aws

Guida per l'utente di Lustre

FSx per Lustre

FSx per Lustre: Guida per l'utente di Lustre

Table of Contents

Cos'è Amazon FSx for Lustre?

FSx for Lustre semplifica ed economicamente vantaggiosa l'avvio e l'esecuzione del popolare file system ad alte prestazioniLustre. Usi Lustre per carichi di lavoro in cui la velocità è importante, come l'apprendimento automatico, l'High Performance Computing (HPC), l'elaborazione video e la modellazione finanziaria.

Il Lustre file system è progettato per applicazioni che richiedono uno storage rapido, laddove si desidera che lo storage rimanga al passo con l'elaborazione. Lustreè stato creato per risolvere il problema dell'elaborazione rapida ed economica dei set di dati in continua crescita a livello mondiale. È un file system ampiamente utilizzato progettato per i computer più veloci al mondo. Fornisce latenze inferiori al millisecondo, fino a multipli TBps di throughput e fino a milioni di IOPS. Per ulteriori informazioni su, consulta il sito Web. LustreLustre

Essendo un servizio completamente gestito, Amazon ne FSx semplifica l'utilizzo Lustre per carichi di lavoro in cui la velocità di archiviazione è importante. FSx for Lustre elimina la tradizionale complessità di configurazione e gestione dei Lustre file system, consentendoti di avviare ed eseguire in pochi minuti un file system ad alte prestazioni testato sul campo. Fornisce inoltre diverse opzioni di implementazione e classi di storage in modo da ottimizzare i costi in base alle proprie esigenze.

FSx for Lustre è conforme a POSIX, quindi puoi usare le tue attuali applicazioni basate su Linux senza dover apportare modifiche. FSx for Lustre fornisce un'interfaccia di file system nativa e funziona come qualsiasi file system con il sistema operativo Linux. Fornisce inoltre read-after-write coerenza e supporta il blocco dei file.

Argomenti

Diverse opzioni di implementazione e classi di archiviazione

Amazon FSx for Lustre offre una scelta di file system scratch e persistenti per soddisfare diverse esigenze di elaborazione dei dati. I file system Scratch sono ideali per l'archiviazione temporanea e l'elaborazione a breve termine dei dati. I dati non vengono replicati e non persistono in caso di guasto di un file server. I file system persistenti sono ideali per lo storage a lungo termine e per carichi di lavoro incentrati sul throughput. Nei file system persistenti, i dati vengono replicati e i file server vengono sostituiti in caso di guasto. Per ulteriori informazioni, consulta Opzioni di implementazione e classe di archiviazione FSx per i file system Lustre.

Amazon FSx for Lustre offre classi di storage per unità a stato solido (SSD), Intelligent-Tiering e unità disco rigido (HDD) ottimizzate per diversi requisiti di elaborazione dei dati:

- La classe di archiviazione SSD è ottimizzata per carichi di lavoro che richiedono operazioni casuali su file di piccole dimensioni e richiedono un throughput massimo. TBps Fornisce un accesso costante con latenza inferiore al millisecondo all'intero set di dati.
- La classe di storage Intelligent-Tiering è adatta e consigliata per la maggior parte dei carichi di lavoro che non richiedono una latenza costante a bassa latenza nell'intero set di dati. Fornisce uno storage completamente elastico ed economico, con velocità effettiva fino a multipli e accesso con latenza inferiore al millisecondo ai dati a cui si accede TBps di frequente con una cache di lettura SSD opzionale.
- La classe di storage HDD può essere utilizzata con carichi di lavoro che richiedono una latenza costante in ms a una cifra e un throughput fino a decine di volte per l'intero set di dati. GBps Opzionalmente, puoi fornire una cache di lettura SSD con dimensioni pari al 20% della capacità di archiviazione dell'HDD.

Per ulteriori informazioni, consulta FSx per le classi di storage Lustre.

FSx per Lustre e gli archivi di dati

Puoi collegare FSx i file system Lustre ai repository di dati su Amazon S3 o agli archivi dati locali.

FSx per l'integrazione del repository di dati Lustre S3

FSx for Lustre si integra con Amazon S3, semplificando l'elaborazione dei set di dati nel cloud utilizzando Lustre il file system ad alte prestazioni. Se collegato a un bucket Amazon S3, un file

system FSx for Lustre presenta in modo trasparente gli oggetti S3 come file. Amazon FSx importa gli elenchi di tutti i file esistenti nel tuo bucket S3 al momento della creazione del file system. Amazon FSx può anche importare elenchi di file aggiunti all'archivio dati dopo la creazione del file system. Puoi impostare le preferenze di importazione in base alle tue esigenze di flusso di lavoro. Il file system consente inoltre di riscrivere i dati del file system su S3. Le attività di data repository semplificano il trasferimento di dati e metadati tra il file system FSx for Lustre e il suo repository di dati durevole su Amazon S3. Per ulteriori informazioni, consultare Utilizzo di repository di dati con Amazon FSx for Lustre e Attività di archiviazione dei dati.

