.

   c. Wählen Sie unter Aktionen die Option Lustre-Version des Dateisystems aktualisieren aus. Oder wählen Sie im Übersichtsfenster neben dem Feld Lustre-Version des Dateisystems die Option Aktualisieren aus. Das Dialogfeld „Lustre-Version des Dateisystems aktualisieren“ wird angezeigt. Das Dialogfeld Lustre-Version des Dateisystems aktualisieren wird angezeigt.

   d. Wählen Sie für das Feld Neue Lustre-Version auswählen eine Lustre-Version aus. Der von Ihnen gewählte Wert muss neuer als die aktuelle Lustre-Version sein.

   e. Wählen Sie Aktualisieren.

   Um die Lustre-Version eines Dateisystems (CLI) zu aktualisieren

   Verwenden Sie den Befehl, um die Lustre-Version eines FSx for Lustre-Dateisystems zu aktualisieren. AWS CLI update-file-system (Die entsprechende API-Aktion ist UpdateFileSystem.) Legen Sie die folgenden Parameter fest:

   - Geben `--file-system-id` Sie die ID des Dateisystems ein, das Sie aktualisieren.
   - Stellen `--file-system-type-version` Sie für das Dateisystem, das Sie aktualisieren, auf eine neuere Lustre-Version ein.

Im folgenden Beispiel wird die Lustre-Version des Dateisystems von 2.12 auf 2.15 aktualisiert:

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --file-system-type-version "2.15"
```

3. Alle Clients einbinden: Sie können den Fortschritt der Lustre-Versionsupdates überwachen, indem Sie den Tab Updates in der FSx Amazon-Konsole oder `describe-file-systems` im AWS CLI. Sobald der Upgrade-Status der Lustre-Version als angezeigt wird`Completed`, können Sie das Dateisystem auf Ihren Client-Instances sicher erneut mounten und Ihre Arbeitslast wieder aufnehmen.

Löschen eines Dateisystems

Sie können ein Amazon FSx for Lustre-Dateisystem mithilfe der FSx Amazon-Konsole AWS CLI, der und der FSx Amazon-API löschen. Bevor Sie ein FSx for Lustre-Dateisystem löschen, sollten Sie es von jeder verbundenen EC2 Amazon-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 von jeder EC2 Amazon-Instance zu löschen:

- Verwenden der Konsole — Folgen Sie dem unter beschriebenen Verfahren. Schritt 5: Bereinigen von -Ressourcen
- Verwenden der API oder CLI — Verwenden Sie den DeleteFileSystemAPI-Vorgang oder den delete-file-systemCLI-Befehl.

Schützen Sie Ihre Daten mit Backups

Mit Amazon FSx for Lustre können Sie automatische tägliche Backups und vom Benutzer initiierte Backups von persistenten Dateisystemen erstellen, die nicht mit einem dauerhaften Amazon S3 S3-Daten-Repository verknüpft sind. FSx Amazon-Backups sind file-system-consistent äußerst robust und inkrementell. Um eine hohe Haltbarkeit zu gewährleisten, speichert Amazon FSx for Lustre Backups im Amazon Simple Storage Service (Amazon S3) mit einer Haltbarkeit von 99,999999999% (11 9).

FSx Bei Lustre handelt es sich bei Dateisystem-Backups um blockbasierte, inkrementelle Backups, unabhängig davon, ob sie mithilfe der automatischen täglichen Sicherung oder der vom Benutzer initiierten Backup-Funktion generiert werden. Das heißt, wenn Sie ein Backup erstellen, FSx vergleicht Amazon die Daten auf Ihrem Dateisystem mit Ihrem vorherigen Backup auf Blockebene. Dann FSx speichert Amazon eine Kopie aller Änderungen auf Blockebene im neuen Backup. Daten auf Blockebene, die seit der vorherigen Sicherung unverändert geblieben sind, werden nicht in der neuen Sicherung gespeichert. Die Dauer des Sicherungsvorgangs hängt davon ab, wie viele Daten sich seit der letzten Sicherung geändert haben, und ist unabhängig von der Speicherkapazität des Dateisystems. Die folgende Liste zeigt die Backup-Zeiten unter verschiedenen Umständen:

- Die erste Sicherung eines brandneuen Dateisystems mit sehr wenigen Daten dauert Minuten.
- Die erste Sicherung eines brandneuen Dateisystems, die nach dem Laden TBs der Daten erstellt wurde, dauert Stunden.
- Eine zweite Sicherung des Dateisystems mit Daten mit TBs minimalen Änderungen an den Daten auf Blockebene (relativ wenige Erstellungen/Änderungen) dauert Sekunden.
- Eine dritte Sicherung desselben Dateisystems, nachdem eine große Datenmenge hinzugefügt und geändert wurde, dauert Stunden.

Wenn Sie eine Sicherung löschen, werden nur die Daten entfernt, die für diese Sicherung eindeutig sind. Jedes FSx For Lustre-Backup enthält alle Informationen, die benötigt werden, um aus dem Backup ein neues Dateisystem zu erstellen, wodurch ein point-in-time Snapshot des Dateisystems effektiv 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. FSx Amazon-Backups unterstützen Sie dabei, Ihre Anforderungen an die Aufbewahrung und Einhaltung von Vorschriften für Backups zu erfüllen. Die Arbeit mit Amazon FSx for Lustre-Backups ist einfach, egal ob es

darum geht, Backups zu erstellen, eine Sicherung zu kopieren, ein Dateisystem aus einer Sicherung wiederherzustellen oder eine Sicherung zu löschen.

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

Themen

Backup-Unterstützung FSx für Lustre

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

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

Arbeiten mit automatischen täglichen Backups

Amazon FSx for Lustre kann täglich ein automatisches Backup Ihres Dateisystems erstellen. Diese automatischen täglichen Backups erfolgen während des täglichen Backup-Fensters, das bei

der Erstellung des Dateisystems festgelegt wurde. Irgendwann während des täglichen Backup-Fensters wird der Speicher I/O möglicherweise kurzzeitig unterbrochen, während der Backup-Vorgang initialisiert wird (normalerweise für weniger als ein paar Sekunden). Wir empfehlen Ihnen, bei der Auswahl Ihres täglichen Backup-Fensters eine passende Tageszeit zu wählen. Diese Zeit liegt idealerweise außerhalb der normalen Betriebszeiten der Anwendungen, die das Dateisystem verwenden.

Automatische tägliche Backups werden für einen bestimmten Zeitraum aufbewahrt, der als Aufbewahrungszeitraum bezeichnet wird. Sie können die Aufbewahrungsfrist auf 0 bis 90 Tage festlegen. Wenn Sie den Aufbewahrungszeitraum auf 0 (Null) Tage festlegen, werden automatische tägliche Backups deaktiviert. Die Standardaufbewahrungsdauer für automatische tägliche Backups beträgt 0 Tage. Automatische tägliche Backups werden gelöscht, wenn das Dateisystem gelöscht wird.

> **Note**
>
> Wenn Sie die Aufbewahrungsfrist auf 0 Tage festlegen, wird Ihr Dateisystem niemals automatisch gesichert. Es wird dringend empfohlen, automatische tägliche Backups für Dateisysteme zu verwenden, mit denen ein gewisses Maß an kritischer Funktionalität verknüpft ist.

Sie können die AWS CLI oder eine der Optionen verwenden AWS SDKs , um das Backup-Fenster und den Aufbewahrungszeitraum für Backups für Ihre Dateisysteme zu ändern. Verwenden Sie die `UpdateFileSystem`API-Operation oder den `update-file-system`CLI-Befehl.

Arbeiten mit vom Benutzer initiierten Backups

Mit Amazon FSx for Lustre können Sie jederzeit manuell Backups Ihrer Dateisysteme erstellen. Sie können dies mit der Amazon FSx for Lustre-Konsole, der API oder der AWS Command Line Interface (CLI) tun. Ihre vom Benutzer initiierten Backups von FSx Amazon-Dateisystemen laufen nie ab und sie sind so lange verfügbar, wie Sie sie behalten möchten. Benutzerinitiierte Backups werden auch nach dem Löschen des Dateisystems, das gesichert wurde, beibehalten. Sie können vom Benutzer initiierte Backups nur mithilfe der Amazon FSx for Lustre-Konsole, API oder CLI löschen. Sie werden niemals automatisch von Amazon gelöscht. FSx Weitere Informationen finden Sie unter Löschen von Backups.

Benutzerinitiierte Backups erstellen

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

So erstellen Sie ein vom Benutzer initiiertes Dateisystem-Backup

1. Öffnen Sie die Amazon FSx for Lustre-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Konsolen-Dashboard den Namen des Dateisystems aus, das Sie sichern möchten.
3. Wählen Sie unter Aktionen die Option Backup erstellen aus.
4. Geben Sie im sich öffnenden Dialogfeld „Backup erstellen“ einen Namen für Ihr Backup ein. Backup-Namen können maximal 256 Unicode-Zeichen enthalten, einschließlich Buchstaben, Leerzeichen, Zahlen und Sonderzeichen. + - = _:/
5. Wählen Sie Create backup (Backup erstellen).

Sie haben jetzt Ihr Dateisystem-Backup erstellt. Sie finden eine Tabelle mit all Ihren Backups in der Amazon FSx for Lustre-Konsole, indem Sie in der linken Navigationsleiste Backups wählen. Sie können nach dem Namen suchen, den Sie Ihrem Backup gegeben haben, und die Tabelle so filtern, dass nur passende Ergebnisse angezeigt werden.

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

Verwendung AWS Backup mit Amazon FSx

AWS Backup ist eine einfache und kostengünstige Möglichkeit, Ihre Daten zu schützen, indem Sie Ihre FSx Amazon-Dateisysteme sichern. AWS Backup ist ein einheitlicher Backup-Service, der das Erstellen, Kopieren, Wiederherstellen und Löschen von Backups vereinfacht und gleichzeitig eine verbesserte Berichterstattung und Prüfung bietet. AWS Backup erleichtert die Entwicklung einer zentralen Backup-Strategie zur Einhaltung gesetzlicher, regulatorischer und professioneller Vorschriften. AWS Backup erleichtert außerdem den Schutz Ihrer AWS Speichervolumes, Datenbanken und Dateisysteme, indem es einen zentralen Ort bereitstellt, an dem Sie Folgendes tun können:

- Konfigurieren und prüfen Sie die AWS Ressourcen, die Sie sichern möchten.
- Automatisieren geplanter Sicherungen
- Festlegen von Aufbewahrungsrichtlinien
- Kopieren Sie Backups zwischen AWS Regionen und AWS Konten.
- Überwachen der letzten Sicherungs- und Wiederherstellungsaktivitäten

AWS Backup verwendet die integrierte Backup-Funktionalität von Amazon FSx. Von der AWS Backup Konsole aus erstellte Backups haben dieselbe Konsistenz und Leistung des Dateisystems und dieselben Wiederherstellungsoptionen wie Backups, die über die FSx Amazon-Konsole erstellt wurden. Wenn Sie AWS Backup diese Backups verwalten, erhalten Sie zusätzliche Funktionen, wie z. B. unbegrenzte Aufbewahrungsoptionen und die Möglichkeit, geplante Backups so oft wie jede Stunde zu erstellen. Darüber hinaus werden Ihre unveränderlichen Backups auch nach dem Löschen des Quelldateisystems AWS Backup beibehalten. Dies schützt vor versehentlichem oder böswilligem Löschen.

Backups, die von erstellt wurden, AWS Backup haben einen Backup-Typ `AWS_BACKUP` und sind inkrementell im Vergleich zu allen anderen FSx Amazon-Backups, die Sie von Ihrem Dateisystem erstellen. Von erstellte Backups AWS Backup gelten als vom Benutzer initiierte Backups und werden auf das vom Benutzer initiierte Backup-Kontingent für Amazon angerechnet. FSx Sie können Backups, die von erstellt wurden, AWS Backup in der FSx Amazon-Konsole, CLI und API anzeigen und wiederherstellen. Sie können die Backups, die von AWS Backup in der FSx Amazon-Konsole, CLI oder API erstellt wurden, jedoch nicht löschen. Weitere Informationen AWS Backup zur Sicherung Ihrer FSx Amazon-Dateisysteme finden Sie unter Arbeiten mit FSx Amazon-Dateisystemen im AWS Backup Entwicklerhandbuch.

Kopieren eines Backups

Sie können Amazon verwenden FSx , um Backups innerhalb desselben AWS Kontos manuell auf ein anderes AWS-Region (regionsübergreifende Kopien) oder innerhalb desselben Kontos AWS-Region (regionsinterne Kopien) zu kopieren. Sie können regionsübergreifende Kopien nur innerhalb derselben Partition erstellen. AWS Sie können mithilfe der FSx Amazon-Konsole oder API benutzerinitiierte Sicherungskopien erstellen. AWS CLI Wenn Sie eine benutzerinitiierte Sicherungskopie erstellen, hat sie den folgenden Typ. `USER_INITIATED`

Sie können es auch verwenden AWS Backup , um Backups kontenübergreifend AWS-Regionen und AWS kontenübergreifend zu kopieren. AWS Backup ist ein vollständig verwalteter Backup-

Management-Service, der eine zentrale Schnittstelle für richtlinienbasierte Backup-Pläne bietet. Dank der kontenübergreifenden Verwaltung können Sie Backup-Richtlinien automatisch verwenden, um Backup-Pläne für alle Konten innerhalb Ihres Unternehmens anzuwenden.

Regionsübergreifende Backup-Kopien sind besonders wertvoll für die regionsübergreifende Notfallwiederherstellung. Sie erstellen Backups und kopieren sie in eine andere AWS Region, sodass Sie im Fall eines Notfalls in der primären AWS-Region Region Daten aus dem Backup wiederherstellen und die Verfügbarkeit in der anderen AWS Region schnell wiederherstellen können. Sie können auch Sicherungskopien verwenden, um Ihren Dateidatensatz in eine andere AWS-Region oder innerhalb derselben zu klonen AWS-Region. Sie erstellen Sicherungskopien innerhalb desselben AWS Kontos (regionsübergreifend oder regionsübergreifend), AWS CLI indem Sie die FSx Amazon-Konsole oder die Amazon FSx for Lustre-API verwenden. Sie können damit auch Sicherungskopien erstellen AWS Backup, entweder auf Abruf oder auf Grundlage von Richtlinien.

Kontoübergreifende Sicherungskopien sind nützlich, wenn es darum geht, Ihre gesetzlichen Anforderungen zu erfüllen und Backups auf ein isoliertes Konto zu kopieren. Sie bieten auch eine zusätzliche Datenschutzebene, um das versehentliche oder böswillige Löschen von Backups, den Verlust von Anmeldeinformationen oder die Kompromittierung von AWS KMS Schlüsseln zu verhindern. Kontoübergreifende Backups unterstützen Fan-In (Kopieren von Backups von mehreren Primärkonten auf ein isoliertes Backup-Kopie-Konto) und Fan-Out (Kopieren von Backups von einem primären Konto auf mehrere isolierte Backup-Kopie-Konten).

Mithilfe von with support können Sie kontoübergreifende Sicherungskopien erstellen. AWS Backup AWS Organizations Kontogrenzen für kontenübergreifende Kopien werden durch AWS Organizations Richtlinien definiert. Weitere Informationen zur Erstellung von AWS Backup kontoübergreifenden Backup-Kopien finden Sie AWS-Konten im AWS Backup Developer Guide unter Backup-Kopien erstellen.

Einschränkungen bei Backup-Kopien

Im Folgenden sind einige Einschränkungen beim Kopieren von Backups aufgeführt:

- Backups von Dateisystemen, die die Intelligent-Tiering-Speicherklasse verwenden, unterstützen keine Sicherungskopien.
- Regionsübergreifende Sicherungskopien werden nur zwischen zwei beliebigen Handelsregionen AWS-Regionen, zwischen den Regionen China (Peking) und China (Ningxia) sowie zwischen den Regionen AWS GovCloud (USA-Ost) und AWS GovCloud (US-West) unterstützt, jedoch nicht zwischen diesen Gruppen von Regionen.

- Regionsübergreifende Backup-Kopien werden in Opt-in-Regionen nicht unterstützt.
- Sie können in jeder Region Sicherungskopien für jede Region erstellen. AWS-Region
- Das Quell-Backup muss den Status von haben, `AVAILABLE` bevor Sie es kopieren können.
- Sie können ein Quell-Backup nicht löschen, wenn es kopiert wird. Zwischen dem Zeitpunkt, zu dem das Ziel-Backup verfügbar wird, und dem Zeitpunkt, zu dem Sie das Quell-Backup löschen dürfen, kann es zu einer kurzen Verzögerung kommen. Sie sollten diese Verzögerung berücksichtigen, wenn Sie erneut versuchen, ein Quell-Backup zu löschen.
- AWS-Region Pro Konto können bis zu fünf Backup-Kopie-Anfragen an ein einziges Ziel ausgeführt werden.

Berechtigungen für regionsübergreifende Sicherungskopien

Sie verwenden eine IAM-Richtlinienanweisung, um Berechtigungen zur Durchführung eines Sicherungskopievorgangs zu erteilen. Um mit der AWS Quellregion zu kommunizieren und eine regionsübergreifende Sicherungskopie anzufordern, muss der Anforderer (IAM-Rolle oder IAM-Benutzer) Zugriff auf das Quell-Backup und die Quellregion haben. AWS

Sie verwenden die Richtlinie, um der `CopyBackup` Aktion für den Sicherungskopievorgang Berechtigungen zu erteilen. Sie geben die Aktion im `Action` Feld der Richtlinie an, und Sie geben den Ressourcenwert im `Resource` Feld der Richtlinie an, wie im folgenden Beispiel.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111122223333:backup/*"
        }
    ]
}
```

Weitere Informationen zu IAM-Richtlinien finden Sie unter Richtlinien und Berechtigungen in IAM im IAM-Benutzerhandbuch.

Vollständige und inkrementelle Kopien

Wenn Sie ein Backup in ein anderes AWS-Region Backup als das Quell-Backup kopieren, ist die erste Kopie eine vollständige Sicherungskopie. Nach der ersten Sicherungskopie sind alle nachfolgenden Sicherungskopien in dieselbe Zielregion innerhalb desselben AWS Kontos inkrementell, sofern Sie nicht alle zuvor kopierten Backups in dieser Region gelöscht haben und denselben Schlüssel verwendet haben. AWS KMS Wenn beide Bedingungen nicht erfüllt sind, führt der Kopiervorgang zu einer vollständigen (nicht inkrementellen) Sicherungskopie.

Backups werden innerhalb derselben Datei kopiert AWS-Konto

Sie können Backups von FSx for Lustre-Dateisystemen mithilfe der AWS-Managementkonsole CLI und der API kopieren, wie in den folgenden Verfahren beschrieben.

Um ein Backup innerhalb desselben Kontos (regionsübergreifend oder regionsübergreifend) mithilfe der Konsole zu kopieren

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Navigationsbereich Sicherungen aus.
3. Wählen Sie in der Tabelle Backups das Backup aus, das Sie kopieren möchten, und wählen Sie dann Backup kopieren aus.
4. Gehen Sie im Abschnitt Settings (Einstellungen) wie folgt vor:

   - Wählen Sie in der Liste Zielregion eine AWS Zielregion aus, in die das Backup kopiert werden soll. Das Ziel kann sich in einer anderen AWS Region (regionsübergreifende Kopie) oder innerhalb derselben AWS Region (regionsinterne Kopie) befinden.
   - (Optional) Wählen Sie „Tags kopieren“, um Tags aus dem Quell-Backup in das Ziel-Backup zu kopieren. Wenn Sie in Schritt 6 „Tags kopieren“ auswählen und auch Tags hinzufügen, werden alle Tags zusammengeführt.
5. Wählen Sie unter Verschlüsselung den AWS KMS Verschlüsselungsschlüssel aus, um das kopierte Backup zu verschlüsseln.
6. Geben Sie unter Tags — optional einen Schlüssel und einen Wert ein, um Tags für Ihr kopiertes Backup hinzuzufügen. Wenn Sie hier Tags hinzufügen und in Schritt 4 auch Tags kopieren ausgewählt haben, werden alle Tags zusammengeführt.
7. Klicken Sie auf Copy backup (Backup kopieren).

   Ihr Backup wird innerhalb desselben in AWS-Konto das ausgewählte kopiert AWS-Region.

Um ein Backup innerhalb desselben Kontos (regionsübergreifend oder regionsübergreifend) mit der CLI zu kopieren

- Verwenden Sie den `copy-backup` CLI-Befehl oder die CopyBackupAPI-Operation, um ein Backup innerhalb desselben AWS Kontos zu kopieren, entweder innerhalb einer AWS Region oder innerhalb einer AWS Region.

  Der folgende Befehl kopiert ein Backup mit der ID `backup-0abc123456789cba7` aus der `us-east-1` Region.

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  Die Antwort enthält die Beschreibung des kopierten Backups.

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

Backups wiederherstellen

Sie können ein verfügbares Backup verwenden, um ein neues Dateisystem zu erstellen und so effektiv einen point-in-time Snapshot eines anderen Dateisystems wiederherzustellen. Sie können ein Backup mithilfe der Konsole oder einer der AWS SDKs. AWS CLI Das Wiederherstellen eines Backups in einem neuen Dateisystem dauert genauso lange wie das Erstellen eines neuen Dateisystems. Die aus dem Backup wiederhergestellten Daten werden verzögert in das Dateisystem geladen. Während dieser Zeit kommt es zu einer etwas höheren Latenz.

> **Note**
>
> Sie können Ihr Backup nur in einem Dateisystem wiederherstellen, das denselben Bereitstellungstyp, dieselbe Speicherklasse, dieselbe Durchsatzkapazität, dieselbe Speicherkapazität und denselben Datenkomprimierungstyp aufweist AWS-Region wie das Original. Sie können die Speicherkapazität Ihres wiederhergestellten Dateisystems erhöhen, sobald es verfügbar ist.

So stellen Sie mithilfe der Konsole ein Dateisystem aus einer Sicherung wieder her

1. Öffnen Sie die Amazon FSx for Lustre-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Konsolen-Dashboard in der linken Navigationsleiste Backups aus.
3. Wählen Sie in der Tabelle Backups das Backup aus, das Sie wiederherstellen möchten, und wählen Sie dann Backup wiederherstellen aus.

   Der Assistent für die Erstellung des Dateisystems wird geöffnet, wobei die meisten Einstellungen auf der Grundlage der Konfiguration des Dateisystems, aus dem das Backup erstellt wurde, bereits ausgefüllt sind. Sie können optional die Virtual Private Cloud (VPC) - Konfiguration ändern oder eine neuere Lustre-Version wählen. Beachten Sie, dass andere Konfigurationseinstellungen, wie der Bereitstellungstyp und der Durchsatz pro Speichereinheit, während der Wiederherstellung nicht geändert werden können.
4. Führen Sie den Assistenten genauso aus, wie Sie es beim Erstellen eines neuen Dateisystems tun.
5. Wählen Sie Review and create.
6. Überprüfen Sie die Einstellungen, die Sie für Ihr Amazon FSx for Lustre-Dateisystem ausgewählt haben, und wählen Sie dann Dateisystem erstellen.

Sie haben die Daten aus einer Sicherungskopie wiederhergestellt, und ein neues Dateisystem wird gerade erstellt. Wenn sich der Status auf ändert`AVAILABLE`, können Sie das Dateisystem wie gewohnt verwenden.

Löschen von Backups

Das Löschen eines Backups ist eine permanente, nicht wiederherstellbare Aktion. Alle Daten in einem gelöschten Backup werden ebenfalls gelöscht. Löschen Sie kein Backup, es sei denn, Sie sind sich sicher, dass Sie dieses Backup in future nicht mehr benötigen werden. Sie können keine Backups löschen, die AWS Backup in der FSx Amazon-Konsole, CLI oder API erstellt wurden.

So löschen Sie ein Backup

1. Öffnen Sie die Amazon FSx for Lustre-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Konsolen-Dashboard in der linken Navigationsleiste Backups aus.
3. Wählen Sie in der Tabelle Backups das Backup aus, das Sie löschen möchten, und wählen Sie dann Backup löschen aus.

4. Vergewissern Sie sich im sich öffnenden Dialogfeld „Backups löschen“, dass die ID des Backups das Backup identifiziert, das Sie löschen möchten.
5. Vergewissern Sie sich, dass das Kontrollkästchen für das Backup, das Sie löschen möchten, aktiviert ist.
6. Wählen Sie Backups löschen.

Ihr Backup und alle enthaltenen Daten sind jetzt dauerhaft und unwiederbringlich gelöscht.

Überwachung von Amazon FSx for Lustre-Dateisystemen

Die Überwachung ist ein wichtiger Bestandteil der Aufrechterhaltung der Zuverlässigkeit, Verfügbarkeit und Leistung Ihres FSx for Lustre-Dateisystems und Ihrer anderen AWS Lösungen. Durch die Erfassung von Überwachungsdaten aus allen Teilen Ihrer AWS Lösung können Sie Fehler, die mehrere Punkte betreffen, einfacher debuggen, falls einer auftritt. Mithilfe der folgenden Tools können Sie Ihr FSx for Lustre-Dateisystem überwachen, melden, wenn etwas nicht stimmt, und bei Bedarf automatisch Maßnahmen ergreifen:

- Amazon CloudWatch — Überwacht Ihre AWS Ressourcen und die Anwendungen, auf denen Sie laufen, AWS in Echtzeit. Sie können Metriken sammeln und verfolgen, benutzerdefinierte Dashboards erstellen und Alarme einrichten, die Sie benachrichtigen, wenn eine bestimmte Metrik einen von Ihnen festgelegten Schwellenwert erreicht. Sie können beispielsweise die Speicherkapazität oder andere Kennzahlen für Ihre Amazon FSx for Lustre-Instances CloudWatch verfolgen und bei Bedarf automatisch neue Instances starten.
- Lustre-Protokollierung — Überwacht die aktivierten Logging-Ereignisse für Ihr Dateisystem. Lustre Logging schreibt diese Ereignisse in Amazon CloudWatch Logs.
- AWS CloudTrail— Erfasst API-Aufrufe und zugehörige Ereignisse, die von Ihnen oder in Ihrem Namen getätigt wurden, AWS-Konto und übermittelt die Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket. Sie können die Benutzer und Konten, die AWS aufgerufen haben, identifizieren, sowie die Quell-IP-Adresse, von der diese Aufrufe stammen, und den Zeitpunkt der Aufrufe ermitteln.

Die folgenden Abschnitte enthalten Informationen zur Verwendung der Tools mit Ihren FSx for Lustre-Dateisystemen.

Themen

Überwachung mit Amazon CloudWatch

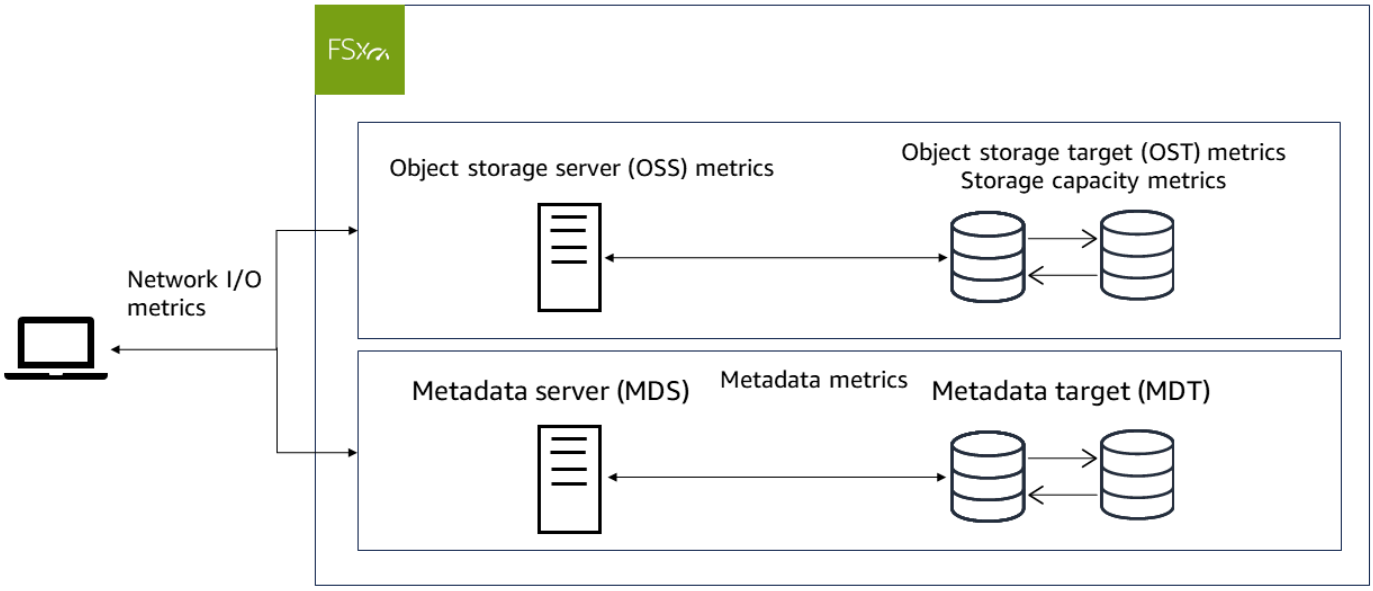
Sie können Amazon FSx for Lustre mithilfe von Amazon for Lustre überwachen CloudWatch, das Rohdaten von Amazon FSx for Lustre sammelt und zu lesbaren, nahezu in Echtzeit verfügbaren

Metriken verarbeitet. Diese Statistiken werden für einen Zeitraum von 15 Monaten aufbewahrt, sodass Sie auf historische Informationen zugreifen und sich einen besseren Überblick über die Leistung Ihrer Anwendung oder Ihres Dienstes verschaffen können. Weitere Informationen zu CloudWatch finden Sie unter Was ist Amazon CloudWatch? im CloudWatch Amazon-Benutzerhandbuch.

CloudWatch Die Metriken FSx für Lustre sind in sechs Kategorien unterteilt:

- I/O Netzwerkmetriken — Messen Sie die Aktivität zwischen Clients und Ihrem Dateisystem.
- Objekt-Storage-Server-Metriken — Messen Sie den Netzwerkdurchsatz und die Festplattendurchsatzauslastung des Object Storage Servers (OSS).
- Zielmetriken für Objektspeicher — Messen Sie den Festplattendurchsatz und die Festplatten-IOPS-Auslastung (Object Storage Target, OST).
- Metriken für Metadaten — Messen Sie die CPU-Auslastung des Metadatenservers (MDS), die IOPS-Auslastung des Metadatenziels (MDT) und die Operationen mit Client-Metadaten.
- Kennzahlen zur Speicherkapazität — Messen Sie die Auslastung der Speicherkapazität.
- S3-Datenrepository-Metriken — Ermitteln das Alter der ältesten Nachricht, die darauf wartet, importiert oder exportiert zu werden, und Umbenennungen, die vom Dateisystem verarbeitet werden.

Das folgende Diagramm zeigt ein FSx For Lustre-Dateisystem, seine Komponenten und seine metrischen Kategorien.



FSx for Lustre sendet Metrikdaten in Intervallen von 1 CloudWatch Minute an.

> **Note**
>
> Während der Wartungsfenster für das Dateisystem Ihres Amazon FSx for Lustre-Dateisystems dürfen keine Messwerte veröffentlicht werden.

Themen

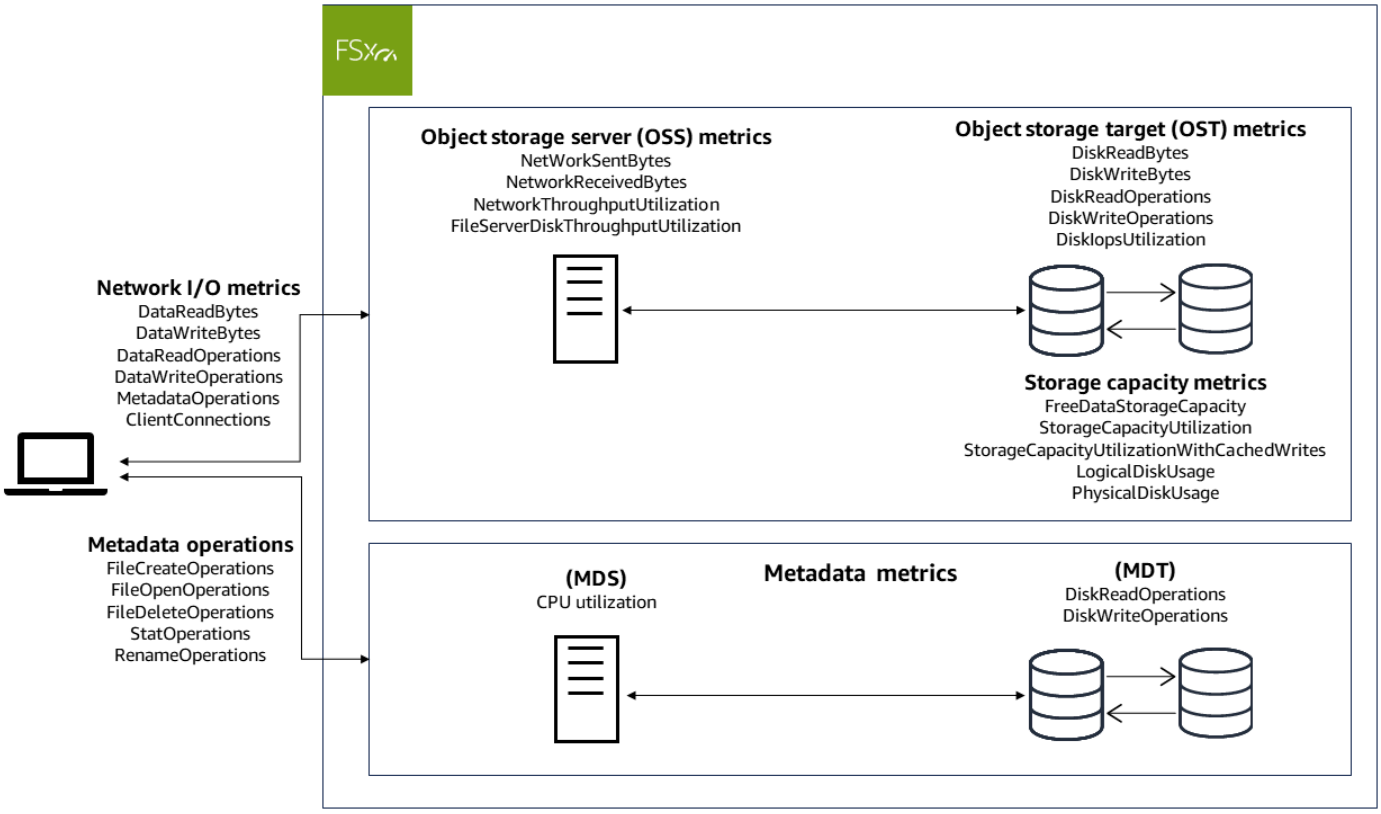
- So verwenden Sie Amazon FSx for Lustre-Metriken CloudWatch
- Zugriff auf Metriken CloudWatch
- Kennzahlen und Dimensionen von Amazon FSx for Lustre
- Leistungswarnungen und Empfehlungen
- CloudWatch Alarme zur Überwachung von Messwerten erstellen

So verwenden Sie Amazon FSx for Lustre-Metriken CloudWatch

Jedes Amazon FSx for Lustre-Dateisystem besteht aus zwei Hauptarchitekturkomponenten:

- Ein oder mehrere Objektspeicherserver (OSSs), die Daten für Clients bereitstellen, die auf das Dateisystem zugreifen. Jedes Betriebssystem ist an ein oder mehrere Speichervolumes angehängt, die als Objektspeicherziele (OSTs) bezeichnet werden und die Daten in Ihrem Dateisystem hosten.
- Ein oder mehrere Metadatenserver (MDSs), die Metadaten für Clients bereitstellen, die auf das Dateisystem zugreifen. Jeder MDS ist an ein Speichervolume angehängt, das als Metadatenziel (MDT) bezeichnet wird und Metadaten wie Dateinamen, Verzeichnisse, Zugriffsberechtigungen und Dateilayouts speichert.

FSx for Lustre berichtet über Metriken, mit CloudWatch denen die Leistung und Ressourcennutzung für die Speicher- und Metadatenserver Ihres Dateisystems sowie die zugehörigen Speichervolumes erfasst werden. Das folgende Diagramm zeigt ein Amazon FSx for Lustre-Dateisystem mit seinen Architekturkomponenten und den Leistungs- und CloudWatch Ressourcenmetriken, die für die Überwachung verfügbar sind.



Sie können den Bereich Überwachung und Leistung im Dashboard Ihres Dateisystems in der Amazon FSx for Lustre-Konsole verwenden, um die in den folgenden Tabellen beschriebenen Kennzahlen einzusehen. Weitere Informationen finden Sie unter Zugriff auf Metriken CloudWatch .

Dateisystemaktivität (auf der Registerkarte „Zusammenfassung“)

Wie kann ich...	Tabelle	Relevante Metriken
... die Menge der verfügbaren Speicherkapazität auf meinem Dateisystem ermitteln?	Verfügbare Speicherkapazität (Byte)	`FreeDataStorageCapacity`
... den gesamten Client-Durchsatz meines Dateisystems ermitteln?	Gesamter Client-Durchsatz (Bytes/Sekunde)	SUMME (`DataReadBytes +DataWriteBytes )`/ ZEITRAUM (in Sekunden)
... die gesamten Client-IOPS meines Dateisystems ermitteln?	Gesamtzahl der Client-IOPS (Operationen/Sekunde)	`SUM(DataReadOperations + DataWriteOperations + MetadataOperations )/PERIOD (in seconds)`
... die Anzahl der Verbindungen ermitteln, die zwischen Clients und meinem Dateiserver hergestellt werden?	Client-Verbindungen (Anzahl)	`ClientConnections`
... die Performance-Auslastung meiner Metadaten in meinem Dateisystem ermitteln?	IOPS-Auslastung von Metadaten (Prozent)	`MAX(MDT Disk IOPS)`

Registerkarte „Speicher“

Wie kann ich...	Tabelle	Relevante Metriken
... ermitteln, wie viel Speicherplatz verfügbar ist?	Verfügbare Speicherk	`FreeDataStorageCapacity`

Wie kann ich...	Tabelle	Relevante Metriken
	apazität (Byte)	
... den Prozentsatz des belegten Speichers für mein Dateisystem ermitteln, ohne Speicherplatz, der für zwischengespeicherte Schreibvorgänge auf Clients reserviert ist?	Gesamtauslastung der Speicherkapazität (Prozent)	`StorageCapacityUtilization`
... den Prozentsatz des belegten Speichers für mein Dateisystem ermitteln, einschließlich des für zwischengespeicherte Schreibvorgänge auf Clients reservierten Speicherplatzes?	Gesamtauslastung der Speicherkapazität (Prozent)	`StorageCapacityUtilizationWithCachedWrites`
... den Prozentsatz des belegten Speichers für mein Dateisystem OSTs ohne den für zwischengespeicherte Schreibvorgänge auf Clients reservierten Speicherplatz ermitteln?	Gesamtauslastung der Speicherkapazität pro OST (Prozent)	`StorageCapacityUtilization`
... den Prozentsatz des belegten Speichers für mein Dateisystem ermitteln OSTs, einschließlich des für zwischengespeicherte Schreibvorgänge auf Clients reservierten Speicherplatzes?	Gesamtauslastung der Speicherkapazität pro OST mit Zuschüssen durch Kunden (Prozent)	`StorageCapacityUtilizationWithCachedWrites`

Wie kann ich...	Tabelle	Relevante Metriken
... die Datenkomprimierungsrate meines Dateisystems ermitteln?	Einsparungen bei der Komprimierung	100* (`LogicalDiskUsage -PhysicalDiskUSage )/LogicalDiskUsage`

Leistung des Objektspeichers (auf der Registerkarte Leistung)

Wie kann ich...	Tabelle	Relevante Metriken
... den Netzwerkdurchsatz zwischen den Clients ermitteln und OSSs als Prozentsatz des bereitgestellten Limits angeben?	Netzwerkdurchsatz (Prozent)	`NetworkThroughputUtilization`
... den Festplattendurchsatz zwischen dem Betriebssystem und seinem OSTs als Prozentsatz des bereitgestellten Limits ermitteln?	Festplattendurchsatz (Prozent)	`FileServerDiskThroughputUtilization`
... die IOPS für Operationen, die Zugriff haben, OSTs als Prozentsatz des bereitgestellten Limits ermitteln?	Festplatten-IOPS (Prozent)	`DiskIopsUtilization`

Leistung der Metadaten (auf der Registerkarte Leistung)

Wie kann ich...	Tabelle	Relevante Metriken
... die prozentuale CPU-Auslastung des Metadatenservers ermitteln?	CPU-Auslastung (Prozent)	`CPUUtilization`
... die IOPS-Auslastung der Metadaten als Prozentsatz des bereitgestellten Limits ermitteln?	IOPS-Nutzung von Metadaten	`MAX(MDT Disk IOPS)`

Zugriff auf Metriken CloudWatch

Sie können auf folgende Weise auf Amazon FSx for CloudWatch Lustre-Metriken für zugreifen:

- Die Amazon FSx for Lustre-Konsole.
- Die CloudWatch Konsole.
- Die CloudWatch Befehlszeilenschnittstelle (CLI).
- Die CloudWatch API.

Die folgenden Verfahren zeigen Ihnen, wie Sie mit diesen Tools auf die Metriken zugreifen können.

Verwenden der Amazon FSx for Lustre-Konsole

So zeigen Sie Metriken mit der Amazon FSx for Lustre-Konsole an

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Navigationsbereich Dateisysteme und dann das Dateisystem aus, das die Metriken enthält, die Sie anzeigen möchten.
3. Wählen Sie auf der Übersichtsseite die Option Überwachung und Leistung aus, um die Metriken für Ihr Dateisystem anzuzeigen.

   Im Bereich Überwachung und Leistung gibt es vier Registerkarten.

   - Wählen Sie Zusammenfassung (die Standardregisterkarte), um alle aktiven Warnungen, CloudWatch Alarme und Grafiken zur Dateisystemaktivität anzuzeigen.
   - Wählen Sie Speicher, um Kennzahlen zur Speicherkapazität, Auslastung und aktive Warnungen anzuzeigen.
   - Wählen Sie Leistung, um Leistungskennzahlen für Dateiserver und Speicher sowie aktive Warnungen anzuzeigen.
   - Wählen Sie CloudWatch Alarme, um Diagramme aller für Ihr Dateisystem konfigurierten Alarme anzuzeigen.

Verwenden der CloudWatch Konsole

Um Metriken mit der CloudWatch Konsole anzuzeigen

1. Öffnen Sie die CloudWatch -Konsole.

2. Wählen Sie im Navigationsbereich Metriken aus.
3. Wählen Sie den FSx-Namespace.
4. (Optional) Geben Sie den Namen einer Metrik in das Suchfeld ein, um sie anzuzeigen.
5. (Optional) Um Metriken zu untersuchen, wählen Sie die Kategorie aus, die Ihrer Frage am besten entspricht.

Verwenden Sie den AWS CLI

Für den Zugriff auf Metriken von AWS CLI

- Verwenden Sie den Befehl `list-metrics` mit dem `--namespace "AWS/FSx"`-Namespace. Weitere Informationen finden Sie in der AWS CLI -Befehlsreferenz.

Mithilfe der CloudWatch API

Um über die CloudWatch API auf Metriken zuzugreifen

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

Kennzahlen und Dimensionen von Amazon FSx for Lustre

Amazon FSx for Lustre veröffentlicht die in den folgenden Tabellen beschriebenen Metriken im `AWS/FSx` Namespace in Amazon CloudWatch for all FSx for Lustre-Dateisysteme.

Themen

FSx für Lustre-Netzwerkmetriken I/O

Der AWS/FSx Namespace umfasst die folgenden I/O Netzwerkmetriken. Alle diese Metriken haben eine Dimension,FileSystemId.

Metrik	Beschreibung
DataReadBytes	Die Anzahl der Byte von Lesevorgängen durch Clients in das Dateisyst em. Die Sum Statistik gibt die Gesamtzahl der Byte an, die Lesevorgä ngen während des angegebenen Zeitraums zugeordnet wurden. Die Minimum Statistik gibt die Mindestanzahl von Byte an, die Lesevorgä ngen auf einer einzelnen OST zugeordnet sind. Die Maximum Statistik gibt die maximale Anzahl von Byte an, die Lesevorgängen auf der OST zugeordnet sind. Die Average Statistik gibt die durchschnittliche Anzahl von Byte an, die Lesevorgängen pro OST zugeordnet sind. Die SampleCount Statistik ist die Anzahl von. OSTs Zum Berechnen des durchschnittlichen Durchsatzes (Byte pro Sekunde) für einen Zeitraum dividieren Sie die Sum-Statistik durch die Anzahl von Sekunden in dem Zeitraum. Einheiten: • Bytes fürSum,, MinimumMaximum,Average. • Anzahl für SampleCount . Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCou nt
DataWriteBytes	Die Anzahl der Byte aus Schreibvorgängen von Clients in das Dateisyst em. Die Sum-Statistik ist die Gesamtzahl von Byte, die mit den Schreibop erationen verknüpft sind. Die Minimum Statistik gibt die Mindestanzahl von Byte an, die Schreiboperationen auf einer einzelnen OST zugeordne t sind. Die Maximum Statistik gibt die maximale Anzahl von Byte an, die

Metrik	Beschreibung
	Schreiboperationen auf der OST zugeordnet sind. Die `Average` Statistik gibt die durchschnittliche Anzahl von Byte an, die Schreiboperationen pro OST zugeordnet sind. Die `SampleCount` Statistik ist die Anzahl von. OSTs Zum Berechnen des durchschnittlichen Durchsatzes (Byte pro Sekunde) für einen Zeitraum dividieren Sie die `Sum`-Statistik durch die Anzahl von Sekunden in dem Zeitraum. Einheiten: • Bytes für`Sum`,, `Minimum``Maximum`,`Average`. • Anzahl für `SampleCount` .  Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`
`DataRead0perations`	Die Anzahl der Lesevorgänge. Die `Sum` Statistik gibt die Gesamtzahl der Lesevorgänge an. Die `Minimum` Statistik ist die Mindestanzahl von Lesevorgängen auf einem einzelnen OST. Die `Maximum` Statistik gibt die maximale Anzahl von Lesevorgängen auf dem OST an. Die `Average` Statistik gibt die durchschnittliche Anzahl von Lesevorgängen pro OST an. Die `SampleCount` Statistik ist die Anzahl von. OSTs Um die durchschnittliche Anzahl von Lesevorgängen (Operationen pro Sekunde) für einen Zeitraum zu berechnen, dividieren Sie die `Sum` Statistik durch die Anzahl der Sekunden in der Periode. Einheiten: • Zählen Sie für `Sum``Minimum`,, `Maximum``Average`,`SampleCount` .  Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Metrik	Beschreibung
`DataWrite Operations`	Die Anzahl der Schreiboperationen. Die `Sum` Statistik gibt die Gesamtzahl der Schreiboperationen an. Die `Minimum` Statistik ist die Mindestanzahl von Schreibvorgängen auf einem einzelnen OST. Die `Maximum` Statistik gibt die maximale Anzahl von Schreiboperationen auf dem OST an. Die `Average` Statistik gibt die durchschnittliche Anzahl von Schreiboperationen pro OST an. Die `SampleCount` Statistik ist die Anzahl von. OSTs Um die durchschnittliche Anzahl von Schreibvorgängen (Operationen pro Sekunde) für einen Zeitraum zu berechnen, dividieren Sie die `Sum` Statistik durch die Anzahl der Sekunden in der Periode. Einheiten: • Zählen Sie für `SumMinimum`,, `MaximumAverage`,`SampleCount` . Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Metrik	Beschreibung
`MetadataOperations`	Die Anzahl der Metadaten-Operationen. Die `Sum` Statistik gibt die Anzahl der Metadatenoperationen an. Die `Minimum` Statistik gibt die Mindestanzahl von Metadatenoperationen pro MDT an. Die `Maximum` Statistik gibt die maximale Anzahl von Metadaten operationen pro MDT an. Die `Average` Statistik gibt die durchschn ittliche Anzahl von Metadatenoperationen pro MDT an. Die `SampleCount` Statistik ist die Anzahl von. MDTs Um die durchschnittliche Anzahl von Metadatenoperationen (Operatio nen pro Sekunde) für einen Zeitraum zu berechnen, dividieren Sie die `Sum` Statistik durch die Anzahl der Sekunden in der Periode. Einheiten: • Zählen Sie für `SumMinimum`,, `MaximumAverage`,`SampleCount` . Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`
`ClientConnections`	Die Anzahl der aktiven Verbindungen zwischen Clients und dem Dateisystem. Einheit: Anzahl

FSx für Lustre-Objektspeicher-Server-Metriken

Der `AWS/FSx` Namespace umfasst die folgenden Object Storage Server (OSS) -Metriken. Alle diese Metriken haben zwei Dimensionen, `FileSystemId` und`FileServer`.

- `FileSystemId`— Die AWS Ressourcen-ID Ihres Dateisystems.
- `FileServer`— Der Name des Object Storage Servers (OSS) in Ihrem Lustre Dateisystem. Jedes OSS ist mit einem oder mehreren Objektspeicherzielen (OSTs) ausgestattet. OSS verwenden die Namenskonvention OSS< HostIndex >, wobei es sich um einen vierstelligen Hexadezimalwert *`HostIndex`* handelt (z. B.). `0SS0001` Die ID eines OSS ist die ID der ersten OST, die an sie angehängt ist. Beispielsweise wird das erste OSS, das an `0ST0000` und angeschlossen

ist`OST0001`, verwenden`OSS0000`, und das zweite OSS, an `OST0003` das angeschlossen ist`OST0002`, verwendet`OSS0002`.

Metrik	Beschreibung
`NetworkThroughputUtilization`	Netzwerkdurchsatzauslastung als Prozentsatz des verfügbaren Netzwerkdurchsatzes für Ihr Dateisystem. Diese Metrik entspricht der Summe `NetworkSentBytes` und `NetworkReceivedBytes` als Prozentsatz der Netzwerkdurchsatzkapazität eines Betriebssystems für Ihr Dateisystem. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben OSSs. Die `Average` Statistik gibt die durchschnittliche Auslastung des Netzwerkdurchsatzes für das angegebene Betriebssystem über den angegebenen Zeitraum an. Die `Minimum` Statistik gibt die niedrigste Netzwerkdurchsatzauslastung für das angegebene Betriebssystem über eine Minute für den angegebenen Zeitraum an. Die `Maximum` Statistik gibt die höchste Netzwerkdurchsatzauslastung für das angegebene Betriebssystem über eine Minute für den angegebenen Zeitraum an. Einheit: Prozent Gültige Statistiken: `Average`, `Minimum`, `Maximum`
`NetworkSentBytes`	Die Anzahl der vom Dateisystem gesendeten Byte. Der gesamte Datenverkehr wird in dieser Metrik berücksichtigt, einschließlich Datenbewegungen zu und von verknüpften Datenrepositorien. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben. OSSs

Metrik	Beschreibung
	Die `Sum` Statistik ist die Gesamtzahl der Byte, die von dem angegebenen Betriebssystem im angegebenen Zeitraum über das Netzwerk gesendet wurden. Die `Average` Statistik ist die durchschnittliche Anzahl der Byte, die von dem angegebenen Betriebssystem im angegebenen Zeitraum über das Netzwerk gesendet wurden. Die `Minimum` Statistik ist die niedrigste Anzahl von Byte, die von dem angegebenen Betriebssystem im angegebenen Zeitraum über das Netzwerk gesendet wurden. Die `Maximum` Statistik gibt die höchste Anzahl von Byte an, die von dem angegebenen Betriebssystem im angegebenen Zeitraum über das Netzwerk gesendet wurden. Um den gesendeten Durchsatz (Byte pro Sekunde) für eine Statistik zu berechnen, dividieren Sie die Statistik durch die Sekunden im angegebenen Zeitraum. Einheit: Byte Gültige Statistiken:`Sum`,, `Average` `Minimum` `Maximum`

Metrik	Beschreibung
`NetworkReceivedBytes`	Die Anzahl der vom Dateisystem empfangenen Byte. Der gesamte Datenverkehr wird in dieser Metrik berücksic htigt, einschließlich Datenbewegungen zu und von verknüpften Datenrepositorien. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben. OSSs Die `Sum` Statistik ist die Gesamtzahl der Byte, die das angegebene Betriebssystem im angegebenen Zeitraum über das Netzwerk empfangen hat. Die `Average` Statistik ist die durchschnittliche Anzahl der Byte, die das angegebene OSS im angegebenen Zeitraum über das Netzwerk empfangen hat. Die `Minimum` Statistik gibt die niedrigste Anzahl von Byte an, die das angegebene Betriebssystem im angegeben en Zeitraum über das Netzwerk empfangen hat. Die `Maximum` Statistik gibt die höchste Anzahl von Byte an, die das angegebene Betriebssystem im angegeben en Zeitraum über das Netzwerk empfangen hat. Um den Durchsatz (Byte pro Sekunde) für eine Statistik zu berechnen, dividieren Sie die Statistik durch die Sekunden im angegebenen Zeitraum. Einheit: Byte Gültige Statistiken:`Sum`,,, `Average` `Minimum` `Maximum`

Metrik	Beschreibung
`FileServerDiskThroughputUtilization`	Der Festplattendurchsatz zwischen Ihrem Betriebssystem und dem zugehörigen OSTs Betriebssystem als Prozentsatz des bereitgestellten Limits, der durch die Durchsatzkapazität bestimmt wird. Diese Metrik entspricht der Summe `DiskReadBytes` und `DiskWriteBytes` als Prozentsatz der Festplattendurchsatzkapazität des OSS für Ihr Dateisystem. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben OSSs. Die `Average` Statistik gibt die durchschnittliche Auslastung des OSS-Festplattendurchsatzes für das angegebene Betriebssystem im angegebenen Zeitraum an. Die `Minimum` Statistik gibt die niedrigste OSS-Festplattendurchsatzauslastung für das angegebene Betriebssystem im angegebenen Zeitraum an. Die `Maximum` Statistik gibt die höchste OSS-Festplattendurchsatzauslastung für das angegebene Betriebssystem im angegebenen Zeitraum an. Einheit: Prozent Gültige Statistiken: `Average`, `Minimum`, `Maximum`

FSx für Zielmetriken für Lustre-Objektspeicher

Der `AWS/FSx` Namespace umfasst die folgenden Messwerte für Object Storage Target (OST). Alle diese Metriken haben zwei Dimensionen, `FileSystemId` und`StorageTargetId`.

> **Note**
>
> `DiskReadOperations`und `DiskWriteOperations` Metriken sind auf Scratch-Dateisystemen nicht verfügbar, und `DiskIopsUtilization` Metriken sind auf Scratch- und Persistent HDD-Dateisystemen nicht verfügbar.

Metrik	Beschreibung
`DiskReadBytes`	Die Anzahl der Byte (Festplatten-IO) von allen Festplatten-Lesevo rgängen aus dieser OST-Datei. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben OSTs. Die `Sum` Statistik ist die Gesamtzahl der Byte, die innerhalb einer Minute aus dem angegebenen OST im angegebenen Zeitraum gelesen wurden. Die `Average` Statistik gibt die durchschnittliche Anzahl der Byte an, die im angegebenen Zeitraum pro Minute aus dem angegebenen OST gelesen wurden. Die `Minimum` Statistik ist die niedrigste Anzahl von Byte, die jede Minute aus dem angegebenen OST im angegebenen Zeitraum gelesen wurden. Die `Maximum` Statistik gibt die höchste Anzahl von Byte an, die im angegebenen Zeitraum pro Minute aus dem angegebenen OST gelesen wurden. Um den Lesefestplattendurchsatz (Byte pro Sekunde) für eine beliebige Statistik zu berechnen, dividieren Sie die Statistik durch die Sekunden innerhalb des Zeitraums. Einheit: Byte Gültige Statistiken:`Sum`,`Average`, und`Minimum`, `Maximum`
`DiskWriteBytes`	Die Anzahl der Byte (Festplatten-IO) von allen Festplatten-Schrei bvorgängen aus dieser OST-Datei. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben OSTs.