FSx per Lustre e gli archivi di dati locali

Con Amazon FSx for Lustre, puoi suddividere i carichi di lavoro di elaborazione dei dati da locale a Cloud AWS importando dati utilizzando o. AWS Direct Connect AWS VPN Per ulteriori informazioni, consulta Usare Amazon FSx con i tuoi dati locali.

Accesso ai file system Lustre FSx

Puoi combinare tipi di istanze di calcolo e Amazon Machine Images (AMIs) Linux collegati a un unico file system FSx for Lustre.

I file system Amazon FSx for Lustre sono accessibili dai carichi di lavoro di calcolo in esecuzione su istanze Amazon Elastic Compute Cloud (Amazon EC2), su contenitori Amazon Elastic Container Service (Amazon ECS) Docker e contenitori in esecuzione su Amazon Elastic Kubernetes Service (Amazon EKS).

- Amazon EC2: accedi al tuo file system dalle tue istanze di EC2 calcolo Amazon utilizzando il client open sourceLustre. EC2 Le istanze Amazon possono accedere al tuo file system da altre zone di disponibilità all'interno dello stesso Amazon Virtual Private Cloud (Amazon VPC), a condizione che la configurazione di rete preveda l'accesso tra sottoreti all'interno del VPC. Dopo aver montato il file system Amazon FSx for Lustre, puoi lavorare con i suoi file e le sue directory proprio come se utilizzassi un file system locale.
- Amazon EKS: accedi ad Amazon FSx for Lustre dai container in esecuzione su Amazon EKS utilizzando il driver CSI open source FSx per Lustre, come descritto nella Guida per l'utente di Amazon EKS. I contenitori in esecuzione su Amazon EKS possono utilizzare volumi persistenti ad alte prestazioni (PVs) supportati da Amazon FSx for Lustre.
- Amazon ECS: accedi ad Amazon FSx for Lustre dai contenitori Amazon ECS Docker su istanze Amazon. EC2 Per ulteriori informazioni, consulta Montaggio da Amazon Elastic Container Service.

Amazon FSx for Lustre è compatibile con i più diffusi sistemi basati su Linux, AMIs tra cui Amazon Linux 2023 e Amazon Linux 2, Red Hat Enterprise Linux (RHEL), CentOS, Ubuntu e SUSE Linux. Il Lustre client è incluso in Amazon Linux 2023 e Amazon Linux 2. Per RHEL, CentOS e Ubuntu, AWS Lustre un repository client fornisce client compatibili con questi sistemi operativi.

Con FSx for Lustre, puoi trasferire i carichi di lavoro ad alta intensità di calcolo dall'ambiente locale all'importazione di dati tramite o. Cloud AWS AWS Direct Connect AWS Virtual Private Network Puoi accedere al tuo FSx file system Amazon da locale, copiare i dati nel file system secondo necessità ed eseguire carichi di lavoro a elaborazione intensiva su istanze in-cloud.

Per ulteriori informazioni sui client, le istanze di calcolo e gli ambienti da cui è possibile accedere ai file system Lustre, consulta. FSx Accesso ai file system

Integrazioni con i servizi AWS

Amazon FSx for Lustre si integra con Amazon SageMaker AI come fonte di dati di input. Quando utilizzi l' SageMaker intelligenza artificiale con FSx for Lustre, i tuoi lavori di formazione sull'apprendimento automatico vengono accelerati eliminando la fase iniziale di download da Amazon S3. Inoltre, il costo totale di proprietà (TCO) viene ridotto evitando il download ripetitivo di oggetti comuni per lavori iterativi sullo stesso set di dati e risparmiando sui costi delle richieste S3. Per ulteriori informazioni, consulta Che cos'è l'IA? SageMaker nella Amazon SageMaker AI Developer Guide. Per una guida dettagliata su come usare Amazon FSx for Lustre come fonte di dati per l' SageMaker intelligenza artificiale, consulta Speed up training on Amazon AI SageMaker using Amazon FSx for Lustre e i file system Amazon EFS sul Machine AWS Learning Blog.

FSx for Lustre si integra con l'utilizzo di Launch Templates. AWS Batch EC2 AWS Batch consente di eseguire carichi di lavoro di elaborazione in batch su Cloud AWS, tra cui High Performance Computing (HPC), machine learning (ML) e altri carichi di lavoro asincroni. AWS Batch ridimensiona automaticamente e dinamicamente le istanze in base ai requisiti delle risorse lavorative. Per ulteriori informazioni, consulta What Is? AWS Batch nella Guida AWS Batch per l'utente.

FSx for Lustre si integra con. AWS ParallelCluster AWS ParallelCluster è uno strumento AWS di gestione dei cluster open source supportato utilizzato per distribuire e gestire i cluster HPC. Può creare automaticamente file system FSx per Lustre o utilizzare file system esistenti durante il processo di creazione del cluster.

Conformità e sicurezza

FSx i file system for Lustre supportano la crittografia a riposo e in transito. Amazon crittografa FSx automaticamente i dati del file system inattivi utilizzando chiavi gestite in AWS Key Management Service (AWS KMS). I dati in transito vengono inoltre crittografati automaticamente sui file system, in alcuni casi Regioni AWS quando vi si accede da EC2 istanze Amazon supportate. Per ulteriori informazioni sulla crittografia dei dati in FSx for Lustre, incluso Regioni AWS dove è supportata la crittografia dei dati in transito, consulta. Crittografia dei dati in Amazon FSx for Lustre Amazon FSx è stata valutata come conforme alle certificazioni ISO, PCI-DSS e SOC ed è idonea allo standard HIPAA. Per ulteriori informazioni, consulta Sicurezza in Amazon FSx for Lustre.

Presupposti

In questa guida, facciamo i seguenti presupposti:

- Se utilizzi Amazon Elastic Compute Cloud (Amazon EC2), supponiamo che tu conosca bene quel servizio. Per ulteriori informazioni su come usare Amazon EC2, consulta la EC2 documentazione di Amazon.
- Partiamo dal presupposto che tu abbia dimestichezza con l'uso di Amazon Virtual Private Cloud (Amazon VPC). Per ulteriori informazioni su come usare Amazon VPC, consulta la Amazon VPC User Guide.
- Partiamo dal presupposto che tu non abbia cambiato le regole sul gruppo di sicurezza predefinito per il tuo VPC basato sul servizio Amazon VPC. In caso affermativo, assicurati di aggiungere le regole necessarie per consentire il traffico di rete dall' EC2 istanza Amazon al file system Amazon FSx for Lustre. Per ulteriori dettagli, consulta Controllo degli accessi ai file system con Amazon VPC.

Prezzi di Amazon FSx for Lustre

Con Amazon FSx for Lustre, non ci sono costi hardware o software iniziali. Paghi solo per le risorse utilizzate, senza impegni minimi, costi di configurazione o costi aggiuntivi. Per informazioni sui prezzi e le commissioni associati al servizio, consulta la pagina dei prezzi di Amazon FSx for Lustre.

Forum Amazon FSx for Lustre

Se riscontri problemi durante l'utilizzo di Amazon FSx for Lustre, consulta i forum.

Sei un utente per la prima volta di Amazon FSx for Lustre?

Se sei un utente alle prime armi di Amazon FSx for Lustre, ti consigliamo di leggere le seguenti sezioni nell'ordine:

1. Se sei pronto a creare il tuo primo file system Amazon FSx for Lustre, provaGuida introduttiva ad Amazon FSx for Lustre.
2. Per ulteriori informazioni sulle prestazioni, consultare la pagina Prestazioni FSx di Amazon for Lustre.
3. Per informazioni sul collegamento del file system a un repository di dati di bucket Amazon S3, consulta. Utilizzo di repository di dati con Amazon FSx for Lustre
4. Per i dettagli sulla sicurezza di Amazon FSx for Lustre, consultaSicurezza in Amazon FSx for Lustre.
5. Per informazioni sui limiti di scalabilità di Amazon FSx for Lustre, inclusi il throughput e le dimensioni del file system, consulta. Quote di servizio per Amazon FSx for Lustre
6. Per informazioni sull'API Amazon FSx for Lustre, consulta l'Amazon FSx for Lustre API Reference.

Configurazione di Amazon FSx for Lustre

Prima di utilizzare Amazon FSx for Lustre per la prima volta, completa le attività nella Registrazione ad Amazon Web Services sezione. Per completare il tutorial introduttivo, assicurati che il bucket Amazon S3 che collegherai al tuo file system disponga delle autorizzazioni elencate in. Aggiungere le autorizzazioni per utilizzare gli archivi di dati in Amazon S3

Argomenti

Registrazione ad Amazon Web Services

Per eseguire la configurazione AWS, completa le seguenti attività:

1. Registrati per un Account AWS
2. Crea un utente con accesso amministrativo

Registrati per un Account AWS

Se non ne hai uno Account AWS, completa i seguenti passaggi per crearne uno.

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

Dopo esserti registrato Account AWS, proteggi Utente root dell'account AWS AWS IAM Identity Center, abilita e crea un utente amministrativo in modo da non utilizzare l'utente root per le attività quotidiane.