Metrik	Beschreibung
	Die `Sum` Statistik ist die Gesamtzahl der Byte, die jede Minute über den angegebenen Zeitraum aus dem angegebenen OST geschrieben wurden. Die `Average` Statistik ist die durchschnittliche Anzahl der Byte, die jede Minute aus dem angegebenen OST im angegebenen Zeitraum geschrieben wurden. Die `Minimum` Statistik ist die niedrigste Anzahl von Byte, die jede Minute aus dem angegebenen OST im angegebenen Zeitraum geschrieben wurden. Bei der `Maximum` Statistik handelt es sich um die höchste Anzahl von Byte, die jede Minute aus dem angegebenen OST im angegebenen Zeitraum geschrieben wurden. Um den Lesefestplattendurchsatz (Byte pro Sekunde) für eine beliebige Statistik zu berechnen, dividieren Sie die Statistik durch die Sekunden innerhalb des Zeitraums Einheit: Byte Gültige Statistiken:`Sum`,`Average`, und`Minimum`, `Maximum`

Metrik	Beschreibung
`DiskRead0 perations`	Die Anzahl der Lesevorgänge (Festplatten-IO) für diese OST. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben OSTs. Die `Sum` Statistik gibt die Gesamtzahl der Lesevorgänge an, die von der angegebenen OST im angegebenen Zeitraum ausgeführt wurden. Die `Average` Statistik ist die durchschnittliche Anzahl der Lesevorgä nge, die jede Minute von der angegebenen OST im angegebenen Zeitraum ausgeführt wurden. Die `Minimum` Statistik gibt die niedrigste Anzahl von Lesevorgängen an, die jede Minute von der angegebenen OST im angegebenen Zeitraum ausgeführt wurden. Die `Maximum` Statistik gibt die höchste Anzahl von Lesevorgängen an, die jede Minute von der angegebenen OST im angegebenen Zeitraum ausgeführt wurden. Verwenden Sie die `Average` Statistik und dividieren Sie das Ergebnis durch 60 (Sekunden), um die durchschnittlichen Festplatten-IOPS über den Zeitraum zu berechnen. Einheiten: Anzahl Gültige Statistiken:`Sum`,`Average`, und `Minimum` `Maximum`

Metrik	Beschreibung
`DiskWriteOperations`	Die Anzahl der Schreibvorgänge (Festplatten-IO) auf diese OST-Datei. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben OSTs. Die `Sum` Statistik gibt die Gesamtzahl der Schreiboperationen an, die vom angegebenen OST im angegebenen Zeitraum ausgeführt wurden. Die `Average` Statistik ist die durchschnittliche Anzahl von Schreibvorgängen, die jede Minute von der angegebenen OST im angegebenen Zeitraum ausgeführt wurden. Die `Minimum` Statistik gibt die niedrigste Anzahl von Schreibvorgängen an, die jede Minute vom angegebenen OST im angegebenen Zeitraum ausgeführt wurden. Die `Maximum` Statistik gibt die höchste Anzahl von Schreibvorgängen an, die jede Minute von der angegebenen OST im angegebenen Zeitraum ausgeführt wurden. Verwenden Sie die `Average` Statistik und dividieren Sie das Ergebnis durch 60 (Sekunden), um die durchschnittlichen Festplatten-IOPS über den Zeitraum zu berechnen. Einheiten: Anzahl Gültige Statistiken:`Sum`,`Average`, und `Minimum` `Maximum`

Metrik	Beschreibung
`DiskIopsU tilization`	Die Festplatten-IOPS-Auslastung eines OST als Prozentsatz des Festplatten-IOPS-Limits des OST. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben. OSTs Die `Average` Statistik gibt die durchschnittliche Festplatten-IOPS-A uslastung für das angegebene OST im angegebenen Zeitraum an. Die `Minimum` Statistik gibt die niedrigste Festplatten-IOPS-Auslastung für den angegebenen OST im angegebenen Zeitraum an. Die `Maximum` Statistik gibt die höchste Festplatten-IOPS-Auslastung für den angegebenen OST im angegebenen Zeitraum an. Einheit: Prozent Gültige Statistiken:`Average`,, und `Minimum` `Maximum`

FSx für Lustre-Metadatenmetriken

Der `AWS/FSx` Namespace umfasst die folgenden Metadaten-Metriken. Die `CPUUtilization` Metrik verwendet die `FileServer` Dimensionen `FileSystemId` und, während die anderen Metriken die `StorageTargetId` Dimensionen `FileSystemId` und verwenden.

- `FileSystemId`— Die AWS Ressourcen-ID Ihres Dateisystems.
- `StorageTargetId`— Der Name des Metadatenziels (MDT). MDTs verwendet die Namenskonvention von MDT< MDTIndex > (zum Beispiel). `MDT0001`
- `FileServer`— Der Name des Metadatenservers (MDS) in Ihrem Lustre Dateisystem. Jeder MDS ist mit einem Metadatenziel (MDT) ausgestattet. MDS verwenden die Namenskonvention MDS< HostIndex >, wobei es sich um einen vierstelligen Hexadezimalwert `HostIndex` handelt, der anhand des MDT-Index auf dem Server abgeleitet wird. Beispielsweise `MDT0000` wird das erste MDS, mit dem bereitgestellt wurde, verwendet, und das zweite MDS, mit dem bereitgestellt wurde`MDS0000`, verwendet. `MDT0001` `MDS0001` Ihr Dateisystem enthält mehrere Metadatenserver, wenn für Ihr Dateisystem eine Metadatenkonfiguration angegeben ist.

Metrik	Beschreibung
`CPUUtilization`	Die prozentuale Auslastung der MDS-CPU-Ressourcen Ihres Dateisystems. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben. MDSs Die `Average` Statistik gibt die durchschnittliche CPU-Auslastung des MDS über einen bestimmten Zeitraum an. Die `Minimum` Statistik gibt die niedrigste CPU-Auslastung für das angegebene MDS über den angegebenen Zeitraum an. Die `Maximum` Statistik gibt die höchste CPU-Auslastung für das angegebene MDS im angegebenen Zeitraum an. Einheit: Prozent Gültige Statistiken:`Average`, und `Minimum` `Maximum`
`FileCreateOperations`	Gesamtzahl der Dateierstellungsvorgänge. Einheit: Anzahl
`FileOpenOperations`	Gesamtzahl der Operationen zum Öffnen von Dateien. Einheit: Anzahl
`FileDeleteOperations`	Gesamtzahl der Dateilöschvorgänge. Einheit: Anzahl
`StatOperations`	Gesamtzahl der Statistikoperationen. Einheit: Anzahl

Metrik	Beschreibung
`RenameOperations`	Gesamtzahl der Verzeichnisumbenennungen, unabhängig davon, ob es sich um direkte oder verzeichnisübergreifende Umbenennungen handelt. Einheit: Anzahl

FSx für Lustre-Metriken zur Speicherkapazität

Der `AWS/FSx` Namespace umfasst die folgenden Messwerte zur Speicherkapazität. Alle diese Metriken haben zwei Dimensionen, `FileSystemId` und zwar `StorageTargetId` außer `LogicalDiskUsage` und `PhysicalDiskUsage` welche haben die `FileSystemId` Dimension.

Metrik	Beschreibung
`FreeDataStorageCapacity`	Die Menge der verfügbaren Speicherkapazität in dieser OST. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben OSTs. Die `Sum` Statistik ist die Gesamtzahl der Byte, die in der angegebenen OST über den angegebenen Zeitraum verfügbar sind. Die `Average` Statistik ist die durchschnittliche Anzahl der in der angegebenen OST im angegebenen Zeitraum verfügbaren Byte. Die `Minimum` Statistik ist die niedrigste Anzahl von Byte, die in der angegebenen OST über den angegebenen Zeitraum verfügbar sind. Die `Maximum` Statistik gibt die höchste Anzahl von Byte an, die in der angegebenen OST über den angegebenen Zeitraum verfügbar sind. Einheit: Byte

Metrik	Beschreibung
	Gültige Statistiken:`Sum`, `AverageMinimum`, und `Maximum`
`StorageCapacityUtilization`	Die Auslastung der Speicherkapazität für ein bestimmte s Dateisystem (OST). Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben OSTs. Die `Average` Statistik gibt die durchschnittliche Auslastung der Speicherkapazität für ein bestimmtes OST über einen bestimmten Zeitraum an. Die `Minimum` Statistik gibt die Mindestauslastung der Speicherkapazität für eine bestimmte OST über einen bestimmten Zeitraum an. Die `Maximum` Statistik gibt die maximale Auslastung der Speicherkapazität für eine bestimmte OST über einen bestimmten Zeitraum an. Einheit: Prozent Gültige Statistiken: `Average`, `Minimum`, `Maximum`

Metrik	Beschreibung
`StorageCapacityUtilizationWithCachedWrites`	Die Speicherkapazitätsauslastung für ein bestimmtes Dateisystem (OST), einschließlich des für zwischeng espeicherte Schreibvorgänge auf dem Client reservier ten Speicherplatzes. Jede Minute wird für jedes Ihrer Dateisysteme eine Metrik ausgegeben. OSTs Die `Average` Statistik gibt die durchschnittliche Auslastung der Speicherkapazität für ein bestimmtes OST über einen bestimmten Zeitraum an. Die `Minimum` Statistik gibt die Mindestauslastung der Speicherkapazität für eine bestimmte OST über einen bestimmten Zeitraum an. Die `Maximum` Statistik gibt die maximale Auslastung der Speicherkapazität für eine bestimmte OST über einen bestimmten Zeitraum an. Einheit: Prozent Gültige Statistiken: `Average`, `Minimum`, `Maximum`

Metrik	Beschreibung
`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 geringste Anzahl logischer Byte, die in einem OST im Dateisystem gespeichert sind. Die `Maximum` Statistik ist die größte Anzahl logischer Byte, die in einem OST im Dateisystem gespeichert sind. Die `Average` Statistik gibt die durchschnittliche Anzahl der pro OST gespeicherten logischen Byte an. Die `SampleCount` Statistik ist die Anzahl von. OSTs Einheiten: • Bytes für`Sum`,`Minimum`,`Maximum`. • Anzahl für `SampleCount` . Gültige Statistiken: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Metrik	Beschreibung
PhysicalDiskUsage	Die Menge an Speicherplatz, die physisch von Dateisyst emdaten belegt wird (komprimiert). Die Sum Statistik gibt die Gesamtzahl der OSTs im Dateisystem belegten Byte an. Die Minimum Statistik gibt die Gesamtzahl der in der entleertesten OST belegten Byte an. Die Maximum Statistik gibt die Gesamtzahl der in der vollständigsten OST belegten Byte an. Die Average Statistik gibt die durchschnittliche Anzahl der pro OST belegten Byte an. Die SampleCount Statistik ist die Anzahl von. OSTs Einheiten: • Bytes fürSum,Minimum,Maximum. • Anzahl für SampleCount . Gültige Statistiken: Sum, Minimum, Maximum, Average, SampleCount

FSx für Lustre S3-Repository-Metriken

FSx for Lustre veröffentlicht die folgenden AutoImport (automatischer Import) und AutoExport (automatischer Export) Metriken im FSx Namespace in. CloudWatch Diese Metriken verwenden Dimensionen, um detailliertere Messungen Ihrer Daten zu ermöglichen. Alle AutoImport AutoExport Metriken haben die Publisher Dimensionen FileSystemId und.

Metrik	Beschreibung
AgeOfOldestQueuedMessage Dimension: AutoExport	Das Alter der ältesten Nachricht in Sekunden, die darauf wartet, exportiert zu werden. Die Average Statistik gibt das Durchschn ittsalter der ältesten Nachricht an, die auf den

Metrik	Beschreibung
	Export wartet. Die `Maximum` Statistik gibt an, wie viele Sekunden eine Nachricht maximal in der Exportwarteschlange verweilte. Die `Minimum` Statistik gibt an, wie viele Sekunden eine Nachricht mindestens in der Exportwarteschlange verweilte. Ein Wert von Null gibt an, dass keine Nachrichten darauf warten, exportiert zu werden. Einheiten: Sekunden Gültige Statistiken: `Average`, `Minimum`, `Maximum`

Metrik	Beschreibung
`RepositoryRenameOperations` Dimension: `AutoExport`	Die Anzahl der Umbenennungen, die vom Dateisystem als Reaktion auf eine größere Verzeichnisumbenennung verarbeitet wurden. Die `Sum` Statistik gibt die Gesamtzahl der Umbenennungsvorgänge an, die sich aus einer Verzeichnisumbenennung ergeben. Die `Average` Statistik gibt die durchschn ittliche Anzahl von Umbenennungsvorgän gen für das Dateisystem an. Die `Maximum` Statistik gibt die maximale Anzahl von Umbenennungsvorgängen an, die mit einer Verzeichnisumbenennung im Dateisystem verbunden sind. Die `Minimum` Statistik gibt die Mindestanzahl von Umbenennungen an, die mit einer Verzeichnisumbenennung im Dateisystem verknüpft sind. Einheiten: Anzahl Gültige Statistiken:`Sum`,,`Average`, `Minimum` `Maximum`

Metrik	Beschreibung
`AgeOfOldestQueuedMessage` Dimension: `AutoImport`	Das Alter der ältesten Nachricht in Sekunden, die darauf wartet, importiert zu werden. Die `Average` Statistik gibt das Durchschn ittsalter der ältesten Nachricht an, die darauf wartet, importiert zu werden. Die `Maximum` Statistik gibt an, wie viele Sekunden eine Nachricht maximal in der Importwarteschlang e verweilte. Die `Minimum` Statistik gibt an, wie viele Sekunden eine Nachricht mindestens in der Importwarteschlange gelebt hat. Ein Wert von Null gibt an, dass keine Nachrichten darauf warten, importiert zu werden. Einheiten: Sekunden Gültige Statistiken: `Average`, `Minimum`, `Maximum`

FSx für Lustre-Dimensionen

Amazon FSx for Lustre-Metriken verwenden den `AWS/FSx` Namespace und verwenden die folgenden Dimensionen.

- Die `FileSystemId` Dimension gibt die ID eines Dateisystems an und filtert die Metriken, die Sie für dieses einzelne Dateisystem anfordern. Sie finden die ID auf der FSx Amazon-Konsole im Bereich Zusammenfassung auf der Seite mit den Dateisystemdetails im Feld Dateisystem-ID. Die Dateisystem-ID hat die Form von*fs-01234567890123456*. Sie können die ID auch in der Antwort auf einen `describe-file-systems`CLI-Befehl sehen (die entsprechende API-Aktion ist `DescribeFileSystems`).
- Die `StorageTargetId` Dimension gibt an, welches OST (Object Storage Target) oder MDT (Metadatenziel) die Metadaten-Metriken veröffentlicht hat. A `StorageTargetId` hat die Form von `OSTxxxx` (zum Beispiel`OST0001`) oder `MDTxxxx` (zum Beispiel`MDT0001`).

- Die `FileServer` Dimension bezeichnet Folgendes
  - Für OSS-Metriken: der Name des Object Storage Servers (OSS). OSS verwenden die `OSSxxxx` Namenskonvention (z. B.`OSS0002`).
  - Für die CPUUtilization Metrik: der Name eines Metadatenservers (MDS). MDS verwendet die `MDSxxxx` Namenskonvention (z. B.`MDS0002`).
- Die `Publisher` Dimension ist in CloudWatch und AWS CLI für die `AutoImport` Metriken und verfügbar `AutoImport` und gibt an, welcher Service die Metriken veröffentlicht hat.

Weitere Informationen zu Abmessungen finden Sie unter Abmessungen im CloudWatch Amazon-Benutzerhandbuch.

Leistungswarnungen und Empfehlungen

FSx for Lustre zeigt eine Warnung für CloudWatch Messwerte an, wenn sich eine dieser Metriken für mehrere aufeinanderfolgende Datenpunkte einem festgelegten Schwellenwert nähert oder diesen überschreitet. Diese Warnungen bieten Ihnen umsetzbare Empfehlungen, mit denen Sie die Leistung Ihres Dateisystems optimieren können.

Auf Warnungen kann in verschiedenen Bereichen des Überwachungs- und Leistungs-Dashboards der Amazon FSx for Lustre-Konsole zugegriffen werden. Alle aktiven oder aktuellen FSx Amazon-Leistungswarnungen und CloudWatch Alarme, die für das Dateisystem konfiguriert wurden und sich im Alarmstatus befinden, werden im Bereich Überwachung und Leistung im Abschnitt Zusammenfassung angezeigt. Die Warnung wird auch in dem Bereich des Dashboards angezeigt, in dem das Metrikdiagramm angezeigt wird. Diese Warnungen werden 24 Stunden, nachdem die zugrunde liegenden Metriken den Warnschwellenwert unterschritten haben, automatisch aus dem Dashboard ausgeblendet.

Sie können CloudWatch Alarme für jede der FSx Amazon-Metriken erstellen. Weitere Informationen finden Sie unter CloudWatch Alarme zur Überwachung von Messwerten erstellen.

Verwenden Sie Leistungswarnungen, um die Leistung des Dateisystems zu verbessern

Amazon FSx bietet umsetzbare Empfehlungen, mit denen Sie die Leistung Ihres Dateisystems optimieren können. Sie können die empfohlenen Maßnahmen ergreifen, wenn Sie davon ausgehen, dass das Problem weiterhin besteht oder wenn es die Leistung Ihres Dateisystems beeinträchtigt. Je nachdem, welche Metrik eine Warnung ausgelöst hat, können Sie diese beheben, indem Sie die

Durchsatzkapazität, Speicherkapazität oder Metadaten-IOPS des Dateisystems erhöhen, wie in der folgenden Tabelle beschrieben.

Abschnitt „Dashboard“	Wenn es für diese Metrik eine Warnung gibt	Vorgehensweise
Speicher	`Storage capacity utilization`	Erhöhen Sie die Speicherkapazität Ihres Dateisystems. Wenn Ihre Speicherkapazitätsauslastung nur für einen Teil der Object Storage-Ziele (OSTs) Ihres Dateisystems höher ist, können Sie auch Ihre Arbeitslast neu verteilen, sodass Ihre Speicherkapazitätsauslastung in Ihrem gesamten Dateisystem gleichmäßiger ist.
	`Storage capacity utilization with cached writes`	Reduzieren Sie die Größe Ihres Client-Schreibcaches, indem Sie den Parameter max_dirty_mb auf Ihren Clients konfigurieren.
Leistung des Objektspeichers	`Network throughput`	Erhöhen Sie die Durchsatzkapazität Ihres Dateisystems. Wenn Ihre Durchsatzauslastung für eine Teilmenge der Objektspeicherserver (OSSs) Ihres Dateisystems höher ist, können Sie auch Ihre Arbeitslast neu verteilen, sodass Ihre Durchsatzauslastung im gesamten Dateisystem gleichmäßiger ist.

Abschnitt „Dashboard“	Wenn es für diese Metrik eine Warnung gibt	Vorgehensweise
	`Disk throughput`	Erhöhen Sie die Durchsatzkapazität Ihres Dateisystems. Wenn Ihre Festplattendurchsatzauslastung für eine Teilmenge der Objektspeicherserver (OSSs) Ihres Dateisystems höher ist, können Sie auch Ihre Arbeitslast neu verteilen, sodass Ihre Festplattendurchsatzauslastung gleichmäßiger über das gesamte Dateisystem verteilt wird.
	`Disk IOPS`	Erhöhen Sie die Speicherkapazität Ihres Dateisystems. Wenn Ihre Festplatten-IOPS-Auslastung für einen Teil der Objektspeicherziele (OSTs) Ihres Dateisystems höher ist, können Sie auch Ihre Arbeitslast neu verteilen, sodass Ihre Festplatten-IOPS-Auslastung gleichmäßiger im gesamten Dateisystem verteilt wird.

Abschnitt „Dashboard“	Wenn es für diese Metrik eine Warnung gibt	Vorgehensweise
Leistung der Metadaten	`CPU utilization`	Erhöhen Sie die Speicherkapazität Ihres Dateisystems. Wenn Sie die Leistung von Metadaten unabhängig von der Speicherkapazität skalieren möchten, können Sie mithilfe des MetadataConfiguration Parameters zu einem neuen Dateisystem migrieren, das die Bereitstellung von Metadaten leistung unabhängig von der Speicherkapazität unterstützt.
	`Metadata IOPS`	Erhöhen Sie die Metadaten-IOPS Ihres Dateisystems.

Weitere Informationen zur Dateisystemleistung finden Sie unterLeistung von Amazon FSx for Lustre.

CloudWatch Alarme zur Überwachung von Messwerten erstellen

Sie können einen CloudWatch Alarm erstellen, der eine Amazon SNS SNS-Nachricht sendet, wenn sich der Status des Alarms ändert. Ein Alarm überwacht eine einzelne Metrik über einen von Ihnen angegebenen Zeitraum und führt eine oder mehrere Aktionen aus, die auf dem Wert der Metrik im Verhältnis zu einem bestimmten Schwellenwert über einen bestimmten Zeitraum basieren. Die Aktion ist eine Benachrichtigung, die an ein Amazon SNS-Thema oder eine Auto Scaling-Richtlinie gesendet wird.

Alarme lösen nur Aktionen für anhaltende Statusänderungen aus. CloudWatch Alarme lösen keine Aktionen aus, da sie sich in einem bestimmten Zustand befinden. Der Status muss sich ändern und für einen bestimmten Zeitraum geändert bleiben. Sie können einen Alarm auf der FSx Amazon-Konsole oder der CloudWatch Konsole erstellen.

Die folgenden Verfahren beschreiben, wie Sie mithilfe der Konsole, und der API Alarme FSx für Amazon for Lustre erstellen. AWS CLI

So richten Sie Alarme mit der Amazon FSx for Lustre-Konsole ein

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Navigationsbereich Dateisysteme und dann das Dateisystem aus, für das Sie den Alarm erstellen möchten.
3. Wählen Sie auf der Übersichtsseite die Option Überwachung und Leistung aus.
4. Wählen Sie „ CloudWatch Alarm erstellen“. Sie werden zur CloudWatch-Konsole umgeleitet.
5. Wählen Sie Metriken auswählen und dann Weiter.
6. Wählen Sie im Abschnitt Metriken die Option FSX aus.
7. Wählen Sie Dateisystem-Metriken, wählen Sie die Metrik aus, für die Sie den Alarm einstellen möchten, und wählen Sie dann Metrik auswählen.
8. Wählen Sie im Abschnitt „Bedingungen“ die Bedingungen für den Alarm aus und klicken Sie auf Weiter.

   > **Note**
   >
   > Während der Wartung des Dateisystems werden Metriken möglicherweise nicht veröffentlicht. 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 der Behandlung fehlender Daten durch CloudWatch Alarme.

9. Wenn Sie Ihnen eine E-Mail oder eine SNS-Benachrichtigung senden möchten CloudWatch , wenn der Alarmstatus die Aktion auslöst, wählen Sie Wann immer dieser Alarmstatus ist.

   Wählen Sie für Wählen Sie ein SNS-Thema aus ein vorhandenes SNS-Thema aus. Wenn Sie Create topic auswählen, können Sie den Namen und die E-Mail Adressen für eine neue E-Mail-Abonnementliste einrichten. Diese Liste wird gespeichert und erscheint für künftige Alarme in der Liste. Wählen Sie Weiter aus.

   > **Warning**
   >
   > Wenn Sie Create topic (Thema erstellen) verwenden, um ein neues Amazon-SNS-Thema einzurichten, müssen die E-Mail Adressen überprüft werden, bevor die

Empfänger Benachrichtigungen erhalten. E-Mail Nachrichten werden nur gesendet, wenn der Alarm in einen Alarmzustand wechselt. Wenn es zu dieser Änderung des Alarmzustands kommt, bevor die E-Mail Adressen überprüft wurden, erhalten die Empfänger keine Benachrichtigung.

10. Geben Sie die Werte Name, Beschreibung und Whenever für die Metrik ein und klicken Sie auf Weiter.
11. Überprüfen Sie auf der Seite „Vorschau und Erstellung“ den Alarm und wählen Sie „Alarm erstellen“.

So richten Sie Alarme mithilfe der CloudWatch Konsole ein

1. Melden Sie sich bei der an AWS-Managementkonsole und öffnen Sie die CloudWatch Konsole unter https://console.aws.amazon.com/cloudwatch/.
2. Wählen Sie „Alarm erstellen“, um den Assistenten zum Erstellen von Alarmen zu starten.
3. Wählen Sie FSx Metriken, um nach einer Metrik zu suchen. Um die Ergebnisse einzugrenzen, können Sie nach Ihrer Dateisystem-ID suchen. Wählen Sie die Metrik aus, für die Sie einen Alarm erstellen möchten, und klicken Sie auf Weiter.
4. Geben Sie einen Namen und eine Beschreibung ein und wählen Sie einen Whenevere-Wert für die Metrik aus.
5. Wenn Sie Ihnen eine E-Mail senden CloudWatch möchten, wenn der Alarmstatus erreicht ist, wählen Sie State is ALARM für Wann immer dieser Alarm erreicht ist. Wählen Sie unter Benachrichtigung senden an: ein vorhandenes SNS-Thema aus. Wenn Sie Thema erstellen auswählen, können Sie die Namen und E-Mail-Adressen für eine neue E-Mail-Abonnementliste einrichten. Diese Liste wird gespeichert und erscheint für künftige Alarme in der Liste.

> **Warning**
>
> Wenn Sie Create topic (Thema erstellen) verwenden, um ein neues Amazon-SNS-Thema einzurichten, müssen die E-Mail Adressen überprüft werden, bevor die Empfänger Benachrichtigungen erhalten. E-Mail Nachrichten werden nur gesendet, wenn der Alarm in einen Alarmzustand wechselt. Wenn es zu dieser Änderung des Alarmzustands kommt, bevor die E-Mail Adressen überprüft wurden, erhalten die Empfänger keine Benachrichtigung.

6. Sehen Sie sich die Alarmvorschau an und wählen Sie dann Alarm erstellen oder gehen Sie zurück, um Änderungen vorzunehmen.

Um einen Alarm einzustellen, verwenden Sie AWS CLI

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

Um einen Alarm einzustellen mit dem CloudWatch

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

Protokollierung mit Amazon CloudWatch Logs

FSx for Lustre unterstützt die Protokollierung von Fehler- und Warnereignissen für Datenrepositorys, die mit Ihrem Dateisystem verknüpft sind, in Amazon CloudWatch Logs.

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

Themen

Überblick über die Protokollierung

Wenn Sie Datenrepositorys mit Ihrem FSx for Lustre-Dateisystem verknüpft haben, können Sie die Protokollierung von Datenrepository-Ereignissen in Amazon CloudWatch Logs aktivieren. Fehler- und Warnereignisse können für Import-, Export- und Wiederherstellungsereignisse protokolliert werden.

Weitere Informationen zu diesen Vorgängen und zur Verknüpfung mit Datenrepositorys finden Sie unterVerwenden von Datenrepositorys mit Amazon FSx for Lustre.

Sie können die Protokollebenen konfigurieren, die Amazon FSx protokolliert, d. h., ob Amazon FSx nur Fehlerereignisse, nur Warnereignisse oder sowohl Fehler- als auch Warnereignisse protokolliert. Sie können die Ereignisprotokollierung auch jederzeit deaktivieren.

> **Note**
>
> Es wird dringend empfohlen, Protokolle für Dateisysteme zu aktivieren, mit denen ein gewisses Maß an kritischer Funktionalität verknüpft ist.

Ziele protokollieren

Wenn die Protokollierung aktiviert ist, muss FSx for Lustre mit einem Amazon CloudWatch Logs-Ziel konfiguriert werden. Das Ereignisprotokollziel ist eine Amazon CloudWatch Logs-Protokollgruppe, und Amazon FSx erstellt innerhalb dieser Protokollgruppe einen Protokollstream für Ihr Dateisystem. CloudWatch Mit Logs können Sie Audit-Ereignisprotokolle in der CloudWatch Amazon-Konsole speichern, anzeigen und durchsuchen, mithilfe von Logs Insights Abfragen zu den CloudWatch Protokollen ausführen und CloudWatch Alarme oder Lambda-Funktionen auslösen.