Proteggi i tuoi Utente root dell'account AWS

1. Accedi AWS Management Consolecome proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

   Per istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente Account AWS root (console) nella Guida per l'utente IAM.

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

   Per istruzioni, consulta Abilitazione di AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. In IAM Identity Center, assegna l'accesso amministrativo a un utente.

   Per un tutorial sull'utilizzo di IAM Identity Center directory come fonte di identità, consulta Configurare l'accesso utente con l'impostazione predefinita IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accesso come utente amministratore

- Per accedere con l'utente IAM Identity Center, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente IAM Identity Center.

Per informazioni sull'accesso utilizzando un utente IAM Identity Center, consulta AWS Accedere al portale di accesso nella Guida per l'Accedi ad AWS utente.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

   Per istruzioni, consulta Aggiungere gruppi nella Guida per l'utente di AWS IAM Identity Center .

Aggiungere le autorizzazioni per utilizzare gli archivi di dati in Amazon S3

Amazon FSx for Lustre è profondamente integrato con Amazon S3. Questa integrazione significa che le applicazioni che accedono al file system FSx for Lustre possono anche accedere senza problemi agli oggetti archiviati nel bucket Amazon S3 collegato. Per ulteriori informazioni, consulta Utilizzo di repository di dati con Amazon FSx for Lustre.

Per utilizzare gli archivi di dati, devi prima concedere ad Amazon FSx for Lustre determinate autorizzazioni IAM in un ruolo associato all'account del tuo utente amministratore.

Per incorporare una policy in linea per un ruolo utilizzando la console

1. Accedi AWS Management Console e apri la console IAM all'indirizzo. https://console.aws.amazon.com/iam/
2. Nel riquadro di navigazione, seleziona Ruoli.
3. Nell'elenco, scegliere il nome del ruolo in cui incorporare una policy.
4. Scegli la scheda Autorizzazioni.
5. Scorrere fino alla parte inferiore della pagina e scegliere Add inline policy (Aggiungi policy inline).

> **Note**
>
> Non puoi incorporare una policy in linea in un ruolo collegato a un servizio in IAM. Poiché il servizio collegato definisce se puoi modificare le autorizzazioni del ruolo, potresti aggiungere ulteriori policy dalla console di servizio, dall'API o dall' AWS CLI. Per visualizzare la documentazione relativa ai ruoli collegati ai servizi per un servizio, consulta AWS Servizi che funzionano con IAM e scegli Sì nella colonna Service-Linked Role relativa al tuo servizio.

6. Scegli Creazione di politiche con Visual Editor
7. Aggiungi la seguente dichiarazione sulla politica delle autorizzazioni.

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

Una volta creata, una policy inline viene automaticamente incorporata nel ruolo. Per ulteriori informazioni sui ruoli collegati al servizio, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

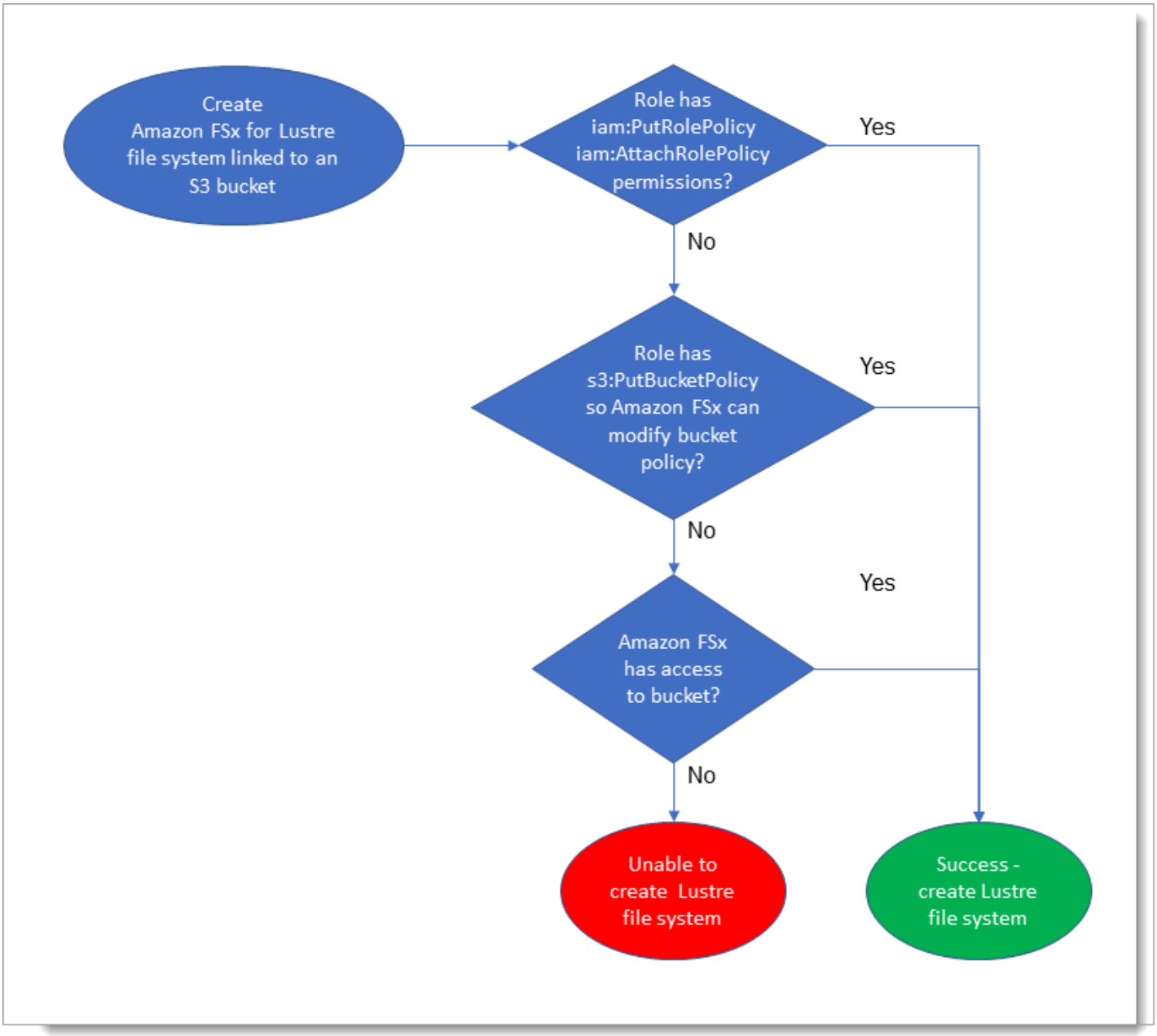
In che modo FSx Lustre verifica l'accesso ai bucket S3 collegati

Se il ruolo IAM che usi per creare il file system FSx for Lustre non dispone delle `iam:PutRolePolicy` autorizzazioni `iam:AttachRolePolicy` and, Amazon FSx verifica se è in grado di aggiornare la tua policy sui bucket S3. Amazon FSx può aggiornare la tua policy sui bucket se l'`s3:PutBucketPolicy`autorizzazione è inclusa nel tuo ruolo IAM per consentire al FSx file system Amazon di importare o esportare dati nel tuo bucket S3. Se è consentito modificare la policy del bucket, Amazon FSx aggiunge le seguenti autorizzazioni alla policy del bucket:

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

Se Amazon non è in FSx grado di modificare la policy del bucket, verifica se la policy del bucket esistente concede ad FSx Amazon l'accesso al bucket.

Se tutte queste opzioni falliscono, la richiesta di creazione del file system fallisce. Il diagramma seguente illustra i controlli che Amazon FSx segue per determinare se un file system può accedere al bucket S3 a cui verrà collegato.



Approfondimenti

Per iniziare a usareFSx for Lustre, consulta le istruzioni Guida introduttiva ad Amazon FSx for Lustre per creare le tue risorse Amazon FSx for Lustre.

Guida introduttiva ad Amazon FSx for Lustre

Di seguito, puoi scoprire come iniziare a usare Amazon FSx for Lustre. Questi passaggi ti guidano nella creazione di un file system Amazon FSx for Lustre e nell'accesso ad esso dalle tue istanze di calcolo. Facoltativamente, mostrano come utilizzare il file system Amazon FSx for Lustre per elaborare i dati nel bucket Amazon S3 con le applicazioni basate su file.

Questo esercizio introduttivo include i seguenti passaggi.

Argomenti

Prerequisiti

Per eseguire questo esercizio introduttivo, è necessario quanto segue:

- Un AWS account con le autorizzazioni necessarie per creare un file system Amazon FSx for Lustre e un'istanza Amazon EC2 . Per ulteriori informazioni, consulta Configurazione di Amazon FSx for Lustre.
- Crea un gruppo di sicurezza Amazon VPC da associare al tuo file system FSx for Lustre e non modificarlo dopo la creazione del file system. Per ulteriori informazioni, consulta Creare un gruppo di sicurezza per il tuo FSx file system Amazon.
- Un' EC2 istanza Amazon che esegue una versione Linux supportata nel tuo cloud privato virtuale (VPC) basato sul servizio Amazon VPC. Per questo esercizio introduttivo, consigliamo di utilizzare Amazon Linux 2023. Installerai il Lustre client su questa EC2 istanza, quindi monterai il file system FSx for Lustre sull' EC2 istanza. Per ulteriori informazioni sulla creazione di un' EC2 istanza, consulta Getting started: Launch an instance o Launch your instance nella Amazon EC2 User Guide.