Sie wählen das Protokollziel bei der Erstellung Ihres FSx for Lustre-Dateisystems oder danach, indem Sie es aktualisieren. Weitere Informationen finden Sie unter Verwaltung der Protokollierung.

Standardmäßig erstellt und verwendet Amazon FSx eine CloudWatch Standard-Logs-Protokollgruppe in Ihrem Konto als Ziel für das Ereignisprotokoll. Wenn Sie eine benutzerdefinierte CloudWatch Protokollgruppe als Ziel für das Ereignisprotokoll verwenden möchten, gelten die folgenden Anforderungen für den Namen und den Speicherort des Ziels für das Ereignisprotokoll:

- Der Name der CloudWatch Logs-Protokollgruppe muss mit dem `/aws/fsx/` Präfix beginnen.
- Wenn Sie beim Erstellen oder Aktualisieren eines Dateisystems auf der Konsole keine bestehende CloudWatch Logs-Protokollgruppe haben, kann Amazon FSx for Lustre einen Standard-Log-Stream in der CloudWatch `/aws/fsx/lustre` Logs-Protokollgruppe erstellen und verwenden. Der Protokollstream wird mit dem folgenden Format erstellt `datarepo_`*`file_system_id`* (z. B.`datarepo_fs-0123456789abcdef0`).
- Wenn Sie die Standard-Protokollgruppe nicht verwenden möchten, können Sie über die Konfigurationsoberfläche eine CloudWatch Logs-Protokollgruppe erstellen, wenn Sie Ihr Dateisystem auf der Konsole erstellen oder aktualisieren.

- Die CloudWatch Zielprotokollgruppe muss sich in derselben AWS Partition und AWS-Konto wie Ihr Amazon FSx for Lustre-Dateisystem befinden. AWS-Region

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

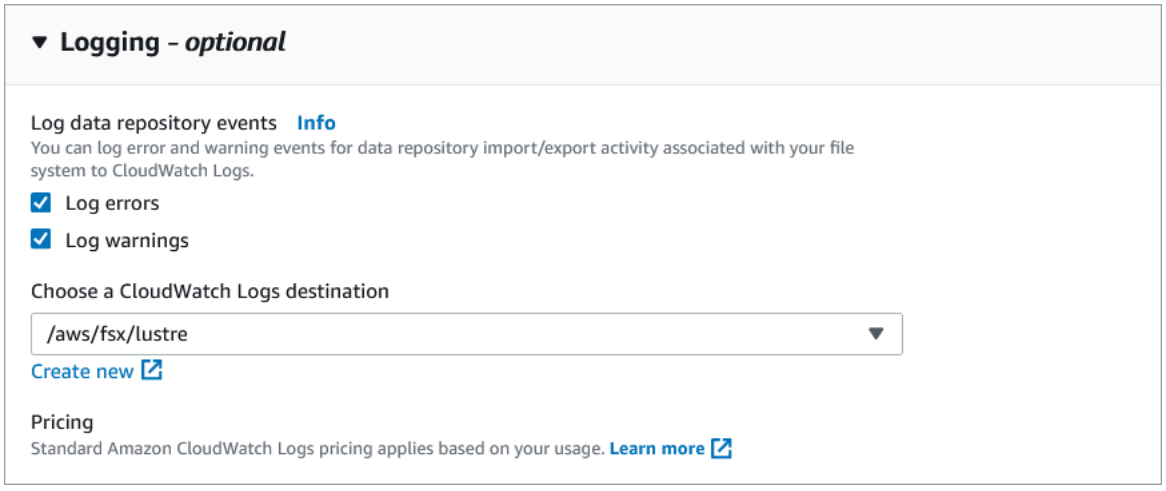
Verwaltung der Protokollierung

Sie können die Protokollierung aktivieren, wenn Sie ein neues Dateisystem FSx für Lustre erstellen oder es anschließend aktualisieren. Die Protokollierung ist standardmäßig aktiviert, wenn Sie ein Dateisystem von der FSx Amazon-Konsole aus erstellen. Die Protokollierung ist jedoch standardmäßig deaktiviert, wenn Sie ein Dateisystem mit der AWS CLI oder der FSx Amazon-API erstellen.

In vorhandenen Dateisystemen, für die die Protokollierung aktiviert ist, können Sie die Einstellungen für die Ereignisprotokollierung ändern, einschließlich der Protokollebene, für die Ereignisse protokolliert werden sollen, und des Protokollziels. Sie können diese Aufgaben mit der FSx Amazon-Konsole oder der FSx Amazon-API ausführen. AWS CLI

Um die Protokollierung beim Erstellen eines Dateisystems (Konsole) zu aktivieren

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



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

Wenn das Dateisystem verfügbar wird, wird die Protokollierung aktiviert.

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

1. Verwenden Sie beim Erstellen eines neuen Dateisystems die `LogConfiguration` Eigenschaft zusammen mit dem CreateFileSystemVorgang, um die Protokollierung für das neue Dateisystem zu aktivieren.

   ```
   create-file-system --file-system-type LUSTRE \
       --storage-capacity 1200 --subnet-id subnet-08b31917a72b548a9  \
       --lustre-configuration "LogConfiguration={Level=WARN_ERROR, \
           Destination="arn:aws:logs:us-east-1:234567890123:log-group:/aws/fsx/
   testEventLogging"}"
   ```

2. Wenn das Dateisystem verfügbar wird, wird die Protokollierungsfunktion aktiviert.

Um die Protokollierungskonfiguration zu ändern (Konsole)

1. Öffnen Sie die FSx Amazon-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 Daten-Repository.
4. Wählen Sie im Bereich „Protokollierung“ die Option „Aktualisieren“.
5. Ändern Sie im Dialogfeld zur Konfiguration der Aktualisierungsprotokollierung die gewünschten Einstellungen.

   a. Wählen Sie Fehler protokollieren, um nur Fehlerereignisse zu protokollieren, oder Warnungen protokollieren, um nur Warnungsereignisse zu protokollieren, oder beides. Die Protokollierung ist deaktiviert, wenn Sie keine Auswahl treffen.

   b. Wählen Sie ein vorhandenes Ziel für das CloudWatch Logs-Protokoll oder erstellen Sie ein neues.
6. Wählen Sie Speichern.

So ändern Sie die Logging-Konfiguration (CLI)

- Verwenden Sie den `update-file-system`CLI-Befehl oder die entsprechende `UpdateFileSystem`API-Operation.

```
update-file-system --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration "LogConfiguration={Level=WARN_ERROR, \
        Destination="arn:aws:logs:us-east-1:234567890123:log-group:/aws/fsx/
testEventLogging"}"
```

Anzeigen von -Protokollen

Sie können die Protokolle einsehen, nachdem Amazon mit der Ausgabe begonnen FSx hat. Sie können die Protokolle wie folgt anzeigen:

- Sie können Protokolle anzeigen, indem Sie zur CloudWatch Amazon-Konsole gehen und die Protokollgruppe und den Protokollstream auswählen, an die Ihre Ereignisprotokolle gesendet werden. Weitere Informationen finden Sie unter An CloudWatch Logs gesendete Protokolldaten anzeigen im Amazon CloudWatch Logs-Benutzerhandbuch.
- Sie können CloudWatch Logs Insights verwenden, um Ihre Protokolldaten interaktiv zu suchen und zu analysieren. Weitere Informationen finden Sie unter Analysieren von Protokolldaten mit CloudWatch Logs Insights im Amazon CloudWatch Logs-Benutzerhandbuch.
- Sie können Protokolle auch nach Amazon S3 exportieren. Weitere Informationen finden Sie unter Exportieren von Protokolldaten nach Amazon S3 im Amazon CloudWatch Logs-Benutzerhandbuch.

Informationen zu den Gründen für Fehler finden Sie unterDatenrepository-Ereignisprotokolle.

Protokollierung FSx von Lustre-API-Aufrufen mit AWS CloudTrail

Amazon FSx for Lustre ist in einen Service integriert AWS CloudTrail, der eine Aufzeichnung der Aktionen bereitstellt, die von einem Benutzer, einer Rolle oder einem AWS Service in Amazon FSx for Lustre ausgeführt wurden. CloudTrail erfasst alle API-Aufrufe für Amazon FSx for Lustre als Ereignisse. Zu den erfassten Aufrufen gehören Aufrufe von der Amazon FSx for Lustre-Konsole und von Codeaufrufen an Amazon FSx for Lustre-API-Operationen.

Wenn Sie einen Trail erstellen, können Sie die kontinuierliche Übermittlung von CloudTrail Ereignissen an einen Amazon S3 S3-Bucket aktivieren, einschließlich Ereignissen für Amazon FSx for Lustre. Wenn Sie keinen Trail konfigurieren, können Sie die neuesten Ereignisse trotzdem in der CloudTrail Konsole im Ereignisverlauf einsehen. Anhand der von gesammelten Informationen können Sie feststellen CloudTrail, welche Anfrage an Amazon FSx for Lustre gestellt wurde. Sie können auch

die IP-Adresse, von der die Anforderung ausging, den Ersteller und den Erstellungszeitpunkt sowie weitere Details bestimmen.

Weitere Informationen CloudTrail dazu finden Sie im AWS CloudTrail Benutzerhandbuch.

Informationen FSx zu Amazon for Lustre in CloudTrail

CloudTrail ist für Ihr AWS Konto aktiviert, wenn Sie das Konto erstellen. Wenn API-Aktivitäten in Amazon FSx for Lustre auftreten, wird diese Aktivität zusammen mit anderen AWS Serviceereignissen in der CloudTrail Ereignishistorie in einem Ereignis aufgezeichnet. Sie können aktuelle Ereignisse in Ihrem AWS Konto ansehen, suchen und herunterladen. Weitere Informationen finden Sie unter Ereignisse mit CloudTrail Ereignisverlauf anzeigen.

Für eine fortlaufende Aufzeichnung von Ereignissen in Ihrem AWS Konto, einschließlich Veranstaltungen für Amazon FSx for Lustre, erstellen Sie einen Trail. Ein Trail ermöglicht CloudTrail die Übermittlung von Protokolldateien an einen Amazon S3 S3-Bucket. Wenn Sie einen Trail in der Konsole erstellen, gilt der Trail standardmäßig für alle AWS Regionen. Der Trail protokolliert Ereignisse aus allen AWS Regionen der AWS Partition und übermittelt die Protokolldateien an den von Ihnen angegebenen Amazon S3 S3-Bucket. Darüber hinaus können Sie andere AWS Dienste konfigurieren, um die in den CloudTrail Protokollen gesammelten Ereignisdaten weiter zu analysieren und darauf zu reagieren. Weitere Informationen finden Sie in folgenden Themen im AWS CloudTrail - Benutzerhandbuch:

- Übersicht zum Erstellen eines Trails
- CloudTrail Unterstützte Dienste und Integrationen
- Konfiguration von Amazon SNS SNS-Benachrichtigungen für CloudTrail
- Empfangen von CloudTrail Protokolldateien aus mehreren Regionen und Empfangen von CloudTrail Protokolldateien von mehreren Konten

Alle API-Aufrufe von Amazon FSx for Lustre werden von CloudTrail protokolliert. Beispielsweise generieren Aufrufe der `CreateFileSystem` und `TagResource` -Operationen Einträge in den CloudTrail Protokolldateien.

Jeder Ereignis- oder Protokolleintrag enthält Informationen zu dem Benutzer, der die Anforderung generiert hat. Die Identitätsinformationen unterstützen Sie bei der Ermittlung der folgenden Punkte:

- Ob die Anfrage mit Root- oder AWS Identity and Access Management (IAM-) Benutzeranmeldedaten gestellt wurde.

- Gibt an, ob die Anforderung mit temporären Sicherheitsanmeldeinformationen für eine Rolle oder einen Verbundbenutzer gesendet wurde.
- Ob die Anfrage von einem anderen AWS Dienst gestellt wurde.

Weitere Informationen finden Sie im CloudTrail UserIdentity-Element im AWS CloudTrail Benutzerhandbuch.

Grundlegendes zu Amazon FSx for Lustre-Protokolldateieinträgen

Ein Trail ist eine Konfiguration, die die Übertragung von Ereignissen als Protokolldateien an einen von Ihnen angegebenen Amazon S3 S3-Bucket ermöglicht. CloudTrail Protokolldateien enthalten einen oder mehrere Protokolleinträge. Ein Ereignis stellt eine einzelne Anforderung aus einer beliebigen Quelle dar und enthält Informationen über die angeforderte Aktion, Datum und Uhrzeit der Aktion, Anforderungsparameter usw. CloudTrail Protokolldateien sind kein geordneter Stack-Trace der öffentlichen API-Aufrufe, sodass sie nicht in einer bestimmten Reihenfolge angezeigt werden.

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der den `TagResource` Vorgang demonstriert, wenn ein Tag für ein Dateisystem von der Konsole aus erstellt wird.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
```

```
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

Das folgende Beispiel zeigt einen CloudTrail Protokolleintrag, der die `UntagResource` Aktion demonstriert, wenn ein Tag für ein Dateisystem von der Konsole gelöscht wird.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
```

```
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

Migration zu Amazon FSx for Lustre mit AWS DataSync

Sie können AWS DataSync es verwenden, um Daten zwischen Dateisystemen FSx für Lustre zu übertragen. DataSync ist ein Datenübertragungsdienst, der das Verschieben und Replizieren von Daten zwischen selbstverwalteten Speichersystemen und AWS Speicherdiensten über das Internet oder vereinfacht, automatisiert und beschleunigt. Direct Connect DataSync kann Ihre Dateisystemdaten und Metadaten wie Eigentum, Zeitstempel und Zugriffsberechtigungen übertragen.

Wie migriert man bestehende Dateien zu FSx for Lustre mit AWS DataSync

Sie können die Dateisysteme von DataSync with FSx for Lustre verwenden, um einmalige Datenmigrationen durchzuführen, regelmäßig Daten für verteilte Workloads aufzunehmen und die Replikation für Datenschutz und Wiederherstellung zu planen. Informationen zu bestimmten Übertragungsszenarien finden Sie unter Wo kann ich meine Daten übertragen? AWS DataSync im AWS DataSync Benutzerhandbuch.

Voraussetzungen

Um Daten in Ihr FSx for Lustre-Setup zu migrieren, benötigen Sie einen Server und ein Netzwerk, die die DataSync Anforderungen erfüllen. Weitere Informationen finden Sie unter Einrichtung von AWS DataSync im AWS DataSync Benutzerhandbuch.

- Sie haben ein Ziel FSx für das Lustre-Dateisystem erstellt. Weitere Informationen finden Sie unter Schritt 1: Erstellen Sie Ihr FSx for Lustre-Dateisystem.
- Die Quell- und Zieldateisysteme sind in derselben Virtual Private Cloud (VPC) verbunden. Das Quelldateisystem kann sich lokal oder in einer anderen Amazon VPC befinden, oder AWS-Konto AWS-Region, es muss sich jedoch in einem Netzwerk befinden, das mit dem des Zieldateisystems über Amazon VPC Peering, Transit Gateway, oder gepeert wird. AWS Direct Connect Site-to-Site VPN Weitere Informationen finden Sie unter Was ist VPC Peering? im Amazon VPC Peering Guide.

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

Grundlegende Schritte für die Migration von Dateien mit DataSync

Das Übertragen von Dateien von einer Quelle zu einem Ziel mithilfe von DataSync umfasst die folgenden grundlegenden Schritte:

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

Weitere Informationen finden Sie in folgenden Themen im AWS DataSync -Benutzerhandbuch:

- Übertragung zwischen lokalem Speicher und AWS
- Konfiguration von AWS DataSync Übertragungen mit Amazon FSx for Lustre.
- Bereitstellung Ihres EC2 Amazon-Agenten

Sicherheit bei Amazon 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. Um mehr über die Compliance-Programme zu erfahren, die gelten für Amazon FSx for Lustre, siehe AWS Leistungen im Leistungsumfang nach Compliance-Programmen.
- Sicherheit in der Cloud — Ihre Verantwortung richtet sich nach dem AWS Dienst, 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 anwenden können, wenn Sie Amazon FSx for Lustre. In den folgenden Themen erfahren Sie, wie Sie Amazon konfigurieren FSx, um Ihre Sicherheits- und Compliance-Ziele zu erreichen. Sie lernen auch, wie Sie andere Amazon-Dienste nutzen können, die Ihnen helfen, Ihre Amazon FSx for Lustre Ressourcen schätzen.

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 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 AWS Cloud alle 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 Informationen zur Verwendung von CloudTrail Pfaden zur Erfassung von AWS Aktivitäten finden Sie unter Arbeiten mit CloudTrail Pfaden im AWS CloudTrail Benutzerhandbuch.
- 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 140-3-validierte kryptografische Module benötigen, verwenden Sie einen FIPS-Endpunkt. Weitere Informationen über verfügbare FIPS-Endpunkte finden Sie unter Federal Information Processing Standard (FIPS) 140-3.

Wir empfehlen dringend, in Freitextfeldern, z. B. im Feld Name, keine vertraulichen oder sensiblen Informationen wie die E-Mail-Adressen Ihrer Kunden einzugeben. Dazu gehört auch, wenn Sie mit arbeiten Amazon FSx oder andere, die die AWS-Services Konsole, die API AWS CLI, oder verwenden AWS SDKs. 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 Arten 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 FSx Amazon-Dateisystem erstellt wird. Die Verschlüsselung von Daten während der Übertragung wird automatisch aktiviert, wenn Sie von EC2Amazon-Instances aus, die diese Funktion unterstützen, auf ein FSx Amazon-Dateisystem zugreifen.

Verwendung von Verschlüsselung

Wenn Ihr Unternehmen Unternehmens- oder behördlichen Richtlinien unterliegt, die die Verschlüsselung von Daten und Metadaten im Speicher 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 von Daten im Ruhezustand wird automatisch aktiviert, wenn Sie ein Amazon FSx for Lustre Dateisystem über die AWS-Managementkonsole AWS CLI, die oder programmgesteuert über die FSx Amazon-API oder eine der. AWS SDKs 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 von Amazon verwalteten Schlüsseln verschlüsselt FSx. 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 nach 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 Lustre finden Sie FSx unter. AWS KMSWie Amazon FSx for Lustre verwendet 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 transparent abgewickelt von Amazon FSx for Lustre, 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.

Wie Amazon FSx for Lustre verwendet 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 for Lustre-Dateisysteme werden im Ruhezustand mit Schlüsseln verschlüsselt, die von verwaltet werden. AWS KMSAmazon FSx for Lustre lässt sich in AWS KMS die 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 FSx wichtigsten Richtlinien von Amazon für AWS KMS

Schlüsselrichtlinien sind die primäre Methode zur Zugriffssteuerung für KMS-Schlüssel. Weitere Informationen zu den wichtigsten Richtlinien finden Sie unter Verwenden wichtiger Richtlinien 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 während der Übertragung automatisch verschlüsseln, wenn auf das Dateisystem von EC2 Amazon-Instances aus 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 EC2 Amazon-Benutzerhandbuch.

Eine Liste der Produkte, AWS-Regionen in denen Amazon FSx for Lustre verfügbar ist, finden Sie unterArt der Bereitstellung, Verfügbarkeit.

Richtlinie für den Datenverkehr zwischen Netzwerken

In diesem Thema wird beschrieben, wie Amazon Verbindungen vom Service zu anderen Standorten FSx sichert.

Verkehr zwischen Amazon FSx und lokalen Kunden

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 Lustre zugreifen FSx , um auf AWS veröffentlichte API-Operationen zur Ausführung administrativer Aufgaben zuzugreifen und Lustre Ports für die Interaktion mit dem Dateisystem.

API-Verkehr verschlüsseln

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 Instanzen aus aktiviert, die von dort aus auf die Dateisysteme zugreifen. AWS Cloud Weitere Informationen finden Sie unterVerschlüsseln von Daten während der Übertragung. FSx for Lustre bietet keine systemeigene Verschlüsselung bei der Übertragung zwischen lokalen Clients und Dateisystemen.

Identitäts- und Zugriffsmanagement für Amazon FSx for Lustre

AWS Identity and Access Management (IAM) hilft einem Administrator AWS-Service , den Zugriff auf AWS Ressourcen sicher zu kontrollieren. IAM-Administratoren kontrollieren, wer authentifiziert (angemeldet) und autorisiert werden kann (über Berechtigungen verfügt), um FSx Amazon-

Ressourcen zu verwenden. IAM ist ein Programm AWS-Service , das Sie ohne zusätzliche Kosten nutzen können.

Themen

Zielgruppe

Wie Sie AWS Identity and Access Management (IAM) verwenden, hängt von Ihrer Rolle ab:

- Servicebenutzer – Fordern Sie von Ihrem Administrator Berechtigungen an, wenn Sie nicht auf Features zugreifen können (siehe Fehlerbehebung bei Identität und Zugriff auf Amazon FSx for Lustre).
- Serviceadministrator – Bestimmen Sie den Benutzerzugriff und stellen Sie Berechtigungsanfragen (siehe So funktioniert Amazon FSx for Lustre mit IAM).
- IAM-Administrator – Schreiben Sie Richtlinien zur Zugriffsverwaltung (siehe Beispiele für identitätsbasierte Richtlinien für Amazon for Lustre FSx).

Authentifizierung mit Identitäten

Authentifizierung ist die Art und Weise, wie Sie sich AWS mit Ihren Identitätsdaten anmelden. Sie müssen sich als IAM-Benutzer authentifizieren oder eine IAM-Rolle annehmen. Root-Benutzer des AWS-Kontos

Sie können sich als föderierte Identität anmelden, indem Sie Anmeldeinformationen aus einer Identitätsquelle wie AWS IAM Identity Center (IAM Identity Center), Single Sign-On-Authentifizierung

oder Anmeldeinformationen verwenden. Google/Facebook Weitere Informationen zum Anmelden finden Sie unter So melden Sie sich bei Ihrem AWS-Konto an im Benutzerhandbuch für AWS-Anmeldung .

AWS Bietet für den programmatischen Zugriff ein SDK und eine CLI zum kryptografischen Signieren von Anfragen. Weitere Informationen finden Sie unter AWS Signature Version 4 for API requests im IAM-Benutzerhandbuch.

AWS-Konto Root-Benutzer

Wenn Sie einen erstellen AWS-Konto, beginnen Sie mit einer Anmeldeidentität, dem sogenannten AWS-Konto Root-Benutzer, der vollständigen Zugriff auf alle AWS-Services Ressourcen hat. Wir raten ausdrücklich davon ab, den Root-Benutzer für Alltagsaufgaben zu verwenden. Eine Liste der Aufgaben, für die Sie sich als Root-Benutzer anmelden müssen, finden Sie unter Tasks that require root user credentials im IAM-Benutzerhandbuch.

Verbundidentität

Es hat sich bewährt, dass menschliche Benutzer für den Zugriff AWS-Services mithilfe temporärer Anmeldeinformationen einen Verbund mit einem Identitätsanbieter verwenden müssen.

Eine föderierte Identität ist ein Benutzer aus Ihrem Unternehmensverzeichnis, Ihrem Directory Service Web-Identitätsanbieter oder der AWS-Services mithilfe von Anmeldeinformationen aus einer Identitätsquelle zugreift. Verbundene Identitäten übernehmen Rollen, die temporäre Anmeldeinformationen bereitstellen.

Für die zentrale Zugriffsverwaltung empfehlen wir AWS IAM Identity Center. Weitere Informationen finden Sie unter Was ist IAM Identity Center? im AWS IAM Identity Center -Benutzerhandbuch.

IAM-Benutzer und -Gruppen

Ein IAM-Benutzer ist eine Identität mit bestimmten Berechtigungen für eine einzelne Person oder Anwendung. Verwenden Sie möglichst temporäre Anmeldeinformationen anstelle von IAM-Benutzern mit langfristigen Anmeldeinformationen. Weitere Informationen finden Sie im IAM-Benutzerhandbuch unter Erfordern, dass menschliche Benutzer den Verbund mit einem Identitätsanbieter verwenden müssen, um AWS mithilfe temporärer Anmeldeinformationen darauf zugreifen zu können.

Eine IAM-Gruppe spezifiziert eine Sammlung von IAM-Benutzern und erleichtert die Verwaltung von Berechtigungen für große Gruppen von Benutzern. Weitere Informationen finden Sie unter Anwendungsfälle für IAM-Benutzer im IAM-Benutzerhandbuch.

IAM-Rollen

Eine IAM-Rolle ist eine Identität mit spezifischen Berechtigungen, die temporäre Anmeldeinformationen bereitstellt. Sie können eine Rolle übernehmen, indem Sie von einer Benutzer- zu einer IAM-Rolle (Konsole) wechseln AWS CLI oder einen AWS API-Vorgang aufrufen. Weitere Informationen finden Sie unter Methoden, um eine Rolle zu übernehmen im IAM-Benutzerhandbuch.

IAM-Rollen sind nützlich für Verbundbenutzerzugriff, temporäre IAM-Benutzerberechtigungen, kontoübergreifenden Zugriff, dienstübergreifenden Zugriff und Anwendungen, die auf Amazon ausgeführt werden. EC2 Weitere Informationen finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwalten des Zugriffs mit Richtlinien

Sie kontrollieren den Zugriff, AWS indem Sie Richtlinien erstellen und diese an Identitäten oder Ressourcen anhängen. AWS Eine Richtlinie definiert Berechtigungen, wenn sie mit einer Identität oder Ressource verknüpft sind. AWS bewertet diese Richtlinien, wenn ein Principal eine Anfrage stellt. Die meisten Richtlinien werden AWS als JSON-Dokumente gespeichert. Weitere Informationen zu JSON-Richtliniendokumenten finden Sie unter Übersicht über JSON-Richtlinien im IAM-Benutzerhandbuch.

Mit Hilfe von Richtlinien legen Administratoren fest, wer Zugriff auf was hat, indem sie definieren, welches Prinzipal welche Aktionen auf welchen Ressourcenund unter welchen Bedingungendurchführen darf.

Standardmäßig haben Benutzer, Gruppen und Rollen keine Berechtigungen. Ein IAM-Administrator erstellt IAM-Richtlinien und fügt sie zu Rollen hinzu, die die Benutzer dann übernehmen können. IAM-Richtlinien definieren Berechtigungen unabhängig von der Methode, die zur Ausführung der Operation verwendet wird.

Identitätsbasierte Richtlinien

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität (Benutzer, Gruppe oder Rolle) anfügen können. Diese Richtlinien steuern, welche Aktionen Identitäten für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten Richtlinien im IAM-Benutzerhandbuch.

Identitätsbasierte Richtlinien können Inline-Richtlinien (direkt in eine einzelne Identität eingebettet) oder verwaltete Richtlinien (eigenständige Richtlinien, die mit mehreren Identitäten verbunden sind)

sein. Informationen dazu, wie Sie zwischen verwalteten und Inline-Richtlinien wählen, finden Sie unter Choose between managed policies and inline policies im IAM-Benutzerhandbuch.

Ressourcenbasierte Richtlinien

Ressourcenbasierte Richtlinien sind JSON-Richtliniendokumente, die Sie an eine Ressource anfügen. Beispiele hierfür sind Vertrauensrichtlinien für IAM-Rollen 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. Sie müssen in einer ressourcenbasierten Richtlinie einen Prinzipal angeben.

Ressourcenbasierte Richtlinien sind Richtlinien innerhalb dieses Diensts. Sie können AWS verwaltete Richtlinien von IAM nicht in einer ressourcenbasierten Richtlinie verwenden.