Oltre ad Amazon Linux 2023, il Lustre client supporta i sistemi operativi Amazon Linux 2, Red Hat Enterprise Linux (RHEL), CentOS, Rocky Linux, SUSE Linux Enterprise Server e Ubuntu. Per ulteriori informazioni, consulta Lustrecompatibilità tra file system e kernel client.

- Quando crei l' EC2 istanza Amazon per questo esercizio introduttivo, tieni presente quanto segue:
  - Ti consigliamo di creare l'istanza nel tuo VPC predefinito.
  - Ti consigliamo di utilizzare il gruppo di sicurezza predefinito durante la creazione dell' EC2 istanza.
- Determina il tipo di file system Amazon FSx for Lustre che desideri creare, scratch o persistente. Per ulteriori informazioni, consulta Opzioni di implementazione e classe di archiviazione FSx per i file system Lustre.
- Ogni file system FSx for Lustre richiede un indirizzo IP per ogni server di metadati (MDS) e un indirizzo IP per ogni server di storage (OSS). Per ulteriori informazioni, consulta Indirizzi IP per file system.
- Un bucket Amazon S3 che archivia i dati per l'elaborazione del carico di lavoro. Il bucket S3 sarà il repository di dati durevole collegato per il file system for Lustre. FSx

Passaggio 1: crea il tuo FSx file system for Lustre

Crei il tuo file system nella FSx console Amazon. Tieni presente che tutti i file system FSx for Lustre sono basati sulla Lustre versione 2.15 se creati utilizzando la console Amazon FSx .

Per creare il file system

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard, scegli Crea file system per avviare la procedura guidata di creazione del file system.
3. Scegli, FSx for Lustrequindi scegli Avanti per visualizzare la pagina Crea file system.

   Inizia la configurazione con la sezione dei dettagli del file system.
4. Per Nome del file system (facoltativo), fornite un nome per il file system. È possibile utilizzare fino a 256 lettere Unicode, spazi bianchi e numeri più i caratteri speciali + - =. _:/.
5. Per la classe di distribuzione e archiviazione, scegli una delle opzioni:

   - Scegli Persistent, SSD per lo storage a lungo termine e per carichi di lavoro sensibili alla latenza. Con lo storage SSD, ti viene fatturata la quantità di storage fornita.

Facoltativamente, scegli con EFA abilitato per abilitare il supporto Elastic Fabric Adapter (EFA) per il file system. Per ulteriori informazioni su EFA, consulta. Utilizzo di file system compatibili con EFA

- Scegli Persistent, Intelligent-Tiering per uno storage a lungo termine. La classe di storage Intelligent-Tiering offre uno storage completamente elastico ed economico, adatto alla maggior parte dei carichi di lavoro, oltre a una cache di lettura SSD opzionale che fornisce latenze SSD per la lettura dei dati a cui si accede di frequente. Con Intelligent-Tiering, ti vengono fatturati i dati archiviati, in base alle dimensioni del set di dati, e non è necessario specificare una dimensione del file system.

  Facoltativamente, scegli con EFA abilitato per abilitare il supporto Elastic Fabric Adapter (EFA) per il file system.
- Scegli Scratch, l'implementazione SSD per l'archiviazione temporanea e l'elaborazione a breve termine dei dati. Con l'archiviazione SSD, ti viene fatturata la quantità di storage fornita.

6. Scegli la quantità di velocità effettiva per il tuo file system. Si paga per la quantità di throughput fornita.

   - Per lo storage SSD persistente, scegli un Throughput per unità di valore di archiviazione. Il throughput per unità di storage è la quantità di velocità effettiva di lettura e scrittura per ogni 1 tebibyte (TiB) di storage fornito.
   - Per lo storage SSD Scratch, scegli un Throughput per unità di valore di storage.
   - Per lo storage Intelligent-Tiering, scegli un valore di capacità di throughput.
7. Per Capacità di archiviazione (solo classe di archiviazione SSD), imposta la quantità di capacità di archiviazione per il file system, in TB:

   - Per un tipo di distribuzione SSD persistente, impostalo su un valore di 1,2 TiB, 2,4 TiB o incrementi di 2,4 TiB.
   - Per un tipo di implementazione SSD persistente abilitato per EFA, imposta questo valore in incrementi di 4,8 TiB, 9,6 TiB, 19,2 TiB e 38,4 TiB per i livelli di throughput rispettivamente di 1000, 500, 250 e 125 /TiB. MBps