Weitere Richtlinientypen

AWS unterstützt zusätzliche Richtlinientypen, mit denen die maximalen Berechtigungen festgelegt werden können, die durch gängigere Richtlinientypen gewährt werden:

- Berechtigungsgrenzen – Eine Berechtigungsgrenze legt die maximalen Berechtigungen fest, die eine identitätsbasierte Richtlinie einer IAM-Entität erteilen kann. Weitere Informationen finden Sie unter Berechtigungsgrenzen für IAM-Entitäten im -IAM-Benutzerhandbuch.
- Richtlinien zur Dienstkontrolle (SCPs) — Geben Sie die maximalen Berechtigungen für eine Organisation oder Organisationseinheit in an AWS Organizations. Weitere Informationen finden Sie unter Service-Kontrollrichtlinien im AWS Organizations -Benutzerhandbuch.
- Richtlinien zur Ressourcenkontrolle (RCPs) — Legen Sie die maximal verfügbaren Berechtigungen für Ressourcen in Ihren Konten fest. Weitere Informationen finden Sie im AWS Organizations Benutzerhandbuch unter Richtlinien zur Ressourcenkontrolle (RCPs).
- Sitzungsrichtlinien – Sitzungsrichtlinien sind erweiterte Richtlinien, die als Parameter übergeben werden, wenn Sie eine temporäre Sitzung für eine Rolle oder einen Verbundbenutzer erstellen. Weitere Informationen finden Sie unter Sitzungsrichtlinien im IAM-Benutzerhandbuch.

Mehrere Richtlinientypen

Wenn für eine Anfrage mehrere Arten von Richtlinien gelten, sind die sich daraus ergebenden Berechtigungen schwieriger zu verstehen. Informationen darüber, wie AWS bestimmt wird, ob eine Anfrage zulässig ist, wenn mehrere Richtlinientypen betroffen sind, finden Sie unter Bewertungslogik für Richtlinien im IAM-Benutzerhandbuch.

So funktioniert Amazon FSx for Lustre mit IAM

Bevor Sie IAM verwenden, um den Zugriff auf Amazon zu verwalten FSx, sollten Sie sich darüber informieren, welche IAM-Funktionen für Amazon verfügbar sind. FSx

IAM-Funktionen, die Sie mit Amazon FSx for Lustre verwenden können

IAM-Feature	FSx Amazon-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 allgemeinen Überblick darüber, wie Amazon FSx und andere AWS Services mit den meisten IAM-Funktionen funktionieren, finden Sie im IAM-Benutzerhandbuch unter AWS Services, die mit IAM funktionieren.

Identitätsbasierte Richtlinien für Amazon FSx

Unterstützt Richtlinien auf Identitätsbasis: Ja

Identitätsbasierte Richtlinien sind JSON-Berechtigungsrichtliniendokumente, die Sie einer Identität anfügen können, wie z. B. IAM-Benutzern, -Benutzergruppen oder -Rollen. Diese Richtlinien steuern, welche Aktionen die Benutzer und Rollen für welche Ressourcen und unter welchen Bedingungen ausführen können. Informationen zum Erstellen identitätsbasierter Richtlinien finden Sie unter Definieren benutzerdefinierter IAM-Berechtigungen mit vom Kunden verwalteten 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. 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 FSx identitätsbasierte Richtlinien von Amazon finden Sie unter. Beispiele für identitätsbasierte Richtlinien für Amazon for Lustre FSx

Ressourcenbasierte Richtlinien innerhalb von Amazon FSx

Unterstützt ressourcenbasierte Richtlinien: Nein

Politische Maßnahmen für Amazon FSx

Unterstützt Richtlinienaktionen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Action` einer JSON-Richtlinie beschreibt die Aktionen, mit denen Sie den Zugriff in einer Richtlinie zulassen oder verweigern können. Nehmen Sie Aktionen in eine Richtlinie auf, um Berechtigungen zur Ausführung des zugehörigen Vorgangs zu erteilen.

Eine Liste der FSx Amazon-Aktionen finden Sie unter Von Amazon FSx für Lustre definierte Aktionen in der Service Authorization Reference.

Richtlinienaktionen in Amazon FSx verwenden das folgende Präfix vor der Aktion:

```
fsx
```

Um mehrere Aktionen in einer einzigen Anweisung anzugeben, trennen Sie sie mit Kommata:

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

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

Politische Ressourcen für Amazon FSx

Unterstützt Richtlinienressourcen: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer auf was Zugriff hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das JSON-Richtlinienelement `Resource` gibt die Objekte an, auf welche die Aktion angewendet wird. Als Best Practice geben Sie eine Ressource mit dem zugehörigen Amazon-Ressourcennamen (ARN) an. Verwenden Sie für Aktionen, die keine Berechtigungen auf Ressourcenebene unterstützen, einen Platzhalter (*), um anzugeben, dass die Anweisung für alle Ressourcen gilt.

```
"Resource": "*"
```

Eine Liste der FSx Amazon-Ressourcentypen und ihrer ARNs Eigenschaften finden Sie unter Von Amazon FSx for Lustre definierte Ressourcen in der Service Authorization Reference. Informationen darüber, mit welchen Aktionen Sie den ARN jeder Ressource angeben können, finden Sie unter Von Amazon FSx for Lustre definierte Aktionen.

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

Schlüssel zu den Versicherungsbedingungen für Amazon FSx

Unterstützt servicespezifische Richtlinienbedingungsschlüssel: Ja

Administratoren können mithilfe von AWS JSON-Richtlinien angeben, wer Zugriff auf was hat. Das heißt, welcher Prinzipal Aktionen für welche Ressourcen und unter welchen Bedingungen ausführen kann.

Das Element `Condition` gibt an, wann Anweisungen auf der Grundlage definierter Kriterien ausgeführt werden. 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. Eine Übersicht aller AWS globalen Bedingungsschlüssel finden Sie unter Kontextschlüssel für AWS globale Bedingungen im IAM-Benutzerhandbuch.

Eine Liste der FSx Amazon-Bedingungsschlüssel finden Sie unter Bedingungsschlüssel für Amazon FSx for Lustre in der Service Authorization Reference. Informationen zu den Aktionen und Ressourcen, mit denen Sie einen Bedingungsschlüssel verwenden können, finden Sie unter Von Amazon FSx for Lustre definierte Aktionen.

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

Zugriffskontrolllisten (ACLs) in Amazon FSx

Unterstützt ACLs: Nein

Attributbasierte Zugriffskontrolle (ABAC) mit Amazon FSx

Unterstützt ABAC (Tags in Richtlinien): Ja

Die attributbasierte Zugriffskontrolle (ABAC) ist eine Autorisierungsstrategie, bei der Berechtigungen basierend auf Attributen, auch als Tags bezeichnet, definiert werden. Sie können Tags an IAM-Entitäten und AWS -Ressourcen anhängen und dann ABAC-Richtlinien entwerfen, um Operationen zu ermöglichen, wenn das Tag des Prinzipals mit dem Tag auf der Ressource übereinstimmt.

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 Definieren von Berechtigungen mit ABAC-Autorisierung im IAM-Benutzerhandbuch. Um ein Tutorial mit Schritten zur Einstellung von ABAC anzuzeigen, siehe Attributbasierte Zugriffskontrolle (ABAC) verwenden im IAM-Benutzerhandbuch.

Weitere Informationen zum Taggen von FSx Amazon-Ressourcen finden Sie unterTaggen Sie Ihre Amazon FSx for Lustre-Ressourcen.

Ein Beispiel für eine identitätsbasierte Richtlinie zur Einschränkung des Zugriffs auf eine Ressource auf der Grundlage der Markierungen dieser Ressource finden Sie unter Verwenden von Tags zur Steuerung des Zugriffs auf Ihre FSx Amazon-Ressourcen.

Temporäre Anmeldeinformationen mit Amazon verwenden FSx

Unterstützt temporäre Anmeldeinformationen: Ja

Temporäre Anmeldeinformationen ermöglichen kurzfristigen Zugriff auf AWS Ressourcen und werden automatisch erstellt, wenn Sie einen Verbund verwenden oder die Rollen wechseln. AWS empfiehlt, temporäre Anmeldeinformationen dynamisch zu generieren, anstatt langfristige Zugriffsschlüssel zu verwenden. Weitere Informationen finden Sie unter Temporäre Anmeldeinformationen in IAM und AWS-Services , die mit IAM funktionieren im IAM-Benutzerhandbuch.

Zugriffssitzungen für Amazon weiterleiten FSx

Unterstützt Forward Access Sessions (FAS): Ja

Forward Access Sessions (FAS) verwenden die Berechtigungen des Principals, der einen aufruft AWS-Service, kombiniert mit der Anfrage, Anfragen AWS-Service an nachgelagerte Dienste zu stellen. Einzelheiten zu den Richtlinien für FAS-Anforderungen 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**
>
> Durch das Ändern der Berechtigungen für eine Servicerolle kann die FSx Amazon-Funktionalität beeinträchtigt werden. Bearbeiten Sie Servicerollen nur, FSx wenn Amazon Sie dazu anleitet.

Servicebezogene Rollen für Amazon FSx

Unterstützt serviceverknüpfte Rollen: Ja

Eine serviceverknüpfte Rolle ist eine Art von Servicerolle, die mit einer verknüpft ist. AWS-Service Der Service kann die Rolle übernehmen, um eine Aktion in Ihrem Namen auszuführen. Dienstbezogene Rollen werden in Ihrem Dienst angezeigt AWS-Konto und gehören dem Dienst. Ein IAM-Administrator kann die Berechtigungen für Service-verknüpfte Rollen anzeigen, aber nicht bearbeiten.

Weitere Informationen zum Erstellen und Verwalten von Rollen, die mit dem Service von FSx Amazon verknüpft sind, finden Sie unterVerwenden von serviceverknüpften Rollen für Amazon FSx.

Beispiele für identitätsbasierte Richtlinien für Amazon for Lustre FSx

Standardmäßig sind Benutzer und Rollen nicht berechtigt, FSx Amazon-Ressourcen zu erstellen oder zu ändern. Ein IAM-Administrator muss IAM-Richtlinien erstellen, die Benutzern die Berechtigung erteilen, Aktionen für die Ressourcen auszuführen, die sie benötigen.

Informationen dazu, wie Sie unter Verwendung dieser beispielhaften JSON-Richtliniendokumente eine identitätsbasierte IAM-Richtlinie erstellen, finden Sie unter Erstellen von IAM-Richtlinien (Konsole) im IAM-Benutzerhandbuch.

Einzelheiten zu den von Amazon definierten Aktionen und Ressourcentypen FSx, einschließlich des Formats ARNs für die einzelnen Ressourcentypen, finden Sie unter Aktionen, Ressourcen und Bedingungsschlüssel für Amazon FSx for Lustre in der Service Authorization Reference.

Themen

- Best Practices für Richtlinien
- Verwenden der FSx Amazon-Konsole
- Gewähren der Berechtigung zur Anzeige der eigenen Berechtigungen für Benutzer

Best Practices für Richtlinien

Identitätsbasierte Richtlinien legen fest, ob jemand FSx Amazon-Ressourcen in Ihrem Konto erstellen, darauf zugreifen oder diese löschen kann. Dies kann zusätzliche Kosten für Ihr verursachen AWS-Konto. Wenn Sie identitätsbasierte Richtlinien erstellen oder bearbeiten, befolgen Sie diese Richtlinien und Empfehlungen:

- Erste Schritte mit AWS verwalteten Richtlinien und Umstellung auf Berechtigungen mit den geringsten Rechten — Verwenden Sie die AWS verwalteten Richtlinien, die Berechtigungen für viele gängige Anwendungsfälle gewähren, um damit zu beginnen, Ihren Benutzern und Workloads Berechtigungen zu gewähren. Sie sind in Ihrem verfügbar. AWS-Konto Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom AWS Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind. Weitere Informationen finden Sie unter Von AWS verwaltete Richtlinien oder Von 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 Serviceaktionen zu gewähren, wenn diese für einen bestimmten Zweck verwendet werden AWS-Service, z. CloudFormation B. Weitere Informationen finden Sie unter IAM-JSON-Richtlinienelemente: Bedingung im IAM-Benutzerhandbuch.
- Verwenden von IAM Access Analyzer zur Validierung Ihrer IAM-Richtlinien, um sichere und funktionale Berechtigungen zu gewährleisten – IAM Access Analyzer validiert neue und vorhandene Richtlinien, damit die Richtlinien der IAM-Richtliniensprache (JSON) und den bewährten IAM-Methoden entsprechen. IAM Access Analyzer stellt mehr als 100 Richtlinienprüfungen und umsetzbare Empfehlungen zur Verfügung, damit Sie sichere und funktionale Richtlinien erstellen können. Weitere Informationen finden Sie unter Richtlinienvalidierung mit IAM Access Analyzer im IAM-Benutzerhandbuch.

- Multi-Faktor-Authentifizierung (MFA) erforderlich — Wenn Sie ein Szenario haben, das IAM-Benutzer oder einen Root-Benutzer in Ihrem System erfordert AWS-Konto, aktivieren Sie MFA für zusätzliche Sicherheit. Um MFA beim Aufrufen von API-Vorgängen anzufordern, fügen Sie Ihren Richtlinien MFA-Bedingungen hinzu. Weitere Informationen finden Sie unter Sicherer API-Zugriff mit MFA im IAM-Benutzerhandbuch.

Weitere Informationen zu bewährten Methoden in IAM finden Sie unter Best Practices für die Sicherheit in IAM im IAM-Benutzerhandbuch.

Verwenden der FSx Amazon-Konsole

Um auf die Amazon FSx for Lustre-Konsole zugreifen zu können, benötigen Sie ein Mindestmaß an Berechtigungen. Diese Berechtigungen müssen es Ihnen ermöglichen, Details zu den FSx Amazon-Ressourcen in Ihrem aufzulisten und anzuzeigen AWS-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.

Sie müssen Benutzern, die nur die API AWS CLI oder die AWS API aufrufen, keine Mindestberechtigungen für die Konsole gewähren. Stattdessen sollten Sie nur Zugriff auf die Aktionen zulassen, die der API-Operation entsprechen, die die Benutzer ausführen möchten.

Um sicherzustellen, dass Benutzer und Rollen die FSx Amazon-Konsole weiterhin 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 finden die `AmazonFSxConsoleReadOnlyAccess` und andere Richtlinien für Amazon FSx Managed Services unterAWS verwaltete Richtlinien für Amazon FSx for Lustre.

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 umfasst Berechtigungen zum Ausführen dieser Aktion auf der Konsole oder programmgesteuert mithilfe der API AWS CLI oder AWS .

```
{
    "Version": "2012-10-17",
```

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

AWS verwaltete Richtlinien für Amazon FSx for Lustre

Eine AWS verwaltete Richtlinie ist eine eigenständige Richtlinie, die von erstellt und verwaltet AWS wird. AWS Verwaltete Richtlinien dienen dazu, Berechtigungen für viele gängige Anwendungsfälle bereitzustellen, sodass Sie damit beginnen können, Benutzern, Gruppen und Rollen Berechtigungen zuzuweisen.

Beachten Sie, dass AWS verwaltete Richtlinien für Ihre speziellen Anwendungsfälle möglicherweise keine Berechtigungen mit den geringsten Rechten gewähren, da sie für alle AWS Kunden verfügbar sind. Wir empfehlen Ihnen, die Berechtigungen weiter zu reduzieren, indem Sie vom Kunden verwaltete Richtlinien definieren, die speziell auf Ihre Anwendungsfälle zugeschnitten sind.

Sie können die in AWS verwalteten Richtlinien definierten Berechtigungen nicht ändern. Wenn die in einer AWS verwalteten Richtlinie definierten Berechtigungen AWS aktualisiert werden, wirkt sich das Update auf alle Prinzidentitäten (Benutzer, Gruppen und Rollen) aus, denen die Richtlinie zugeordnet ist. AWS aktualisiert eine AWS verwaltete Richtlinie höchstwahrscheinlich, wenn eine neue Richtlinie eingeführt AWS-Service wird oder neue API-Operationen für bestehende Dienste verfügbar werden.

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

Amazon FSx ServiceRolePolicy

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

AWS verwaltete Richtlinie: Amazon FSx DeleteServiceLinkedRoleAccess

Sie können `AmazonFSxDeleteServiceLinkedRoleAccess` nicht an Ihre IAM-Entitäten anhängen. Diese Richtlinie ist mit einem Service verknüpft und wird nur mit der serviceverknüpften Rolle für diesen Service verwendet. Sie können diese Richtlinie nicht anhängen, trennen, ändern oder löschen. Weitere Informationen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon FSx.

Diese Richtlinie gewährt Administratorberechtigungen, die es Amazon FSx ermöglichen, seine Service Linked Role für den Zugriff auf Amazon S3 zu löschen, die nur von Amazon FSx for Lustre verwendet wird.

Details zu Berechtigungen

Diese Richtlinie beinhaltet Berechtigungen, `iam` die es Amazon ermöglichen, FSx den Löschstatus für den Zugriff auf FSx Service Linked Roles for Amazon S3 einzusehen, zu löschen und einzusehen.

Die Berechtigungen für diese Richtlinie finden Sie unter Amazon FSx DeleteServiceLinkedRoleAccess im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: Amazon FSx FullAccess

Sie können Amazon FSx FullAccess an Ihre IAM-Entitäten anhängen. Amazon FSx verknüpft diese Richtlinie auch mit einer Servicerolle, die es Amazon FSx ermöglicht, Aktionen in Ihrem Namen durchzuführen.

Bietet vollen Zugriff auf Amazon FSx und Zugriff auf verwandte AWS Services.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Prinzipalen vollen Zugriff auf die Ausführung aller FSx Amazon-Aktionen, mit Ausnahme `BypassSnaplockEnterpriseRetention` von.
- `ds`— Ermöglicht Prinzipalen, Informationen über die Verzeichnisse einzusehen. Directory Service
- `ec2`
  - Ermöglicht Prinzipalen das Erstellen von Tags unter den angegebenen Bedingungen.
  - Um eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.
- `iam`— Ermöglicht Principles, im Namen des Benutzers eine mit Amazon FSx Service verknüpfte Rolle zu erstellen. Dies ist erforderlich, damit Amazon AWS Ressourcen im Namen des Benutzers verwalten FSx kann.
- `firehose`— Ermöglicht Prinzipalen das Schreiben von Datensätzen in eine Amazon Data Firehose. Dies ist erforderlich, damit Benutzer den Zugriff auf das Windows-Dateiserver-Dateisystem überwachen FSx können, indem sie Audit-Zugriffsprotokolle an Firehose senden.
- `logs`— Ermöglicht Prinzipalen, Protokollgruppen zu erstellen, Streams zu protokollieren und Ereignisse in Protokolldatenströme zu schreiben. Dies ist erforderlich, damit Benutzer den Zugriff auf das Dateisystem auf dem Windows-Dateiserver überwachen FSx können, indem sie CloudWatch Audit-Zugriffsprotokolle an Logs senden.

Die Berechtigungen für diese Richtlinie finden Sie unter Amazon FSx FullAccess im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: Amazon FSx ConsoleFullAccess

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

Diese Richtlinie gewährt Administratorberechtigungen, die den vollen Zugriff auf Amazon FSx und den Zugriff auf verwandte AWS Dienste über die ermöglichen AWS-Managementkonsole.

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Prinzipalen, alle Aktionen in der FSx Amazon-Managementkonsole auszuführen, mit Ausnahme `BypassSnaplockEnterpriseRetention` von.

- `cloudwatch`— Ermöglicht Principals, CloudWatch Alarme und Messwerte in der Amazon FSx Management Console einzusehen.
- `ds`— Ermöglicht Prinzipalen, Informationen über ein Directory Service Verzeichnis aufzulisten.
- `ec2`
  - Ermöglicht Principals, Tags für Routing-Tabellen zu erstellen, Netzwerkschnittstellen, Routing-Tabellen, Sicherheitsgruppen, Subnetze und die einem FSx Amazon-Dateisystem zugeordnete VPC aufzulisten.
  - Ermöglicht Prinzipalen die erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen, die mit einer VPC verwendet werden können.
  - Ermöglicht Prinzipalen die Anzeige der Elastic Network-Schnittstellen, die einem FSx Amazon-Dateisystem zugeordnet sind.
- `kms`— Ermöglicht Prinzipalen, Aliase für Schlüssel aufzulisten. AWS Key Management Service
- `s3`— Ermöglicht Prinzipalen, einige oder alle Objekte in einem Amazon S3 S3-Bucket aufzulisten (bis zu 1000).
- `iam`— Erteilt die Erlaubnis, eine serviceverknüpfte Rolle FSx zu erstellen, die es Amazon ermöglicht, Aktionen im Namen des Benutzers durchzuführen.

Die Berechtigungen für diese Richtlinie finden Sie unter Amazon FSx ConsoleFullAccess im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: Amazon FSx ConsoleReadOnlyAccess

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

Diese Richtlinie gewährt Amazon FSx und verwandten AWS Diensten nur Leseberechtigungen, sodass Benutzer Informationen zu diesen Diensten in der einsehen können. AWS-Managementkonsole

Details zu Berechtigungen

Diese Richtlinie umfasst die folgenden Berechtigungen.

- `fsx`— Ermöglicht Prinzipalen, Informationen über FSx Amazon-Dateisysteme, einschließlich aller Tags, in der Amazon FSx Management Console einzusehen.
- `cloudwatch`— Ermöglicht Prinzipalen die Anzeige von CloudWatch Alarmen und Kennzahlen in der Amazon FSx Management Console.

- `ds`— Ermöglicht Principals, Informationen zu einem Directory Service Verzeichnis in der Amazon FSx Management Console einzusehen.
- `ec2`
  - Ermöglicht Principals, Netzwerkschnittstellen, Sicherheitsgruppen, Subnetze und die einem FSx Amazon-Dateisystem zugeordnete VPC in der Amazon FSx Management Console einzusehen.
  - Ermöglicht Prinzipalen die erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen, die mit einer VPC verwendet werden können.
  - Ermöglicht Prinzipalen die Anzeige der Elastic Network-Schnittstellen, die einem FSx Amazon-Dateisystem zugeordnet sind.
- `kms`— Ermöglicht Prinzipalen, Aliase für AWS Key Management Service Schlüssel in der Amazon FSx Management Console einzusehen.
- `log`— Ermöglicht Principals, die Amazon CloudWatch Logs-Protokollgruppen zu beschreiben, die dem Konto zugeordnet sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit die Hauptbenutzer die bestehende Konfiguration für die Überwachung des Dateizugriffs für ein Dateisystem FSx für Windows-Dateiserver einsehen können.
- `firehose`— Ermöglicht Principals, die Amazon Data Firehose-Lieferdatenströme zu beschreiben, die dem Konto zugeordnet sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit die Principals die bestehende Konfiguration für die Dateizugriffsprüfung für ein Dateisystem FSx für Windows-Dateiserver einsehen können.

Die Berechtigungen für diese Richtlinie finden Sie unter Amazon FSx ConsoleReadOnlyAccess im Referenzhandbuch für AWS verwaltete Richtlinien.

AWS verwaltete Richtlinie: Amazon FSx ReadOnlyAccess

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

- `fsx`— Ermöglicht Prinzipalen, Informationen über FSx Amazon-Dateisysteme, einschließlich aller Tags, in der Amazon FSx Management Console einzusehen.
- `ec2`— Bereitstellung einer erweiterten Sicherheitsgruppenvalidierung aller Sicherheitsgruppen, die mit einer VPC verwendet werden können.

Die Berechtigungen für diese Richtlinie finden Sie unter Amazon FSx ReadOnlyAccess im Referenzhandbuch für AWS verwaltete Richtlinien.

FSx Aktualisierungen der AWS verwalteten Richtlinien durch Amazon

Sehen Sie sich Details zu Aktualisierungen der AWS verwalteten Richtlinien für Amazon an, FSx seit dieser Service begonnen hat, diese Änderungen zu verfolgen. Abonnieren Sie den RSS-Feed auf der Amazon-Seite, um automatische Benachrichtigungen über Änderungen an dieser FSx Dokumentverlauf Seite zu erhalten.

Änderung	Beschreibung	Datum
Amazon FSx ServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:AssignIpv6Addresses` die es Principals ermöglicht, Kundennetzwerkschnittstellen mit einem `AmazonFSx.FileSystemId` Tag IPv6 Adressen zuzuweisen.	22. Juli 2025
Amazon FSx ServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:UnassignIpv6Addresses` die es Principals ermöglicht, IPv6 Adressen von Kundennetzwerkschnittstellen, die über ein `AmazonFSx.FileSystemId` Tag verfügen, zuzuweisen.	22. Juli 2025
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `fsx:CreateAndAttachS3AccessPoint` die es Principals ermöglicht, einen S3-Zugangspunkt zu erstellen und ihn an ein FSx Volume anzuhängen.	25. Juni 2025

Änderung	Beschreibung	Datum
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `fsx:DescribeS3AccessPointAttachments` die es Principals ermöglicht, alle S3-Zugangspunkte AWS-Konto in einem AWS-Region aufzulisten.	25. Juni 2025
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `fsx:DetachAndDeleteS3AccessPoint` die es Principals ermöglicht, einen S3-Zugangspunkt zu löschen.	25. Juni 2025
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `fsx:CreateAndAttachS3AccessPoint` die es Principals ermöglicht, einen S3-Zugangspunkt zu erstellen und ihn an ein FSx Volume anzuhängen.	25. Juni 2025
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `fsx:DescribeS3AccessPointAttachments` die es Principals ermöglicht, alle S3-Zugangspunkte AWS-Konto in einem AWS-Region aufzulisten.	25. Juni 2025

Änderung	Beschreibung	Datum
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `fsx:DetachAndDeleteS3AccessPoint` die es Principals ermöglicht, einen S3-Zugangspunkt zu löschen.	25. Juni 2025
Amazon FSx ConsoleReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:DescribeNetworkInterfaces` die es Principals ermöglicht, die mit ihrem Dateisystem verknüpften Elastic Network-Schnittstellen einzusehen.	25. Februar 2025
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:DescribeNetworkInterfaces` die es Principals ermöglicht, die mit ihrem Dateisystem verknüpften Elastic Network-Schnittstellen einzusehen.	07. Februar 2025
Amazon FSx ServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen vorzunehmen, die mit einer VPC verwendet werden können.	9. Januar 2024

Änderung	Beschreibung	Datum
Amazon FSx ReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen vorzunehmen, die mit einer VPC verwendet werden können.	9. Januar 2024
Amazon FSx ConsoleReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen vorzunehmen, die mit einer VPC verwendet werden können.	9. Januar 2024
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen vorzunehmen, die mit einer VPC verwendet werden können.	9. Januar 2024

Änderung	Beschreibung	Datum
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, `ec2:GetSecurityGroupsForVpc` die es Principals ermöglicht, eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen vorzunehmen, die mit einer VPC verwendet werden können.	9. Januar 2024
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, die es Benutzern ermöglicht, regionsübergreifende und kontoübergreifende Datenreplikation FSx für OpenZFS-Dateisysteme durchzuführen.	20. Dezember 2023
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, die es Benutzern ermöglicht, regionsübergreifende und kontoübergreifende Datenreplikation FSx für OpenZFS-Dateisysteme durchzuführen.	20. Dezember 2023
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, um Benutzern die On-Demand-Replikation von Volumes FSx für OpenZFS-Dateisysteme zu ermöglichen.	26. November 2023

Änderung	Beschreibung	Datum
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat eine neue Berechtigung hinzugefügt, um Benutzern die On-Demand-Replikation von Volumes FSx für OpenZFS-Dateisysteme zu ermöglichen.	26. November 2023
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, mit denen Benutzer die gemeinsame VPC-Unterstützung FSx für ONTAP Multi-AZ-Dateisysteme anzeigen, aktivieren und deaktivieren können.	14. November 2023
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, mit denen Benutzer die gemeinsame VPC-Unterstützung FSx für ONTAP Multi-AZ-Dateisysteme anzeigen, aktivieren und deaktivieren können.	14. November 2023
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Netzwerkkonfigurationen FSx für OpenZFS Multi-AZ-Dateisysteme zu verwalten.	9. August 2023