   È possibile aumentare la quantità di capacità di storage in base alle esigenze dopo aver creato il file system. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione.
8. Per la configurazione dei metadati, scegliete una delle seguenti opzioni per assegnare il numero di IOPS di metadati per il vostro file system:

- Scegli Automatico (solo classe di storage SSD) se desideri che Amazon FSx for Lustre fornisca e ridimensioni automaticamente gli IOPS dei metadati sul tuo file system in base alla capacità di storage del file system.
- Scegli User-provisioned se desideri specificare il numero di IOPS di metadati da fornire per il tuo file system con classe di storage SSD o Intelligent-Tiering. I valori validi sono:
  - Per i file system SSD, i valori validi sono`1500`,, e multipli fino a un `3000` massimo `6000` di. `12000` `12000` `192000`
  - Per i file system Intelligent-Tiering, i valori validi sono e. `6000` `12000`

Per ulteriori informazioni su Metadata IOPS, vedere. Lustreconfigurazione delle prestazioni dei metadati

9. Per la cache di lettura SSD (solo Intelligent-Tiering), seleziona Automatica (proporzionale alla capacità di trasmissione) o Personalizzata (fornita dall'utente). Con l'opzione Automatic, Amazon FSx for Lustre sceglie automaticamente la dimensione della cache di lettura in base al throughput assegnato. Se conosci la dimensione approssimativa del tuo set di dati di lavoro attivo, puoi selezionare Personalizzato per personalizzare le dimensioni della cache di lettura SSD. Per ulteriori informazioni, consulta Gestione della cache di lettura SSD fornita.
10. Per il tipo di compressione dei dati, scegli NONE per disattivare la compressione dei dati o scegli di LZ4attivare la compressione dei dati con l'algoritmo. LZ4 Per ulteriori informazioni, consulta Lustrecompressione dei dati.
11. Nella sezione Rete e sicurezza, fornisci le seguenti informazioni sul gruppo di rete e sicurezza:

    - Per Virtual Private Cloud (VPC), scegli il VPC che desideri associare al tuo file system. Per questo esercizio introduttivo, scegli lo stesso VPC che hai scelto per la tua istanza Amazon EC2 .
    - Per i gruppi di sicurezza VPC, l'ID del gruppo di sicurezza predefinito per il tuo VPC dovrebbe essere già stato aggiunto.

      Se non utilizzi il gruppo di sicurezza predefinito, assicurati di aggiungere la seguente regola in entrata al gruppo di sicurezza che stai utilizzando per questo esercizio introduttivo.

Tipo	Protocollo	Intervallo porte	Origine	Descrizione
Tutte le regole TCP	TCP	0-65535	Personalizzato *the_ID_of_this_security_group*	Regola Lustre del traffico in entrata

> **Important**
>
> - Assicurati che il gruppo di sicurezza che stai utilizzando segua le istruzioni di configurazione fornite inControllo degli accessi ai file system con Amazon VPC. È necessario configurare il gruppo di sicurezza per consentire il traffico in entrata sulle porte 988 e 1018-1023 dal gruppo di sicurezza stesso o dall'intera sottorete CIDR, necessaria per consentire agli host del file system di comunicare tra loro.
> - Se state creando un file system compatibile con EFA, assicuratevi di specificare un gruppo di sicurezza abilitato per EFA.

- Per Subnet, scegliete un valore qualsiasi dall'elenco delle sottoreti disponibili.

12. Per la sezione Crittografia, le opzioni disponibili variano a seconda del tipo di file system che state creando:

    - Per un file system persistente, puoi scegliere una chiave di crittografia AWS Key Management Service (AWS KMS) per crittografare i dati del file system inattivo.
    - Per un file system scratch, i dati inattivi vengono crittografati utilizzando chiavi gestite da AWS.
    - Per i file system scratch 2 e persistenti, i dati in transito vengono crittografati automaticamente quando si accede al file system da un tipo di EC2 istanza Amazon supportato. Per ulteriori informazioni, consulta Crittografia dei dati in transito.

13. Per la sezione opzionale Data Repository Import/Export, il collegamento del file system agli archivi di dati di Amazon S3 è disabilitato per impostazione predefinita. Per informazioni sull'attivazione di questa opzione e sulla creazione di un'associazione di repository di dati a un bucket S3 esistente, consulta. Per collegare un bucket S3 durante la creazione di un file system (console)

> **Important**
>
> - La selezione di questa opzione disabilita anche i backup e non sarà possibile abilitarli durante la creazione del file system.
> - Se colleghi uno o più file system Amazon FSx for Lustre a un bucket Amazon S3, non eliminare il bucket Amazon S3 finché tutti i file system collegati non sono stati eliminati.
> - I file system Intelligent-Tiering non supportano il collegamento a repository di dati Amazon S3.