Änderung	Beschreibung	Datum
AWS verwaltete Richtlinie: Amazon FSx ServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon hat die bestehende `cloudwatch:PutMetricData` Berechtigung FSx geändert, sodass Amazon CloudWatch Metriken im `AWS/FSx` Namespace FSx veröffentlicht.	24. Juli 2023
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon hat die Richtlinie FSx aktualisiert, um die `fsx:*` Genehmigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen.	13. Juli 2023
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon hat die Richtlinie FSx aktualisiert, um die `fsx:*` Genehmigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen.	13. Juli 2023
Amazon FSx ConsoleReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Benutzer erweiterte Leistungskennzahlen und Handlungsempfehlungen FSx für Windows File Server-Dateisysteme in der FSx Amazon-Konsole einsehen können.	21. September 2022

Änderung	Beschreibung	Datum
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Benutzer erweiterte Leistungskennzahlen und Handlungsempfehlungen FSx für Windows File Server-Dateisysteme in der FSx Amazon-Konsole einsehen können.	21. September 2022
Amazon FSx ReadOnlyAccess — Richtlinien zur Sendungsverfolgung gestartet	Diese Richtlinie gewährt Lesezugriff auf alle FSx Amazon-Ressourcen und alle damit verbundenen Tags.	4. Februar 2022
Amazon FSx DeleteServiceLinkedRoleAccess — Richtlinien zur Sendungsverfolgung gestartet	Diese Richtlinie gewährt Administratorberechtigungen, die es Amazon FSx ermöglichen, seine Service Linked Role für den Zugriff auf Amazon S3 zu löschen.	7. Januar 2022
Amazon FSx ServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon FSx ermöglichen, Netzwerkkonfigurationen für Amazon FSx für NetApp ONTAP-Dateisysteme zu verwalten.	2. September 2021

Änderung	Beschreibung	Datum
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon ermöglichen FSx , Tags in EC2 Routing-Tabellen für Anrufe mit eingeschränktem Geltungsbereich zu erstellen.	2. September 2021
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Amazon FSx Multi-AZ-Dateisysteme von Amazon FSx for NetApp ONTAP erstellen kann.	2. September 2021
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon ermöglichen FSx , Tags in EC2 Routing-Tabellen für Anrufe mit eingeschränktem Geltungsbereich zu erstellen.	2. September 2021

Änderung	Beschreibung	Datum
Amazon FSx ServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Amazon ermöglichen, CloudWatch Log-Streams FSx zu beschreiben und in sie zu schreiben. Dies ist erforderlich, damit Benutzer mithilfe CloudWatch von Logs Audit-Logs Dateizugriffs-Audit-Logs FSx für Windows-Dateiserver-Dateisysteme einsehen können.	8. Juni 2021
Amazon FSx ServiceRolePolicy — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, FSx damit Amazon Data Firehose-Lieferstreams beschreiben und in sie schreiben kann. Dies ist erforderlich, damit Benutzer die Dateizugriffs-Audit-Logs für ein Dateisystem FSx für Windows File Server mithilfe von Amazon Data Firehose einsehen können.	8. Juni 2021

Änderung	Beschreibung	Datum
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Prinzipalen ermöglichen, CloudWatch Log-Log-Gruppen und Log-Streams zu beschreiben und zu erstellen und Ereignisse in Log-Streams zu schreiben. Dies ist erforderlich, damit Prinzipale mithilfe CloudWatch von Protokollen die Auditprotokolle für Dateizugriffe FSx für Windows-Dateiserver-Dateisysteme einsehen können.	8. Juni 2021
Amazon FSx FullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, die es Prinzipalen ermöglichen, Datensätze zu beschreiben und in eine Amazon Data Firehose zu schreiben. Dies ist erforderlich, damit Benutzer die Dateizugriffs-Audit-Logs für ein Dateisystem FSx für Windows File Server mithilfe von Amazon Data Firehose einsehen können.	8. Juni 2021

Änderung	Beschreibung	Datum
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon CloudWatch Logs-Protokollgruppen beschreiben können, die dem Konto zugeordnet sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit Principals bei der Konfiguration der Dateizugriffsüberwachung für ein Dateisystem FSx für Windows-Dateiserver eine bestehende CloudWatch Logs-Protokollgruppe auswählen können.	8. Juni 2021
Amazon FSx ConsoleFullAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon Data Firehose-Lieferströme beschreiben können, die mit dem Konto verknüpft sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit Principals bei der Konfiguration der Dateizugriffsüberwachung für ein Dateisystem FSx für Windows File Server einen vorhandenen Firehose-Lieferstream auswählen können.	8. Juni 2021

Änderung	Beschreibung	Datum
Amazon FSx ConsoleReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon CloudWatch Logs-Protokollgruppen beschreiben können, die dem Konto zugeordnet sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit die Hauptbenutzer die bestehende Konfiguration für die Dateizugriffsprüfung für ein Dateisystem FSx für Windows-Dateiserver einsehen können.	8. Juni 2021
Amazon FSx ConsoleReadOnlyAccess — Aktualisierung einer bestehenden Richtlinie	Amazon FSx hat neue Berechtigungen hinzugefügt, damit Principals die Amazon Data Firehose-Lieferströme beschreiben können, die mit dem Konto verknüpft sind, das die Anfrage gestellt hat. Dies ist erforderlich, damit die Hauptbenutzer die bestehende Konfiguration für die Dateizugriffsprüfung für ein Dateisystem FSx für Windows-Dateiserver einsehen können.	8. Juni 2021
Amazon FSx hat begonnen, Änderungen zu verfolgen	Amazon FSx hat damit begonnen, Änderungen an seinen AWS verwalteten Richtlinien nachzuverfolgen.	8. Juni 2021

Fehlerbehebung bei Identität und Zugriff auf Amazon FSx for Lustre

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

Themen

Ich bin nicht berechtigt, eine Aktion in Amazon durchzuführen FSx

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht zur Durchführung einer Aktion berechtigt sind, müssen Ihre Richtlinien aktualisiert werden, damit Sie die Aktion durchführen können.

Der folgende Beispielfehler tritt auf, wenn der IAM-Benutzer `mateojackson` versucht, über die Konsole Details zu einer fiktiven *`my-example-widget`*-Ressource anzuzeigen, jedoch nicht über `fsx:`*`GetWidget`*-Berechtigungen verfügt.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

In diesem Fall muss die Richtlinie für den Benutzer `mateojackson` aktualisiert werden, damit er mit der `fsx:`*`GetWidget`*-Aktion auf die *`my-example-widget`*-Ressource zugreifen kann.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich bin nicht berechtigt, iam durchzuführen: PassRole

Wenn Sie eine Fehlermeldung erhalten, dass Sie nicht berechtigt sind, die `iam:PassRole` Aktion durchzuführen, müssen Ihre Richtlinien aktualisiert werden, damit Sie eine Rolle an Amazon weitergeben können FSx.

Einige AWS-Services ermöglichen es Ihnen, eine bestehende Rolle an diesen Service zu übergeben, anstatt eine neue Servicerolle oder eine dienstbezogene Rolle zu erstellen. Hierzu benötigen Sie Berechtigungen für die Übergabe der Rolle an den Dienst.

Der folgende Beispielfehler tritt auf, wenn ein IAM-Benutzer mit dem Namen `marymajor` versucht, die Konsole zu verwenden, um eine Aktion in Amazon FSx auszuführen. Die Aktion erfordert jedoch, dass der Service über Berechtigungen verfügt, die durch eine Servicerolle gewährt werden. Mary besitzt keine Berechtigungen für die Übergabe der Rolle an den Dienst.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In diesem Fall müssen die Richtlinien von Mary aktualisiert werden, um die Aktion `iam:PassRole` ausführen zu können.

Wenn Sie Hilfe benötigen, wenden Sie sich an Ihren AWS Administrator. Ihr Administrator hat Ihnen Ihre Anmeldeinformationen zur Verfügung gestellt.

Ich möchte Personen außerhalb von mir den Zugriff AWS-Konto auf meine FSx Amazon-Ressourcen ermöglichen

Sie können eine Rolle erstellen, mit der Benutzer in anderen Konten oder Personen außerhalb Ihrer Organisation auf Ihre Ressourcen zugreifen können. Sie können festlegen, wem die Übernahme der Rolle anvertraut wird. Für Dienste, die ressourcenbasierte Richtlinien oder Zugriffskontrolllisten (ACLs) unterstützen, können Sie diese Richtlinien verwenden, um Personen Zugriff auf Ihre Ressourcen zu gewähren.

Weitere Informationen dazu finden Sie hier:

- Informationen darüber, ob Amazon diese Funktionen FSx unterstützt, finden Sie unterSo funktioniert Amazon FSx for Lustre mit IAM.
- Informationen dazu, wie Sie Zugriff auf Ihre Ressourcen gewähren können, AWS-Konten die Ihnen gehören, finden Sie im IAM-Benutzerhandbuch unter Bereitstellen von Zugriff für einen IAM-Benutzer in einem anderen AWS-Konto , den Sie besitzen.
- Informationen dazu, wie Sie Dritten Zugriff auf Ihre Ressourcen gewähren können AWS-Konten, finden Sie AWS-Konten im IAM-Benutzerhandbuch unter Gewähren des Zugriffs für Dritte.
- Informationen dazu, wie Sie über einen Identitätsverbund Zugriff gewähren, finden Sie unter Gewähren von Zugriff für extern authentifizierte Benutzer (Identitätsverbund) im IAM-Benutzerhandbuch.
- Informationen zum Unterschied zwischen der Verwendung von Rollen und ressourcenbasierten Richtlinien für den kontoübergreifenden Zugriff finden Sie unter Kontoübergreifender Ressourcenzugriff in IAM im IAM-Benutzerhandbuch.

Verwenden von Tags mit Amazon FSx

Sie können Tags verwenden, um den Zugriff auf FSx Amazon-Ressourcen zu kontrollieren und die attributebasierte Zugriffskontrolle (ABAC) zu implementieren. Um während der Erstellung Tags auf FSx Amazon-Ressourcen anzuwenden, müssen Benutzer über bestimmte AWS Identity and Access Management (IAM-) Berechtigungen verfügen.

Erteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung

Bei einigen ressourcenschaffenden Amazon FSx for Lustre-API-Aktionen können Sie Tags angeben, wenn Sie die Ressource erstellen. Sie können diese Ressourcen-Tags verwenden, um die attributebasierte Zugriffskontrolle (ABAC) zu implementieren. Weitere Informationen finden Sie unter Wozu dient ABAC? AWS im IAM-Benutzerhandbuch.

Damit Benutzer Ressourcen bei der Erstellung taggen können, müssen sie über die Berechtigung verfügen, die Aktion zu verwenden, mit der die Ressource erstellt wurde, z. B. `fsx:CreateFileSystem` Wenn bei der Aktion zur Erstellung von Ressourcen Tags angegeben werden, führt IAM eine zusätzliche Autorisierung für die `fsx:TagResource` Aktion durch, um zu überprüfen, ob Benutzer berechtigt sind, Tags zu erstellen. 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 Tags zuzuweisen. AWS-Konto

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

In ähnlicher Weise ermöglicht die folgende Richtlinie Benutzern, Backups auf einem bestimmten Dateisystem zu erstellen und während der Backup-Erstellung beliebige Tags auf die Sicherung anzuwenden.

```
{
  "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 während der Aktion zur Erstellung der Ressource Tags angewendet werden. Daher benötigt ein Benutzer, der berechtigt ist, eine Ressource zu erstellen (vorausgesetzt, es gibt keine Tagging-Bedingungen), keine Erlaubnis, die `fsx:TagResource` Aktion zu verwenden, wenn in der Anforderung keine Tags angegeben sind. 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 zum Taggen von FSx Amazon-Ressourcen finden Sie unterTaggen Sie Ihre Amazon FSx for Lustre-Ressourcen. Weitere Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf Amazon FSx for Lustre-Ressourcen finden Sie unterVerwenden von Tags zur Steuerung des Zugriffs auf Ihre FSx Amazon-Ressourcen.

Verwenden von Tags zur Steuerung des Zugriffs auf Ihre FSx Amazon-Ressourcen

Um den Zugriff auf FSx Amazon-Ressourcen und -Aktionen zu kontrollieren, können Sie IAM-Richtlinien verwenden, die auf Tags basieren. Sie können diese Kontrolle auf zwei Arten ausüben:

- Sie können den Zugriff auf FSx Amazon-Ressourcen anhand der Tags auf diesen Ressourcen steuern.
- Sie können steuern, welche Tags in einer IAM-Anforderungsbedingung übergeben werden können.

Informationen zur Verwendung von Tags zur Steuerung des Zugriffs auf AWS Ressourcen finden Sie unter Steuern des Zugriffs mithilfe von Tags im IAM-Benutzerhandbuch. Weitere Informationen zum Taggen von FSx Amazon-Ressourcen bei der Erstellung finden Sie unterErteilen der Berechtigung zum Markieren von Ressourcen während der Erstellung. Weitere Informationen über das Markieren von -Ressourcen mit Tags finden Sie unter Taggen Sie Ihre Amazon FSx for Lustre-Ressourcen.

Bestimmung des Zugriffs auf Ressourcen basierend auf Tags

Um zu kontrollieren, welche Aktionen ein Benutzer oder eine Rolle an einer FSx Amazon-Ressource ausführen kann, können Sie Tags für die Ressource verwenden. So können Sie beispielsweise bestimmte API-Vorgänge für eine Dateisystemressource auf der Grundlage des Schlüssel-Wert-Paares des Tags der Ressource zulassen oder verbieten.

Example Beispielrichtlinie — Erstellen Sie ein Dateisystem, auf dem Sie ein bestimmtes Tag angeben

Diese Richtlinie ermöglicht es dem Benutzer, ein Dateisystem nur dann zu erstellen, wenn er es mit einem bestimmten Tag-Schlüssel-Wert-Paar kennzeichnet, 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 — Erstellen Sie Backups nur auf Dateisystemen mit einem bestimmten Tag

Diese Richtlinie ermöglicht es Benutzern, Backups nur auf Dateisystemen zu erstellen, die mit dem Schlüssel-Wert-Paar gekennzeichnet sind`key=Department, value=Finance`, und das Backup wird mit dem Tag erstellt`Deparment=Finance`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 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`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Beispielrichtlinie — Dateisysteme mit bestimmten Tags löschen

Diese Richtlinie ermöglicht es einem Benutzer, nur Dateisysteme zu löschen, die mit gekennzeichnet sind`Department=Finance`. Wenn sie ein letztes Backup erstellen, muss es mit gekennzeichnet werden`Department=Finance`. FSx Für Lustre-Dateisysteme benötigen Benutzer das Recht, `fsx:CreateBackup` das endgültige Backup zu erstellen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333: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 markiert sind`Department=Finance`, und nur auf Dateisystemen, die mit gekennzeichnet sind`Department=Finance`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateDataRepositoryTask",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:task/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Verwenden von serviceverknüpften Rollen für Amazon FSx

Amazon FSx verwendet AWS Identity and Access Management (IAM) serviceverknüpfte Rollen. Eine serviceverknüpfte Rolle ist eine einzigartige Art von IAM-Rolle, die direkt mit Amazon verknüpft ist. FSx Servicebezogene Rollen sind von Amazon vordefiniert FSx und beinhalten alle Berechtigungen, die der Service benötigt, um andere AWS Dienste in Ihrem Namen aufzurufen.

Eine serviceverknüpfte Rolle FSx erleichtert die Einrichtung von Amazon, da Sie die erforderlichen Berechtigungen nicht manuell hinzufügen müssen. Amazon FSx definiert die Berechtigungen seiner serviceverknüpften Rollen, und sofern nicht anders definiert, FSx kann nur Amazon seine Rollen übernehmen. Die definierten Berechtigungen umfassen die Vertrauens- und Berechtigungsrichtlinie. Diese Berechtigungsrichtlinie kann keinen anderen IAM-Entitäten zugewiesen werden.

Sie können eine serviceverknüpfte Rolle erst löschen, nachdem ihre verwandten Ressourcen gelöscht wurden. Dies schützt Ihre FSx Amazon-Ressourcen, da Sie die Zugriffsberechtigung für die Ressourcen nicht versehentlich entziehen können.

Informationen zu anderen Services, die serviceverknüpfte Rollen unterstützen, finden Sie unter AWS Services, die mit IAM funktionieren. Suchen Sie dort in der Spalte Service-verknüpfte Rollen nach den Services, für die Ja steht. Wählen Sie über einen Link Ja aus, um die Dokumentation zu einer serviceverknüpften Rolle für diesen Service anzuzeigen.

Servicebezogene Rollenberechtigungen für Amazon FSx

Amazon FSx verwendet zwei mit Services verknüpfte Rollen`AWSServiceRoleForFSxS3Access_`*`fs-01234567890`*, die benannt sind `AWSServiceRoleForAmazonFSx` und bestimmte Aktionen in Ihrem Konto ausführen. Beispiele für diese Aktionen sind die Erstellung elastischer Netzwerkschnittstellen für Ihre Dateisysteme in Ihrer VPC und der Zugriff auf Ihr Daten-Repository in einem Amazon S3 S3-Bucket. Denn `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`* diese serviceverknüpfte Rolle wird für jedes Amazon FSx for Lustre-Dateisystem erstellt, das Sie erstellen und das mit einem S3-Bucket verknüpft ist.

AWSServiceRoleForAmazonFSx Einzelheiten zu den Berechtigungen

Denn `AWSServiceRoleForAmazonFSx` die Rollenberechtigungsrichtlinie ermöglicht es Amazon FSx , die folgenden administrativen Aktionen im Namen des Benutzers für alle zutreffenden AWS Ressourcen durchzuführen:

Aktualisierungen dieser Richtlinie finden Sie unter Amazon FSx ServiceRolePolicy.

> **Note**
>
> Das AWSService RoleForAmazon FSx wird von allen FSx Amazon-Dateisystemtypen verwendet; einige der aufgelisteten Berechtigungen gelten nicht FSx für Lustre.

- `ds`— Ermöglicht Amazon, Anwendungen FSx in Ihrem Verzeichnis einzusehen, zu autorisieren und deren Autorisierung aufzuheben. Directory Service
- `ec2`— Ermöglicht Amazon FSx , Folgendes zu tun:
  - Netzwerkschnittstellen, die mit einem FSx Amazon-Dateisystem verknüpft sind, anzeigen, erstellen und deren Zuordnung aufheben.
  - Zeigen Sie eine oder mehrere Elastic IP-Adressen an, die mit einem FSx Amazon-Dateisystem verknüpft sind.
  - Sehen Sie sich Amazon VPCs, Sicherheitsgruppen und Subnetze an, die mit einem FSx Amazon-Dateisystem verknüpft sind.
  - Weisen Sie den Netzwerkschnittstellen von Kunden, die über ein `AmazonFSx.FileSystemId` Tag verfügen, IPv6 Adressen zu.
  - Hebt die Zuweisung von IPv6 Adressen zu Netzwerkschnittstellen von Kunden auf, die über ein `AmazonFSx.FileSystemId` Tag verfügen.
  - Um eine erweiterte Sicherheitsgruppenvalidierung aller Sicherheitsgruppen bereitzustellen, die mit einer VPC verwendet werden können.
  - Erstellen Sie eine Berechtigung für einen AWS-autorisierten Benutzer, bestimmte Operationen an einer Netzwerkschnittstelle auszuführen.
- `cloudwatch`— Ermöglicht Amazon FSx , metrische Datenpunkte CloudWatch unter dem FSx Namespace AWS/zu veröffentlichen.
- `route53`— Ermöglicht Amazon FSx , eine Amazon-VPC mit einer privaten gehosteten Zone zu verknüpfen.
- `logs`— Ermöglicht Amazon FSx , CloudWatch Log-Streams zu beschreiben und in sie zu schreiben. Auf diese Weise können Benutzer Auditprotokolle für den Dateizugriff auf ein Dateisystem FSx für Windows-Dateiserver an einen CloudWatch Logs-Stream senden.
- `firehose`— Ermöglicht Amazon FSx , Amazon Data Firehose-Lieferstreams zu beschreiben und in sie zu schreiben. Auf diese Weise können Benutzer die Dateizugriffs-Audit-Logs für ein Dateisystem FSx für Windows File Server in einem Amazon Data Firehose-Lieferstream veröffentlichen.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },
```

```
        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Alle Aktualisierungen dieser Richtlinie werden unter beschrieben FSx Aktualisierungen der AWS verwalteten Richtlinien durch Amazon.

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.

AWSServiceRoleForFSxEinzelheiten zu den S3Access-Berechtigungen

Denn die Rollenberechtigungsrichtlinie ermöglicht es Amazon `AWSServiceRoleForFSxS3Access_`*`file-system-id`* FSx , die folgenden Aktionen in einem Amazon S3-Bucket durchzuführen, der das Daten-Repository für ein Amazon FSx for Lustre-Dateisystem hostet.

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:Get*`
- `s3:List*`
- `s3:PutBucketNotification`
- `s3:PutObject`

Sie müssen Berechtigungen konfigurieren, damit eine juristische Stelle von IAM (z. B. Benutzer, Gruppe oder Rolle) eine serviceverknüpfte Rolle erstellen, bearbeiten oder löschen kann. Weitere Informationen finden Sie unter Serviceverknüpfte Rollenberechtigung im IAM-Benutzerhandbuch.

Eine servicebezogene Rolle für Amazon erstellen FSx

Sie müssen eine serviceverknüpfte Rolle nicht manuell erstellen. Wenn Sie ein Dateisystem in der AWS-Managementkonsole, der oder der AWS API erstellen AWS CLI, FSx erstellt Amazon 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, FSx erstellt Amazon die serviceverknüpfte Rolle erneut für Sie.

Bearbeitung einer serviceverknüpften Rolle für Amazon FSx

Amazon FSx erlaubt Ihnen nicht, diese serviceverknüpften Rollen zu bearbeiten. Da möglicherweise verschiedene Entitäten auf die Rolle verweisen, kann der 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 FSx Amazon-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 Rollen im FSx Zusammenhang mit Amazon Services

Amazon FSx unterstützt die Verwendung von Rollen im Zusammenhang mit Services 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 FSx Amazon-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 FSx Amazon-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 Amazon FSx elastic network interface 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 Kunden.

EFA-fähige Sicherheitsgruppen

Wenn Sie eine EFA-fähige Sicherheitsgruppe FSx für Lustre erstellen möchten, sollten Sie zunächst eine EFA-fähige Sicherheitsgruppe erstellen und diese als Sicherheitsgruppe für das Dateisystem angeben. Eine EFA erfordert eine Sicherheitsgruppe, die den gesamten ein- und ausgehenden Datenverkehr zu und von der Sicherheitsgruppe selbst und der Sicherheitsgruppe der Clients zulässt, wenn sich die Clients in einer anderen Sicherheitsgruppe befinden. Weitere Informationen finden Sie unter Schritt 1: Eine EFA-fähige Sicherheitsgruppe vorbereiten im EC2 Amazon-Benutzerhandbuch.

Steuern des Zugriffs mithilfe von Regeln für eingehenden und ausgehenden Datenverkehr

Um eine Sicherheitsgruppe zu verwenden, um den Zugriff auf Ihr FSx Amazon-Dateisystem zu kontrollieren und Lustre Clients fügen Sie die eingehenden Regeln zur Steuerung des eingehenden Datenverkehrs und die Regeln für ausgehenden Datenverkehr zur Steuerung des ausgehenden Datenverkehrs aus Ihrem Dateisystem hinzu und Lustre Kunden. Stellen Sie sicher, dass Ihre Sicherheitsgruppe über die richtigen Regeln für den Netzwerkverkehr verfügt, um die FSx Dateifreigabe Ihres Amazon-Dateisystems einem Ordner auf Ihrer unterstützten Compute-Instance zuzuordnen.

Weitere Informationen zu Sicherheitsgruppenregeln finden Sie unter Sicherheitsgruppenregeln im EC2 Amazon-Benutzerhandbuch.

Um eine Sicherheitsgruppe für Ihr FSx Amazon-Dateisystem zu erstellen

1. Öffnen Sie die EC2 Amazon-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 Ihrem FSx Amazon-Dateisystem zugeordnete 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 zur Aktivierung erstellt haben, Regeln für eingehenden Datenverkehr hinzu Lustre Datenverkehr zwischen Ihren FSx for Lustre-Dateiservern.

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,	Erlaubt Lustre Verkehr zwischen vier FSx Lustre-Dateiservern

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
			die Sie gerade erstellt haben	
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppe IDs der Sicherheitsgruppen ein, die zu Ihrem gehören Lustre clients	Erlaubt Lustre Verkehr zwischen unseren FSx Lustre-Dateiservern und Lustre clients
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-ID der Sicherheitsgruppe ein, die Sie gerade erstellt haben	Erlaubt Lustre Verkehr zwischen vier FSx Lustre-Dateiservern

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppe IDs der Sicherheitsgruppen ein, die zu Ihrem gehören Lustre clients	Erlaubt Lustre Verkehr zwischen unseren FSx 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 unseren FSx Lustre-Dateiservern und Lustre Clients und zwischen Lustre Dateiserver.

Um Ihrer Sicherheitsgruppe Regeln für ausgehenden Datenverkehr hinzuzufügen

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	Sobald Sie die Details auf dieser

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
			geben Sie die Sicherheitsgruppen-ID der Sicherheitsgruppe ein, die Sie gerade erstellt haben	Seite überprüft haben, klicken Sie auf Lustre Verkehr zwischen vier FSx Lustre-Dateiservern
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppe IDs der Sicherheitsgruppe ein, die zu Ihrem gehört Lustre clients	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf Lustre Verkehr zwischen unseren FSx Lustre-Dateiservern und Lustre clients
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppen-ID der Sicherheitsgruppe ein, die Sie gerade erstellt haben	Erlaubt Lustre Verkehr zwischen vier FSx Lustre-Dateiservern

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppe IDs der Sicherheitsgruppen ein, die zu Ihrem gehören Lustre clients	Erlaubt Lustre Verkehr zwischen unseren FSx Lustre-Dateiservern und Lustre clients

3. Wählen Sie Speichern, um die neuen Regeln für ausgehenden Datenverkehr zu speichern und anzuwenden.

So verknüpfen Sie eine Sicherheitsgruppe mit Ihrem FSx Amazon-Dateisystem

1. Öffnen Sie die FSx Amazon-Konsole unter https://console.aws.amazon.com/fsx/.
2. Wählen Sie im Konsolen-Dashboard Ihr Dateisystem aus, um dessen Details einzusehen.
3. Klicken Sie auf der Registerkarte Netzwerk und Sicherheit unter Netzwerkschnittstelle (n) auf den Link zur EC2 Amazon-Konsole, um alle Netzwerkschnittstellen für Ihr Dateisystem anzuzeigen.
4. Wählen Sie für jede Netzwerkschnittstelle Aktionen und anschließend Sicherheitsgruppen ändern aus.
5. Wählen Sie im Dialogfeld Sicherheitsgruppen ändern die Sicherheitsgruppen aus, die Sie der Netzwerkschnittstelle zuordnen möchten.
6. Wählen Sie Save (Speichern) aus.

Lustre Regeln für Client-VPC-Sicherheitsgruppen

Sie verwenden VPC-Sicherheitsgruppen, um den Zugriff auf Ihre Lustre Clients, indem Sie Regeln für eingehenden Datenverkehr hinzufügen, um den eingehenden Verkehr zu kontrollieren, und Regeln für ausgehenden Datenverkehr, um den ausgehenden Verkehr von Ihrem Lustre Kunden. Stellen Sie sicher, dass Ihre Sicherheitsgruppe über die richtigen Regeln für den Netzwerkverkehr verfügt, um

Folgendes sicherzustellen Lustre Der Verkehr kann zwischen Ihren fließen Lustre Kunden und Ihre FSx Amazon-Dateisysteme.

Fügen Sie den Sicherheitsgruppen, die auf Ihre Anwendung angewendet werden, die folgenden Regeln für eingehenden Datenverkehr hinzu Lustre Kunden.

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
Benutzerd efinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherhei tsgruppe IDs der Sicherhei tsgruppen ein, die auf Ihre angewendet werden Lustre clients	Erlaubt Lustre Verkehr zwischen Lustre clients
Benutzerd efinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherhei tsgruppe IDs der Sicherhei tsgruppen ein, die Ihren FSx for Lustre-Da teisystemen zugeordnet sind	Erlaubt Lustre Verkehr zwischen FSx Dateiservern für Lustre und Lustre clients
Benutzerd efinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherhei tsgruppe IDs	Erlaubt Lustre Verkehr zwischen Lustre clients

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
			der Sicherhei tsgruppen ein, die auf Ihre Lustre clients	
Benutzerd efinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherhei tsgruppe IDs der Sicherhei tsgruppen ein, die Ihren FSx for Lustre-Da teisystemen zugeordnet sind	Erlaubt Lustre Verkehr zwischen FSx Dateiservern für Lustre und Lustre clients

Fügen Sie den Sicherheitsgruppen, die auf Ihre Anwendung angewendet werden, die folgenden Regeln für ausgehenden Datenverkehr hinzu Lustre Kunden.

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
Benutzerd efinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherhei tsgruppe IDs der Sicherhei tsgruppen ein, die auf Ihre angewendet	Erlaubt Lustre Verkehr zwischen Lustre clients

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
			werden Lustre clients	
Benutzerdefinierte TCP-Regel	TCP	988	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppe IDs der Sicherheitsgruppen ein, die Ihren FSx for Lustre-Dateisystemen zugeordnet sind	Sobald Sie die Details auf dieser Seite überprüft haben, klicken Sie auf Lustre Verkehr zwischen FSx Dateiservern für Lustre und Lustre clients
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppe IDs der Sicherheitsgruppen ein, die auf Ihre Lustre clients	Erlaubt Lustre Verkehr zwischen Lustre clients

Typ	Protocol (Protokoll)	Port-Bereich	Quelle	Beschreibung
Benutzerdefinierte TCP-Regel	TCP	1018-1023	Wählen Sie Benutzerdefiniert und geben Sie die Sicherheitsgruppe IDs der Sicherheitsgruppen ein, die Ihren FSx for Lustre-Dateisystemen zugeordnet sind	Erlaubt Lustre Verkehr zwischen FSx Dateiservern für Lustre 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. Netzwerke 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 über das Netzwerk ACLs finden Sie unter Steuern des Datenverkehrs zu Subnetzen mithilfe des Netzwerks ACLs im Amazon VPC-Benutzerhandbuch.

Konformitätsvalidierung für Amazon FSx for Lustre

Informationen darüber, ob AWS-Service ein in den Geltungsbereich bestimmter Compliance-Programme fällt, finden Sie unter AWS-Services Umfang nach Compliance-Programm unter Umfang nach Compliance-Programm AWS-Services das Compliance-Programm aus, an dem Sie interessiert sind. Allgemeine Informationen finden Sie unter AWS Compliance-Programme AWS .

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

Ihre Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services hängt von der Vertraulichkeit Ihrer Daten, den Compliance-Zielen Ihres Unternehmens und den geltenden Gesetzen

und Vorschriften ab. Weitere Informationen zu Ihrer Verantwortung für die Einhaltung der Vorschriften bei der Nutzung AWS-Services finden Sie in der AWS Sicherheitsdokumentation.

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

Sie können die Sicherheitslage Ihrer VPC verbessern, indem Sie Amazon so konfigurieren, FSx dass es einen VPC-Endpunkt mit Schnittstelle verwendet. Interface-VPC-Endpunkte basieren auf einer Technologie AWS PrivateLink, die es Ihnen ermöglicht, privat auf Amazon zuzugreifen, FSx APIs ohne ein Internet-Gateway, ein NAT-Gerät, eine VPN-Verbindung oder Direct Connect eine Verbindung zu benötigen. Instances in Ihrer VPC benötigen keine öffentlichen IP-Adressen, um mit Amazon FSx APIs zu kommunizieren. Der Verkehr zwischen Ihrer VPC und Amazon FSx verlässt das AWS Netzwerk nicht.

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

Überlegungen zu VPC-Endpunkten mit FSx Amazon-Schnittstelle

Bevor Sie einen Schnittstellen-VPC-Endpunkt für Amazon einrichten FSx, sollten Sie die Eigenschaften und Einschränkungen von Interface VPC-Endpunkten im Amazon VPC-Benutzerhandbuch lesen.

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

Überlegungen zum VPC-Peering

Sie können mithilfe von VPCs VPC-Peering andere VPC-Endpunkte mit der VPC über die Schnittstelle verbinden. VPC-Peering ist eine Netzwerkverbindung zwischen zwei. VPCs Sie können eine VPC-Peering-Verbindung zwischen Ihren eigenen beiden VPCs oder mit einer VPC in einer anderen herstellen. AWS-Konto VPCs Sie können auch zwei verschiedene sein. AWS-Regionen

Der Verkehr zwischen Peers VPCs verbleibt im AWS Netzwerk und durchquert nicht das öffentliche Internet. Sobald VPCs das Peering abgeschlossen ist, VPCs können Ressourcen wie Amazon Elastic

Compute Cloud (Amazon EC2) -Instances in beiden über VPC-Schnittstellen-Endpunkte, die in einem der beiden erstellt wurden, auf die FSx Amazon-API zugreifen. VPCs

Erstellen eines VPC-Schnittstellen-Endpunkts für Amazon API FSx

Sie können einen VPC-Endpunkt für die FSx Amazon-API entweder mit der Amazon VPC-Konsole oder mit AWS Command Line Interface ()AWS CLI erstellen. Weitere Informationen finden Sie unter Erstellen eines Schnittstellen-VPC-Endpunkts im Amazon VPC-Benutzerhandbuch.

Eine vollständige Liste der FSx Amazon-Endpunkte finden Sie unter FSx Amazon-Endpunkte und Kontingente in der. Allgemeine Amazon Web Services-Referenz

Verwenden Sie eine der folgenden Methoden FSx, um einen VPC-Schnittstellen-Endpunkt für Amazon zu erstellen:

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

Um die private DNS-Option zu verwenden, müssen Sie die `enableDnsSupport` Attribute `enableDnsHostnames` und für Ihre VPC festlegen. Weitere Informationen finden Sie unter DNS-Unterstützung für Ihre VPC anzeigen und aktualisieren im Amazon VPC-Benutzerhandbuch.

Mit Ausnahme AWS-Regionen von China können Sie, wenn Sie privates DNS für den Endpunkt aktivieren, API-Anfragen an Amazon FSx mit dem VPC-Endpunkt stellen AWS-Region, indem Sie beispielsweise `fsx.us-east-1.amazonaws.com` seinen Standard-DNS-Namen für verwenden. Für China (Peking) und China (Ningxia) AWS-Regionen können Sie API-Anfragen mit dem VPC-Endpunkt jeweils mit `fsx-api.cn-north-1.amazonaws.com.cn` und `fsx-api.cn-northwest-1.amazonaws.com.cn` stellen.

Weitere Informationen finden Sie unter Zugreifen auf einen Service über einen Schnittstellen-VPC-Endpunkt im Amazon VPC-Benutzerhandbuch.

Erstellen einer VPC-Endpunktrichtlinie für Amazon FSx

Um den Zugriff auf die FSx Amazon-API weiter zu kontrollieren, können Sie optional eine AWS Identity and Access Management (IAM-) Richtlinie an Ihren VPC-Endpunkt anhängen. Die Richtlinie legt Folgendes fest:

- Prinzipal, der die Aktionen ausführen kann.
- Aktionen, die ausgeführt werden können
- Die Ressourcen, für die Aktionen ausgeführt werden können.

Weitere Informationen finden Sie unter Steuerung des Zugriffs auf Services mit VPC-Endpunkten im Amazon-VPC-Benutzerhandbuch.

Servicekontingente für Amazon FSx for Lustre

Im Folgenden erfahren Sie mehr über Kontingente bei der Arbeit mit Amazon FSx for Lustre.

Themen

Kontingente, die Sie erhöhen können

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

Ressource	Standard	Beschreibung
LustrePersistent: 1 Dateisysteme	100	Die maximale Anzahl von Amazon FSx for Lustre Persistent 1-Dateisystemen, die Sie in diesem Konto erstellen können.
Lustre2 persistente Dateisysteme	100	Die maximale Anzahl von Amazon FSx for Lustre Persistent 2-Dateisystemen, die Sie in diesem Konto erstellen können.
LustrePersistente Festplattenspeicherkapazität (pro Dateisystem)	102000	Die maximale Menge an Festplattenspeicherkapazität (in GiB), die Sie für ein persistentes Amazon FSx for Lustre-Dateisystem konfigurieren können.

Ressource	Standard	Beschreibung
LustrePersistent: Speicherkapazität für 1 Datei.	100800	Die maximale Speicherkapazität (in GiB), die Sie für alle Amazon FSx for Lustre Persistent 1-Dateisysteme in diesem Konto konfigurieren können.
LustreSpeicherkapazität für persistente Dateien: 2	100800	Die maximale Speicherkapazität (in GiB), die Sie für alle Amazon FSx for Lustre Persistent 2-Dateisysteme in diesem Konto konfigurieren können.
LustreScratch-Dateisysteme	100	Die maximale Anzahl von Amazon FSx for Lustre-Scratch-Dateisystemen, die Sie in diesem Konto erstellen können.
LustreScratch-Speicherkapazität	100800	Die maximale Speicherkapazität (in GiB), die Sie für alle Amazon FSx for Lustre-Scratch-Dateisysteme in diesem Konto konfigurieren können.
LustreDauerhafte Intelligent-Tiering-Durchsatzkapazität	100000	Die Gesamtmenge der Durchsatzkapazität (in MBps), die für alle Amazon FSx for Lustre Intelligent-Tiering-Dateisysteme in diesem Konto zulässig ist.

Ressource	Standard	Beschreibung
LustrePersistente Intelligent-Tiering-SSD-Lesecache-Speicherkapazität	100800	Die maximale Menge an bereitgestellter SSD-Lese-Cache-Speicherkapazität (in GiB), die Sie für alle Amazon FSx for Lustre Intelligent-Tiering-Dateisysteme in diesem Konto konfigurieren können.
LustreBackups	500	Die maximale Anzahl von benutzerinitiierten Backups, die Sie für alle Amazon FSx for Lustre-Dateisysteme 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 Lustre.
4. Wählen Sie ein Kontingent.
5. Wählen Sie „Kontingenterhöhung beantragen“ und folgen Sie den Anweisungen, um eine Kontingenterhöhung zu beantragen.
6. Um den Status der Kontingentanfrage einzusehen, wählen Sie im Navigationsbereich der Konsole die Option Kontingentanforderungsverlauf aus.

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

Ressourcenkontingente für jedes Dateisystem

Im Folgenden sind die Beschränkungen FSx für Amazon for Lustre-Ressourcen für jedes Dateisystem in einer AWS Region aufgeführt.

Ressource	Limit pro Dateisystem
Maximale Anzahl von Tags	50
Maximale Aufbewahrungsdauer für automatisierte Backups	90 Tage
Maximale Anzahl laufender Backup-Kopie-Anfragen an eine einzelne Zielregion pro Konto.	5
Anzahl der Dateiaktualisierungen aus dem verknüpften S3-Bucket pro Dateisystem	10 Millionen pro Monat
Mindestspeicherkapazität, SSD-Dateisysteme	1,2 TiB
Mindestspeicherkapazität, HDD-Dateisysteme	6 TiB
Minimaler Durchsatz pro Speichereinheit, SSD	50 MBps
Maximaler Durchsatz pro Speichereinheit, SSD	1000 MBps
Mindestdurchsatz pro Speichereinheit, HDD	12 MBps
Maximaler Durchsatz pro Speichereinheit, HDD	40 MBps

Weitere Überlegungen

Beachten Sie außerdem Folgendes:

- Sie können jede Taste AWS Key Management Service (AWS KMS) auf bis zu 125 Amazon FSx for Lustre-Dateisystemen verwenden.
- Eine Liste der AWS Regionen, in denen Sie Dateisysteme erstellen können, finden Sie unter Amazon FSx Endpoints and Quotas in der Allgemeine AWS-Referenz.

Problembehebung bei Amazon FSx for Lustre

In diesem Abschnitt werden verschiedene Problemlösungsszenarien und Lösungen für Amazon FSx for Lustre-Dateisysteme behandelt.

Wenn Sie auf Probleme stoßen, die im Folgenden nicht aufgeführt sind, versuchen Sie, eine Frage im Amazon FSx for Lustre-Forum zu stellen.

Themen

Das Erstellen eines FSx for Lustre-Dateisystems 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 EFA-fähiges Dateisystem erstellt werden

Das Erstellen eines EFA-fähigen Dateisystems FSx für Lustre schlägt mit der folgenden Fehlermeldung fehl:

```
Insufficient security group permissions to create an EFA-enabled file system.
Update security group to allow all internal inbound and outbound traffic.
```

Maßnahme

Stellen Sie sicher, dass die VPC-Sicherheitsgruppe, die Sie für den Erstellungsvorgang verwenden, wie unter beschrieben konfiguriert ist. EFA-fähige Sicherheitsgruppen Eine EFA erfordert eine

Sicherheitsgruppe, die den gesamten eingehenden und ausgehenden Datenverkehr zur und von der Sicherheitsgruppe selbst und zur Sicherheitsgruppe der Clients zulässt, wenn sich die Clients in einer anderen Sicherheitsgruppe befinden.

Aufgrund einer falsch konfigurierten Sicherheitsgruppe kann kein Dateisystem erstellt werden

Das Erstellen eines FSx For Lustre-Dateisystems schlägt fehl und es wird die folgende Fehlermeldung angezeigt:

```
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.

Ein Dateisystem kann aufgrund von Fehlern aufgrund unzureichender Kapazität nicht erstellt werden

Möglicherweise wird ein Fehler mit unzureichender Kapazität angezeigt, wenn Sie versuchen, ein neues Dateisystem zu erstellen, die Speicherkapazität zu aktualisieren oder die Durchsatzkapazität zu ändern.

Ursache

Dieser Fehler tritt auf, wenn FSx for Lustre derzeit nicht über genügend Hardwarekapazität in der angeforderten Availability Zone verfügt, um Ihre Anfrage zu bearbeiten.

Lösung

Versuchen Sie, das Problem wie folgt zu beheben:

- Warten Sie einige Minuten und wiederholen Sie Ihre Anfrage, da sich die Kapazitätsverfügbarkeit häufig ändert.

- Testen Sie Ihre Anfrage in einer anderen Availability Zone.
- Versuchen Sie den Vorgang mit einer kleineren Speichergröße oder einem niedrigeren Durchsatz

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 Amazon FSx for Lustre-Rolle, 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 auch das Hinzufügen der Berechtigungsrichtlinie, die die serviceverknüpfte Amazon FSx for Lustre-Rolle unterstützt. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zur Verwendung von Datenrepositorys in Amazon S3.

Weitere Informationen zu serviceverknüpften Rollen finden Sie unter Verwenden von serviceverknüpften Rollen für Amazon FSx.

Behebung von Problemen beim Einhängen des Dateisystems

Es gibt eine Reihe möglicher Ursachen, wenn ein Befehl zum Einhängen eines Dateisystems fehlschlägt, wie in den folgenden Themen beschrieben.

Das Einhängen des Dateisystems schlägt sofort fehl

Der Befehl zum Einhängen des Dateisystems schlägt sofort fehl. Der folgende Code zeigt ein Beispiel dafür.

```
mount.lustre: mount fs-0123456789abcdef0.fsx.us-east-1.aws@tcp:/fsx at /lustre
```

```
failed: No such file or directory

Is the MGS specification correct?
Is the filesystem name correct?
```

Dieser Fehler kann auftreten, wenn Sie beim Mounten eines persistenten Dateisystems oder eines Scratch-2-Dateisystems mithilfe des mount Befehls nicht den richtigen `mountname` Wert verwenden. Sie können den `mountname` Wert aus der Antwort des describe-file-systems AWS CLI Befehls oder der DescribeFileSystemsAPI-Operation abrufen.

Das Mounting des Dateisystems hängt und schlägt dann mit einem Timeout-Fehler fehl

Der Mounting-Befehl des Dateisystems hängt eine oder zwei Minuten lang und schlägt dann mit einem Timeout-Fehler fehl.

Der folgende Code zeigt ein Beispiel dafür.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx

[2+ minute wait here]
Connection timed out
```

Dieser Fehler kann auftreten, weil die Sicherheitsgruppen für die EC2 Amazon-Instance oder das Dateisystem nicht richtig konfiguriert sind.

Maßnahme

Stellen Sie sicher, dass Ihre Sicherheitsgruppen für das Dateisystem die unter angegebenen Regeln für eingehenden Datenverkehr haben. Amazon VPC-Sicherheitsgruppen

Automatisches Mounting schlägt fehl und die Instance reagiert nicht

In einigen Fällen schlägt das automatische Mounten für ein Dateisystem möglicherweise fehl und Ihre EC2 Amazon-Instance reagiert möglicherweise nicht mehr.

Dieses Problem kann auftreten, wenn die `_netdev` Option nicht deklariert wurde. Wenn `_netdev` es fehlt, reagiert Ihre EC2 Amazon-Instance möglicherweise nicht mehr. Der Grund dafür ist, dass zuerst das Netzwerk auf der Datenverarbeitungs-Instance gestartet worden sein muss. Die Netzwerkdateisysteme müssen danach initialisiert werden.

Maßnahme

Wenn dieses Problem auftritt, wenden Sie sich an AWS Support.

Das Einhängen des Dateisystems schlägt beim Systemstart fehl

Das Einhängen des Dateisystems schlägt beim Systemstart fehl. Die Montage erfolgt automatisiert mit`/etc/fstab`. Wenn das Dateisystem nicht gemountet ist, wird im Syslog für den Zeitraum, in dem die Instanz gestartet wurde, der folgende Fehler angezeigt.

```
LNetError: 3135:0:(lib-socket.c:583:lnet_sock_listen()) Can't create socket: port 988
 already in use
LNetError: 122-1: Can't start acceptor on port 988: port already in use
```

Dieser Fehler kann auftreten, wenn Port 988 nicht verfügbar ist. Wenn die Instanz für das Mounten von NFS-Dateisystemen konfiguriert ist, ist es möglich, dass die NFS-Mounts ihren Client-Port an Port 988 binden

Maßnahme

Sie können dieses Problem umgehen, indem Sie die Optionen des NFS-Clients `noresvport` und `noauto` der Mount-Optionen nach Möglichkeit anpassen.

Das Einhängen des Dateisystems mithilfe des DNS-Namens schlägt fehl

Falsch konfigurierte DNS-Namen (Domain Name Service) können zu Fehlern beim Einhängen des Dateisystems führen, wie in den folgenden Szenarien gezeigt.

Szenario 1: Eine Dateisystembereitstellung, die einen DNS-Namen (Domain Name Service) verwendet, schlägt fehl. Der folgende Code zeigt ein Beispiel dafür.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: Can't parse NID
'file_system_dns_name@tcp:/mountname'
```

Maßnahme

Überprüfen Sie Ihre Virtual Private Cloud (VPC) -Konfiguration. Wenn Sie eine benutzerdefinierte VPC verwenden, müssen Sie sicherstellen, dass die DNS-Einstellungen aktiviert sind.
Weitere Informationen finden Sie unter Verwendung von DNS in Ihrer VPC im Amazon VPC Benutzerhandbuch.

Gehen Sie wie folgt vor, um im `mount` Befehl einen DNS-Namen anzugeben:

- Stellen Sie sicher, dass sich die EC2 Amazon-Instance in derselben VPC wie Ihr Amazon FSx for Lustre-Dateisystem befindet.
- Connect Ihre EC2 Amazon-Instance mit 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 EC2 Amazon-Instance DNS-Hostnamen aktiviert sind. Weitere Informationen finden Sie unter Aktualisieren der DNS-Unterstützung für Ihre VPC im Amazon VPC-Benutzerhandbuch.

Szenario 2: Ein Dateisystem-Mount, der einen DNS-Namen (Domain Name Service) verwendet, schlägt fehl. Der folgende Code zeigt ein Beispiel dafür.

```
mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: mount file_system_dns_name@tcp:/mountname at /mnt/fsx failed: Input/
output error Is the MGS running?
```

Maßnahme

Stellen Sie sicher, dass auf die VPC-Sicherheitsgruppen des Clients die richtigen Regeln für ausgehenden Datenverkehr angewendet werden. Diese Empfehlung gilt insbesondere dann, wenn Sie die Standardsicherheitsgruppe nicht verwenden oder wenn Sie die Standardsicherheitsgruppe geändert haben. Weitere Informationen finden Sie unter Amazon VPC-Sicherheitsgruppen.

Sie können nicht auf Ihr Dateisystem zugreifen

Es gibt eine Reihe möglicher Ursachen dafür, dass Sie nicht auf Ihr Dateisystem zugreifen können. Jede hat ihre eigene Auflösung, wie folgt.

Die Elastic IP-Adresse, die an die elastic network interface des Dateisystems angehängt ist, wurde gelöscht

Amazon unterstützt den Zugriff auf Dateisysteme über das öffentliche Internet FSx nicht. Amazon trennt FSx 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 eines DRA nicht validiert werden

Das Erstellen einer Data Repository Association (DRA) über die FSx Amazon-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 über die FSx Amazon-Konsole oder den `create-file-system` CLI-Befehl (entspricht der entsprechenden API-Aktion) mit einem Datenrepository (S3-Bucket oder Präfix) verknüpft CreateFileSystemist.

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 Amazon FSx for Lustre-Rolle, 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 der Zugriff von dem Konto aus möglich ist, in dem der FSx for Lustre erstellt wurde.

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 es vorkommen, dass der verknüpfte S3-Bucket eines FSx for Lustre-Dateisystems einen falsch konfigurierten Lebenszyklusstatus für das Datenrepository aufweist.

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 Amazon FSx for Lustre-Rolle, 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 auch das Hinzufügen der Berechtigungsrichtlinie, die die serviceverknüpfte Amazon FSx for Lustre-Rolle unterstützt. Weitere Informationen finden Sie unter Hinzufügen von Berechtigungen zur Verwendung von Datenrepositorys 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-Datenrepository über eine bestehende Konfiguration für Ereignisbenachrichtigungen mit Ereignistypen verfügt, die sich mit der Amazon-Konfiguration für FSx Ereignisbenachrichtigungen (`s3:ObjectCreated:*`,`s3:ObjectRemoved:*`) überschneiden.

Dies kann auch der Fall sein, wenn die Konfiguration der FSx Amazon-Ereignisbenachrichtigung im verknüpften S3-Bucket gelöscht oder geändert wurde.

Maßnahme

1. Entfernen Sie alle vorhandenen Ereignisbenachrichtigungen aus dem verknüpften S3-Bucket, die einen oder beide Ereignistypen verwenden, die in der FSx Ereigniskonfiguration verwendet werden, `s3:ObjectCreated:*` und`s3:ObjectRemoved:*`.
2. Stellen Sie sicher, dass sich in Ihrem verknüpften S3-Bucket eine Konfiguration für S3-Ereignisbenachrichtigungen mit dem Namen`FSx`, den Ereignistypen `s3:ObjectCreated:*` und `s3:ObjectRemoved:*` der Option „Senden“ an das SNS-Thema befindet. 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 beschriebenSpeicherlayout des Dateisystems. Das `filesystem_summary` Feld gibt die gesamte Speichernutzung des Dateisystems an.

Wenn die Festplattenauslastung des Dateisystems bei 100% liegt, sollten Sie erwägen, die Speicherkapazität Ihres Dateisystems zu erhöhen. Weitere Informationen finden Sie unter Verwaltung der Speicherkapazität.

Wenn die Speicherauslastung des Dateisystems nicht zu 100% beträgt und Sie immer noch Schreibfehler erhalten, kann es sein, dass die Datei, in die Sie schreiben, auf einem vollen OST gestreift wird.

Maßnahme

- Wenn viele Ihrer Dateien voll OSTs sind, erhöhen Sie die Speicherkapazität Ihres Dateisystems. Prüfen Sie, ob unsymmetrischer Speicher aktiviert ist, OSTs indem Sie den Anweisungen im Unausgeglichener Speicher aktiviert OSTs Abschnitt folgen.
- Wenn Sie nicht voll OSTs sind, optimieren Sie die Größe des Client-Buffers für Dirty Page, indem Sie die folgende Optimierung auf alle Ihre Client-Instances anwenden:

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

Unausgeglichener Speicher aktiviert OSTs

Amazon FSx for Lustre verteilt neue Dateistreifen gleichmäßig auf die einzelnen Dateien. 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 „mehr voll“ in „weniger voll“ zu verschieben. OSTs 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 EC2 `c5n.4xlarge` Amazon-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 0STS durch die Werte von Ihrem OSTs.
  - Geben Sie einen Integer-Wert für annproc, um die Anzahl der Max-Procs-Prozesse festzulegen, die parallel ausgeführt werden sollen. Der EC2 `c5n.4xlarge` Amazon-Instance-Typ hat beispielsweise 16 vCPUs, sodass Sie 16 (oder einen Wert < 16) für verwenden könnennproc.
  - Geben Sie Ihren Mount-Verzeichnispfad in einmnt_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 feststellt, OSTs dass mehr als 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 unterStriping von Daten in Ihrem Dateisystem.

Fehlerbehebung FSx bei Problemen mit dem Lustre CSI-Treiber

Amazon FSx for Lustre unterstützt den Zugriff von Containern, die auf Amazon EKS laufen, mithilfe des Open-Source-CSI-Treibers FSx für Lustre. Informationen zur Bereitstellung finden Sie unter Verwenden von Amazon FSx for Lustre Storage im Amazon EKS-Benutzerhandbuch.

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 zu unterstützten, aber veralteten FSx Amazon-Funktionen.

Themen

Einen benutzerdefinierten Backup-Zeitplan einrichten

Wir empfehlen AWS Backup die Verwendung, um einen benutzerdefinierten Backup-Zeitplan für Ihr Dateisystem einzurichten. Die hier bereitgestellten Informationen dienen zu Referenzzwecken, falls Sie Backups häufiger planen müssen, als dies bei der Verwendung möglich ist AWS Backup.

Wenn diese Option aktiviert ist, erstellt Amazon innerhalb eines täglichen Backup-Fensters FSx automatisch einmal täglich eine Sicherungskopie Ihres Dateisystems. Amazon FSx erzwingt eine Aufbewahrungsfrist, die 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 Implementierung einer benutzerdefinierten Backup-Planung. Die benutzerdefinierte Sicherungsplanung führt vom Benutzer initiierte Backups auf einem Amazon FSx for Lustre-Dateisystem nach einem von Ihnen definierten Zeitplan durch. Beispiele könnten einmal alle sechs Stunden, einmal pro Woche usw. sein. Dieses Skript konfiguriert auch das Löschen von Backups, die älter als der angegebene Aufbewahrungszeitraum sind.

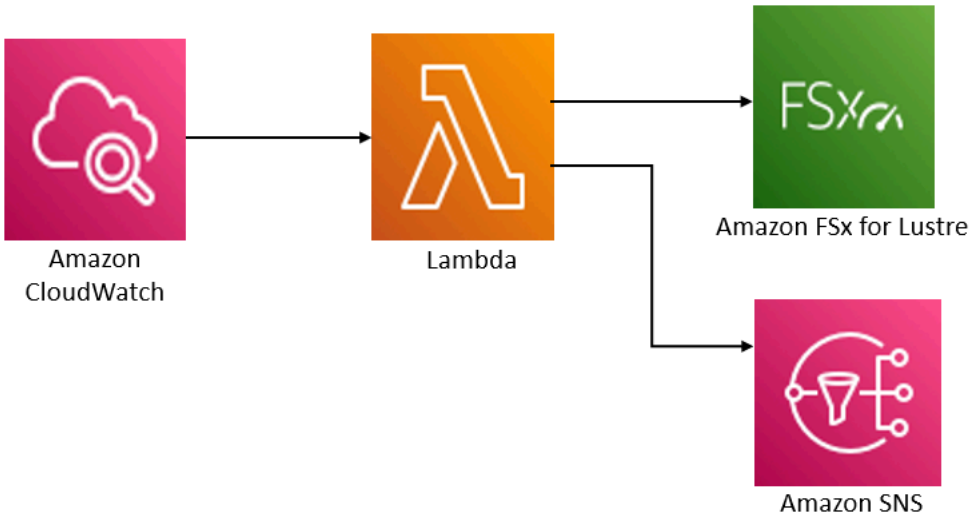
Die Lösung stellt automatisch alle benötigten Komponenten bereit und berücksichtigt die folgenden Parameter:

- Das Dateisystem
- Ein CRON-Zeitplanmuster für die Durchführung von Backups
- Die Aufbewahrungsfrist für Backups (in Tagen)
- Die Backup-Namensschilder

Weitere Informationen zu CRON-Zeitplanmustern finden Sie unter Schedule Expressions for Rules im CloudWatch Amazon-Benutzerhandbuch.

Übersicht über die Architektur

Durch die Bereitstellung dieser Lösung werden die folgenden Ressourcen in der AWS Cloud bereitgestellt.



Diese Lösung macht Folgendes:

1. Die CloudFormation Vorlage stellt ein CloudWatch Ereignis, eine Lambda-Funktion, eine Amazon SNS SNS-Warteschlange und eine IAM-Rolle bereit. Die IAM-Rolle erteilt der Lambda-Funktion die Erlaubnis, die Amazon FSx for Lustre-API-Operationen aufzurufen.
2. Das CloudWatch Ereignis wird während der ersten Bereitstellung nach einem Zeitplan ausgeführt, den Sie als CRON-Muster definiert haben. Dieses Ereignis ruft die Backup-Manager-Lambda-Funktion der Lösung auf, die den Amazon FSx for `CreateBackup` Lustre-API-Vorgang aufruft, um ein Backup zu initiieren.
3. Der Backup-Manager ruft mithilfe von eine Liste vorhandener benutzerinitiierter Backups für das angegebene Dateisystem ab. `DescribeBackups` Anschließend werden Backups gelöscht, die älter sind als der Aufbewahrungszeitraum, den Sie bei der ersten Bereitstellung angegeben haben.
4. Der Backup-Manager sendet bei einem erfolgreichen Backup eine Benachrichtigung an die Amazon SNS SNS-Warteschlange, wenn Sie die Option wählen, bei der ersten Bereitstellung benachrichtigt zu werden. Im Falle eines Fehlers wird immer eine Benachrichtigung gesendet.

CloudFormation Vorlage

Diese Lösung automatisiert CloudFormation die Bereitstellung der benutzerdefinierten Backup-Planungslösung von Amazon FSx for Lustre. Um diese Lösung zu verwenden, laden Sie die fsx-scheduled-backupVorlage .template CloudFormation herunter.

Automatisierte Bereitstellung

Mit dem folgenden Verfahren wird diese benutzerdefinierte Lösung zur Planung von Backups konfiguriert und bereitgestellt. Die Bereitstellung dauert etwa fünf Minuten. Bevor Sie beginnen, müssen Sie die ID eines Amazon FSx for Lustre-Dateisystems, das in einer Amazon Virtual Private Cloud (Amazon VPC) läuft, in Ihrem AWS Konto haben. Weitere Informationen zur Erstellung dieser Ressourcen finden Sie unter. Erste Schritte mit Amazon FSx for Lustre

> **Note**
>
> Bei der Implementierung dieser Lösung müssen die zugehörigen AWS Dienste in Rechnung gestellt werden. Weitere Informationen finden Sie auf den Seiten mit den Preisdetails für diese Dienste.

Um den Stack für benutzerdefinierte Backup-Lösungen zu starten

1. Laden Sie die fsx-scheduled-backupVorlage CloudFormation .template herunter. Weitere Informationen zum Erstellen eines CloudFormation Stacks finden Sie im AWS CloudFormation Benutzerhandbuch unter Erstellen eines Stacks auf der AWS CloudFormation Konsole.

   > **Note**
   >
   > Standardmäßig wird diese Vorlage in der AWS Region USA Ost (Nord-Virginia) gestartet. Amazon FSx for Lustre ist derzeit nur in bestimmten AWS-Regionen Fällen verfügbar. Sie müssen diese Lösung in einer AWS Region einführen, in der Amazon FSx for Lustre verfügbar ist. Weitere Informationen finden Sie auf der Amazon FSx Abschnitt von AWS-Regionen und Endpunkte in der Allgemeine AWS-Referenz.

2. Überprüfen Sie unter Parameter die Parameter für die Vorlage und ändern Sie sie an die Anforderungen Ihres Dateisystems. Diese Lösung verwendet die folgenden Standardwerte.

Parameter	Standard	Beschreibung
Dateisystem-ID von Amazon FSx for Lustre	Kein Standardwert	Die Dateisystem-ID für das Dateisystem, das Sie sichern möchten.
CRON-Zeitplanmuster für Backups.	0 0/4 * *? *	Der Zeitplan für die Ausführung des CloudWatch Ereignisses, das Auslösen eines neuen Backups und das Löschen alter Backups außerhalb des Aufbewahrungszeitraums.
Aufbewahrung von Backup (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 Backups	Der Name für diese Backups, der in der Spalte Backup-Name der Amazon FSx for Lustre-Managementkonsole angezeigt wird.
Backup-Benachrichtigungen	Ja	Wählen Sie aus, ob Sie benachrichtigt werden möchten, wenn Backups erfolgreich initiiert wurden. Bei einem Fehler wird immer eine Benachrichtigung gesendet.

Parameter	Standard	Beschreibung
E-Mail-Adresse	Kein Standardwert	Die E-Mail-Adresse, um die SNS-Benachrichtigungen zu abonnieren.

3. Wählen Sie Weiter.
4. Wählen Sie unter Optionen die Option Weiter aus.
5. Überprüfen und bestätigen Sie die Einstellungen zur Überprüfung. Sie müssen das Kontrollkästchen aktivieren, das bestätigt, dass die Vorlage IAM-Ressourcen erstellt.
6. Wählen Sie Create aus, um den Stack bereitzustellen.

Sie können den Status des Stacks in der CloudFormation Konsole in der Spalte Status einsehen. In etwa fünf Minuten sollte der Status CREATE_COMPLETE angezeigt werden.

Zusätzliche Optionen

Sie können die mit dieser Lösung erstellte Lambda-Funktion verwenden, um benutzerdefinierte geplante Backups von mehr als einem Amazon FSx for Lustre-Dateisystem durchzuführen. Die Dateisystem-ID wird im Eingabe-JSON FSx für das CloudWatch Ereignis an die Amazon for Lustre-Funktion übergeben. Das Standard-JSON, das an die Lambda-Funktion übergeben wird, lautet wie folgt, wobei die Werte für `FileSystemId` und aus den Parametern übergeben `SuccessNotification` werden, die beim Starten des CloudFormation Stacks 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 Schedule-Ereignisquelle mit der von dieser Lösung erstellten Lambda-Funktion als Ziel. Wählen Sie unter Eingabe konfigurieren die Option Constant (JSON-Text) aus. Ersetzen Sie für die JSON-Eingabe einfach die Dateisystem-ID des Amazon FSx for Lustre-Dateisystems, das gesichert werden soll, anstelle von`${FileSystemId}`. Ersetzen Sie außerdem `No` im obigen JSON-Code entweder `Yes` oder anstelle von`${SuccessNotification}`.

Alle zusätzlichen CloudWatch Event-Regeln, die Sie manuell erstellen, gehören nicht zum Paket der individuell geplanten Backup-Lösungen von Amazon FSx for Lustre CloudFormation . Sie werden also nicht entfernt, wenn Sie den Stack löschen.

Dokumentverlauf

- API-Version: 01.03.2018
- Letzte Aktualisierung der Dokumentation: 30. September 2025

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
Zusätzliche AWS-Region Unterstützung für den Bereitstellungstyp Persistent 2 hinzugefügt	Persistent 2 SSD FSx für Lustre-Dateisysteme sind jetzt in der lokalen Zone USA West (Phoenix) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit der Bereitstellungstypen.	30. September 2025
LustreClient-Unterstützung für Ubuntu 24 Kernel 6.14.0 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen Ubuntu 24.04 Kernel 6.14.0 ausgeführt wird. Weitere Informationen finden Sie unter Installation des Clients. Lustre	24. September 2025
LustreClient-Unterstützung für Amazon Linux 2023 Kernel 6.12 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen Amazon Linux 2023 Kernel 6.12 ausgeführt wird. Weitere Informationen finden Sie unter Installation des Lustre Clients.	9. September 2025

Zusätzliche AWS-Region Unterstützung hinzugefügt	FSx Dateisysteme für Lustre sind jetzt im asiatisch-pazifischen Raum (Taipeh) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit der Bereitstellungstypen.	18. August 2025
Amazon hat die von Amazon FSx ServiceRolePolicy AWS verwaltete Richtlinie FSx aktualisiert	Amazon FSx hat dem Amazon die `ec2:UnassignIpv6Addresses` Berechtigungen `ec2:AssignIpv6Addresses` und hinzugefügt FSxServiceRolePolicy. Weitere Informationen finden Sie unter FSx Amazon-Updates zu AWS verwalteten Richtlinien.	22. Juli 2025
LustreClient-Unterstützung für Rocky Linux und Red Hat Enterprise Linux (RHEL) 9.6 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen Rocky Linux und Red Hat Enterprise Linux (RHEL) 9.6 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Lustre Clients.	1. Juli 2025

Amazon hat die von Amazon FSx FullAccess AWS verwaltete Richtlinie FSx aktualisiert	Die von Amazon FSx FullAccess verwaltete Richtlinie wurde aktualisiert, um die `fsx:DetachAndDeleteS3AccessPoint` Berechtigungen `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , und hinzuzufügen.	25. Juni 2025
Amazon hat die von Amazon FSx ConsoleFullAccess AWS verwaltete Richtlinie FSx aktualisiert	Die von Amazon FSx ConsoleFullAccess verwaltete Richtlinie wurde aktualisiert, um die `fsx:DetachAndDeleteS3AccessPoint` Berechtigungen `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , und hinzuzufügen.	25. Juni 2025

Support für die Intelligent-Tiering-Speicherklasse hinzugefügt	Sie können jetzt Dateisysteme FSx für Lustre mit der Intelligent-Tiering-Speicherklasse erstellen. Intelligent-Tiering bietet vollständig elastischen Speicher mit einem optionalen SSD-Cache für den Zugriff auf häufig aufgerufene Daten mit geringer Latenz. Weitere Informationen finden Sie unter Leistungsmerkmale der Intelligent-Tiering-Speicherklasse.	29. Mai 2025
Zusätzliche Unterstützung hinzugefügt AWS-Region	FSx for Lustre-Dateisysteme sind jetzt in Asien-Pazifik (Thailand) und Mexiko (Zentral) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit der Bereitstellungstypen.	8. Mai 2025
LustreClient-Unterstützung für Ubuntu 24 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen Ubuntu 24.04 ausgeführt wird. Weitere Informationen finden Sie unter Installation des Clients. Lustre	19. März 2025

Amazon hat die von Amazon FSx ConsoleReadOnlyAccess AWS verwaltete Richtlinie FSx aktualisiert	Amazon hat die FSx ConsoleReadOnlyAccess Amazon-Richtlinie FSx aktualisiert, um die `ec2:DescribeNetworkInterfaces` Genehmigung hinzuzufügen. Weitere Informationen finden Sie in der FSxConsoleReadOnlyAccessAmazon-Richtlinie.	25. Februar 2025
Support für das Upgrade der Lustre-Version hinzugefügt	Sie können jetzt die Lustre-Version Ihres FSx for Lustre-Dateisystems auf eine neuere Version aktualisieren. Weitere Informationen finden Sie unter Lustre-Version verwalten.	12. Februar 2025
Amazon hat die von Amazon FSx ConsoleFullAccess AWS verwaltete Richtlinie FSx aktualisiert	Amazon hat die FSx ConsoleFullAccess Amazon-Richtlinie FSx aktualisiert, um die `ec2:DescribeNetworkInterfaces` Genehmigung hinzuzufügen. Weitere Informationen finden Sie in der FSxConsoleFullAccessAmazon-Richtlinie.	7. Februar 2025
Zusätzliche AWS-Region Unterstützung für den Bereitstellungstyp Persistent 2 hinzugefügt	Persistent 2 SSD FSx für Lustre-Dateisysteme sind jetzt im asiatisch-pazifischen Raum (Malaysia) AWS-Region erhältlich. Weitere Informationen finden Sie unter Verfügbarkeit der Bereitstellungstypen.	2. Januar 2025

LustreClient-Unterstützung für Rocky Linux und Red Hat Enterprise Linux (RHEL) 9.5 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen Rocky Linux und Red Hat Enterprise Linux (RHEL) 9.5 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Lustre Clients.	26. Dezember 2024
Support für EFA hinzugefügt	Sie können jetzt ein Dateisystem FSx für Lustre Persistent 2 mit Unterstützung für Elastic Fabric Adapter (EFA) erstellen, das eine höhere Netzwerkleistung für Client-Instances bietet, die EFA unterstützen. Durch die Aktivierung von EFA werden auch GPUDirect Storage (GDS) und ENA Express unterstützt. Weitere Informationen finden Sie unter Arbeiten mit EFA-fähigen Dateisystemen.	27. November 2024
Zusätzliche AWS-Region Unterstützung für den Bereitstellungstyp Persistent 2 hinzugefügt	Persistent 2 SSD FSx für Lustre-Dateisysteme sind jetzt in den USA West (Nordkalifornien) AWS-Region verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit der Bereitstellungstypen.	27. November 2024

LustreClient-Unterstützung für Ubuntu 22 Kernel 6.8.0 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen Ubuntu 22.04 Kernel 6.8.0 ausgeführt wird. Weitere Informationen finden Sie unter Installation des Clients. Lustre	8. November 2024
Support für zusätzliche CloudWatch Amazon-Metriken und ein verbessertes Monitoring-Dashboard hinzugefügt	FSx for Lustre bietet jetzt zusätzliche Netzwerk-, Leistungs- und Speichermetriken sowie ein erweitertes Monitoring-Dashboard für einen besseren Einblick in die Dateisystemaktivitäten. Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch.	25. September 2024
Zusätzliche AWS-Region Unterstützung für den Bereitstellungstyp Persistent 2 hinzugefügt	Persistent 2 SSD FSx für Lustre-Dateisysteme sind jetzt in der lokalen Zone USA Ost (Dallas) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit der Bereitstellungstypen.	20. September 2024
LustreClient-Unterstützung für Ubuntu 22 Kernel 6.5.0 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen Ubuntu 22.04 Kernel 6.5.0 ausgeführt wird. Weitere Informationen finden Sie unter Installation des Clients. Lustre	1. August 2024

LustreClient-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.10 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.10 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Clients. Lustre	18. Juni 2024
Support zur Steigerung der Metadaten-Performance hinzugefügt	Sie können jetzt ein Dateisyst em FSx für Lustre Persisten t 2 mit einer Metadaten konfiguration erstellen, die die Möglichkeit bietet, die Metadaten-Performance zu erhöhen. Weitere Informati onen finden Sie unter Leistung von Dateisystem-Metadaten und Verwaltung der Leistung von Metadaten.	6. Juni 2024
Zusätzliche AWS-Regio n Unterstützung für den Bereitstellungstyp Persistent 2 hinzugefügt	Persistent 2 SSD FSx für Lustre-Dateisysteme sind jetzt in der lokalen Zone USA Ost (Atlanta) verfügbar. Weitere Informationen finden Sie unter Verfügbarkeit der Bereitste llungstypen.	29. Mai 2024
LustreClient-Unterstützung für Rocky Linux und Red Hat Enterprise Linux (RHEL) 9.4 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen Rocky Linux und Red Hat Enterprise Linux (RHEL) 9.4 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Lustre Clients.	16. Mai 2024

Zusätzliche AWS-Region Unterstützung für den Bereitstellungstyp Persistent 2 hinzugefügt	Persistent 2 SSD FSx für Lustre-Dateisysteme sind jetzt in Kanada West (Calgary) erhältlich. AWS-Region Weitere Informationen finden Sie unter Verfügbarkeit der Bereitstellungstypen.	3. Mai 2024
LustreClient-Unterstützung für Amazon Linux 2023 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen Amazon Linux 2023 ausgeführt wird. Weitere Informationen finden Sie unter Installation des Lustre Clients.	25. März 2024
LustreClient-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.9 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.9 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Clients. Lustre	9. Januar 2024

Amazon hat die von Amazon FSx FullAccess FSxConsoleFullAccess, Amazon FSx ReadOnlyAccess FSxConsoleReadOnlyAccess, Amazon und Amazon FSx ServiceRolePolicy AWS verwalteten Richtlinien FSx aktualisiert	Amazon hat die FSx ServiceRolePolicy Richtlinien von Amazon FSx FullAccess FSxConsoleFullAccess, Amazon FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon und Amazon FSx aktualisiert, um die `ec2:GetSecurityGroupsForVpc` Genehmigung hinzuzufügen. Weitere Informationen finden Sie unter FSx Amazon-Updates zu AWS verwalteten Richtlinien.	9. Januar 2024
LustreClient-Unterstützung für Rocky Linux und Red Hat Enterprise Linux (RHEL) 9.0 und 9.3 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen 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 von Amazon FSx FullAccess und von Amazon FSx ConsoleFullAccess AWS verwalteten Richtlinien aktualisiert	Amazon hat die FSx ConsoleFullAccess Richtlinien von Amazon FSx FullAccess und Amazon FSx aktualisiert, um die `ManageCrossAccountDataReplication` Aktion hinzuzufügen. Weitere Informationen finden Sie unter FSx Amazon-Updates zu AWS verwalteten Richtlinien.	20. Dezember 2023

Amazon hat die von Amazon FSx FullAccess und von Amazon FSx ConsoleFullAccess AWS verwalteten Richtlinien FSx aktualisiert	Amazon hat die FSx ConsoleFullAccess Richtlinien von Amazon FSx FullAccess und Amazon FSx aktualisiert, um die `fsx:CopySnapshotAndUpdateVolume` Genehmigung hinzuzufügen. Weitere Informationen finden Sie unter FSx Amazon-Updates zu AWS verwalteten Richtlinien.	26. November 2023
Support für die Skalierung der Durchsatzkapazität hinzugefügt	Sie können jetzt die Durchsatzkapazität für bestehende persistente SSD-basierte Dateisysteme FSx für Lustre ändern, wenn sich Ihre Durchsatzanforderungen ändern. Weitere Informationen finden Sie unter Verwaltung der Durchsatzkapazität.	16. November 2023
Amazon hat die von Amazon FSx FullAccess und von Amazon FSx ConsoleFullAccess AWS verwalteten Richtlinien FSx aktualisiert	Amazon hat die FSx ConsoleFullAccess Richtlinien von Amazon FSx FullAccess und Amazon FSx aktualisiert, um die `fsx:UpdateSharedVPCConfiguration` Berechtigungen `fsx:DescribeSharedVPCConfiguration` und hinzuzufügen. Weitere Informationen finden Sie unter FSx Amazon-Updates zu AWS verwalteten 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 FSx Amazon-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 2 hinzugefügt	Persistent 2 FSx für Lustre-Dateisysteme sind jetzt in Israel (Tel Aviv) AWS-Region verfügbar. Weitere Informationen finden Sie unter Bereitstellungsoptionen FSx für Lustre-Dateisysteme.	24. August 2023

Support für Release-Daten-Repository-Aufgaben hinzugefügt	FSx for Lustre bietet jetzt Release-Daten-Repository-Aufgaben zur Freigabe archivierter Dateien aus einem Dateisystem, das mit einem S3-Datenrepository verknüpft ist. Beim Freigeben einer Datei werden die Dateiliste und die Metadaten beibehalten, die lokale Kopie des Dateiinhalts wird jedoch entfernt. Weitere Informationen finden Sie unter Verwenden von Datenrepository-Aufgaben zur Freigabe von Dateien.	9. August 2023
Amazon hat die von Amazon FSx ServiceRolePolicy AWS verwaltete Richtlinie FSx aktualisiert	Amazon hat die `cloudwatch:PutMetricData` Genehmigung im Amazon FSx aktualisiert FSxServiceRolePolicy. Weitere Informationen finden Sie unter FSx Amazon-Updates zu AWS verwalteten Richtlinien.	24. Juli 2023
Amazon hat die von Amazon FSx FullAccess AWS verwaltete Richtlinie FSx aktualisiert	Amazon hat die FSx FullAccess Amazon-Richtlinie FSx aktualisiert, um die `fsx:*` Genehmigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen. Weitere Informationen finden Sie in den FSx FullAccess Richtlinien von Amazon.	13. Juli 2023

Amazon hat die von Amazon FSx ConsoleFullAccess AWS verwaltete Richtlinie FSx aktualisiert	Amazon hat die FSx ConsoleFullAccess Amazon-Richtlinie FSx aktualisiert, um die `fsx:*` Genehmigung zu entfernen und bestimmte `fsx` Aktionen hinzuzufügen. Weitere Informationen finden Sie in den FSx ConsoleFullAccess Richtlinien von Amazon.	13. Juli 2023
LustreClient-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.8 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.8 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Clients. Lustre	25. Mai 2023
Support für AutoImport und AutoExport Metriken hinzugefügt	FSx for Lustre bietet jetzt CloudWatch Amazon-Metriken, die automatische Import- und Exportaktualisierungen für Dateisysteme überwachen, die mit Datenrepositorys verknüpft sind. Weitere Informationen finden Sie unter Überwachung mit Amazon CloudWatch.	31. März 2023

DRA-Unterstützung für die Bereitstellungstypen Persistent 1 und Scratch 2 hinzugefügt	Sie können jetzt Datenrepository-Verknüpfungen erstellen, um 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
LustreClient-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.7 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.7 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Clients. Lustre	5. Dezember 2022
Zusätzliche AWS-Region Unterstützung für den Bereitstellungstyp Persistent 2 hinzugefügt	Persistent 2 SSD der nächsten Generation FSx 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 FSx für Lustre-Dateisysteme.	10. November 2022

LustreClient-Unterstützung für CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.6 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen CentOS, Rocky Linux und Red Hat Enterprise Linux (RHEL) 8.6 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Clients. Lustre	8. September 2022
LustreClient-Unterstützung für Ubuntu 2.2 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen Ubuntu 22.04 ausgeführt wird. Weitere Informationen finden Sie unter Installation des Lustre Clients.	28. Juli 2022
LustreClient-Unterstützung für Rocky Linux hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-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 LustreRoot Squash.	25. Mai 2022

Zusätzliche AWS-Region Unterstützung für den Bereitstellungstyp Persistent 2 hinzugefügt	Persistent 2 SSD der nächsten Generation FSx 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 FSx für 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 zu FSx for Lustre-Dateisystemen zu migrieren. Weitere Informationen finden Sie unter So migrieren Sie vorhandene Dateien zu 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 FSx Amazon-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
LustreClient-Unterstützung für CentOS und Red Hat Enterprise Linux (RHEL) 8.5 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen CentOS und Red Hat Enterprise Linux (RHEL) 8.5 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Clients. Lustre	20. Dezember 2021

Support für den Export von Änderungen aus FSx for Lustre in ein Linked Data Repository	Sie können Lustre jetzt so konfigurieren FSx , 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 jetzt so konfigurieren FSx , dass Lustre Fehler- und Warnereignisse für Datenrepositorys, die mit Ihrem Dateisystem verknüpft sind, in Amazon CloudWatch Logs protokolliert. 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 für Lustre-Dateisysteme der nächsten Generation bieten Optionen für höheren Durchsatz und eine geringere Mindestspeicherkapazität. Weitere Informationen finden Sie unter Bereitstellungsoptionen FSx für 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
LustreClient-Unterstützung für CentOS und Red Hat Enterprise Linux (RHEL) 8.4 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen CentOS und Red Hat Enterprise Linux (RHEL) 8.4 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Clients. Lustre	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 für ein vorhandenes FSx for Lustre-Dateisystem aktivieren oder deaktivieren. Weitere Informationen finden Sie unter LustreDatenkomprimierung.	27. Mai 2021
Support für das Kopieren von Backups hinzugefügt	Sie können jetzt Amazon verwenden FSx , um Backups innerhalb derselben AWS-Konto auf eine andere AWS-Region (regionsübergreifende Kopien) oder innerhalb derselben AWS-Region (regionsinterne Kopien) zu kopieren. Weitere Informationen finden Sie unter Backups kopieren.	12. April 2021
LustreClient-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 mit nicht-privaten IP-Adressen auf Lustre-Dateisysteme zugreifen FSx . Weitere Informationen finden Sie unter Mounten von Amazon FSxDateisystemen vor Ort oder über eine Peering-Amazon-VPC.	17. Dezember 2020
LustreClient-Unterstützung für ARM-basiertes CentOS 7.9 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen CentOS 7.9 auf ARM-Basis ausgeführt wird. Weitere Informationen finden Sie unter Installation des Clients. Lustre	17. Dezember 2020
LustreClient-Unterstützung für CentOS und Red Hat Enterprise Linux (RHEL) 8.3 hinzugefügt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen CentOS und Red Hat Enterprise Linux (RHEL) 8.3 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Clients. Lustre	16. Dezember 2020
Support für die Skalierung von Speicher- und Durchsatzkapazität hinzugefügt	Sie können jetzt die Speicher- und Durchsatzkapazität vorhandener Dateisysteme FSx für Lustre 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 nutzen kann. Weitere Informationen finden Sie unter Speicherkontingente.	9. November 2020
Amazon FSx ist jetzt integriert in AWS Backup	Sie können jetzt zusätzlich AWS Backup zur Verwendung der nativen FSx Amazon-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 Lustre jetzt die Speicheroption HDD (Festplattenlaufwerk). FSx Sie können Ihr Dateisystem so konfigurieren, dass HDD für durchsatzintensive Workloads verwendet wird, bei denen es in der Regel um große, sequentielle Dateioperationen geht. Weitere Informationen finden Sie unter Mehrere Speicheroptionen.	12. August 2020

Support für den Import von Änderungen im Linked Data Repository in FSx for Lustre	Sie können Ihr FSx for Lustre-Dateisystem jetzt so konfiguri eren, dass neue Dateien, die nach der Erstellung des Dateisystems zu einem Linked Data Repository hinzugefü gt wurden, und Dateien, die sich dort geändert haben, automatisch importiert werden. Weitere Informationen finden Sie unter Automatisches Importieren von Updates aus dem Daten-Repository.	23. Juli 2020
LustreClient-Unterstützung für SUSE Linux SP4 und hinzugefügt SP5	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen SUSE Linux SP4 ausgeführt wird und. SP5 Weitere Informati onen finden Sie unter Installat ion des Lustre Clients.	20. Juli 2020
LustreClient-Unterstützung für CentOS und Red Hat Enterpris e Linux (RHEL) 8.2 hinzugefü gt	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, auf denen CentOS und Red Hat Enterprise Linux (RHEL) 8.2 ausgeführt werden. Weitere Informationen finden Sie unter Installation des Clients. Lustre	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 Lustre-Bereitstellungsoptionen.	12. Februar 2020
Support für POSIX-Metadaten hinzugefügt	FSx for Lustre behält die zugehörigen POSIX-Metadaten bei, wenn Dateien in ein verknüpftes dauerhaftes Daten-Repository auf Amazon S3 importiert und exportiert werden. 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 Aufgaben im Daten-Repository.	23. Dezember 2019
Zusätzliche AWS-Region Unterstützung hinzugefügt	FSx for Lustre ist jetzt in der Region AWS-Region Europa (London) verfügbar. Informationen zu FSx den regionsspezifischen Grenzwerten von Lustre finden Sie unter Grenzwerte.	9. Juli 2019
Zusätzliche Unterstützung hinzugefügt AWS-Region	FSx for Lustre ist jetzt im asiatisch-pazifischen Raum (Singapur) AWS-Region erhältlich. Informationen zu FSx den regionsspezifischen Grenzwerten von Lustre finden Sie unter Grenzwerte.	26. Juni 2019
LustreKundenunterstützung für und hinzugefügt Amazon LinuxAmazon Linux 2	Der FSx for Lustre-Client unterstützt jetzt EC2 Amazon-Instances, die ausgeführt werden Amazon Linux undAmazon Linux 2. 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, um Lustre in Ihre Datenverarbeitungs-Workflows zu integrieren FSx . 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 FSx für alle Dateisysteme von Lustre 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.