14. Per la registrazione facoltativa, la registrazione è abilitata per impostazione predefinita. Se abilitato, gli errori e gli avvisi relativi all'attività di archiviazione dei dati sul tuo file system vengono registrati in Amazon Logs. CloudWatch Per informazioni sulla configurazione della registrazione, consulta. Gestione della registrazione
15. In Backup e manutenzione opzionale, puoi fare quanto segue.
    - Disabilita il backup automatico giornaliero. Questa opzione è abilitata per impostazione predefinita, a meno che non sia stata abilitata l'opzione Import/Export di Data Repository.
    - Imposta l'ora di inizio per la finestra di backup automatico giornaliero.
    - Imposta il periodo di conservazione del backup automatico, da 1 a 35 giorni.
    - Imposta l'ora di inizio della finestra di manutenzione settimanale o mantienila impostata sull'impostazione predefinita Nessuna preferenza.

    Per ulteriori informazioni, consultare Protezione dei dati con backup e Finestre di manutenzione Amazon FSx for Lustre.
16. Per Root Squash (facoltativo), root squash è disabilitato per impostazione predefinita. Per informazioni sull'attivazione e la configurazione di root squash, consulta. Per abilitare root squash durante la creazione di un file system (console)
17. Crea tutti i tag che desideri applicare al tuo file system.
18. Scegli Avanti per visualizzare la pagina di riepilogo della creazione del file system.
19. Controlla le impostazioni del tuo file system Amazon FSx for Lustre e scegli Create file system.

Ora che hai creato il tuo file system, annota il nome di dominio completo e il nome di montaggio per un passaggio successivo. Puoi trovare il nome di dominio completo e il nome di mount per un file system scegliendo il nome del file system nella dashboard File systems e quindi selezionando Allega.

Fase 2: Installare e configurare il Lustre client

Prima di poter accedere al file system Amazon FSx for Lustre dall' EC2 istanza Amazon, devi fare quanto segue:

- Verifica che l' EC2 istanza soddisfi i requisiti minimi del kernel.
- Aggiorna il kernel se necessario.
- Scarica e installa il Lustre client.

Per verificare la versione del kernel e scaricare il client Lustre

1. Apri una finestra di terminale sulla tua EC2 istanza.
2. Determina quale kernel è attualmente in esecuzione sulla tua istanza di calcolo eseguendo il comando seguente.

   ```
   uname -r
   ```
3. Esegui una di queste operazioni:

   - Se il comando ritorna `6.1.79-99.167.amzn2023.x86_64` per le istanze basate su x86 o `6.1.79-99.167.amzn2023.aarch64` o superiore per EC2 le istanze basate su Graviton2, scarica e EC2 installa il client con il seguente comando. Lustre

     ```
     sudo dnf install -y lustre-client
     ```
   - Se il comando restituisce un risultato inferiore a quello delle `6.1.79-99.167.amzn2023.x86_64` istanze basate su x86 o inferiore `6.1.79-99.167.amzn2023.aarch64` a quello EC2 delle istanze basate su Graviton2, aggiorna il kernel e riavvia l' EC2 istanza Amazon eseguendo il comando seguente. EC2

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

     Conferma che il kernel è stato aggiornato utilizzando il comando. uname -r Quindi scarica e installa il Lustre client come descritto sopra.

Per informazioni sull'installazione del Lustre client su altre distribuzioni Linux, consultaInstallazione del client Lustre.

Fase 3: Montare il file system

Per montare il file system, è necessario creare una directory o un punto di montaggio, quindi montare il file system sul client e verificare che il client possa accedere al file system.

Per montare il file system

1. Utilizzare il comando seguente per creare una cartella da usare come punto di montaggio.

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

2. Installa il file system Amazon FSx for Lustre nella directory che hai creato. Usa il seguente comando e sostituisci i seguenti elementi:

   - Sostituire *file_system_dns_name* con il nome DNS (Domain Name System) effettivo del file system.
   - Sostituiscilo *mountname* con il nome di mount del file system, che puoi ottenere eseguendo il describe-file-systems AWS CLI comando o l'operazione DescribeFileSystemsAPI.

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

   Questo comando monta il file system con due opzioni `-o relatime eflock`:

   - `relatime`— Sebbene l'`atime`opzione mantenga `atime` (tempi di accesso agli inode) i dati per ogni accesso a un file, l'`relatime`opzione mantiene anche `atime` i dati, ma non per ogni volta che si accede a un file. Con l'`relatime`opzione abilitata, `atime` i dati vengono scritti su disco solo se il file è stato modificato dall'ultimo aggiornamento `atime` dei dati (`mtime`) o se l'ultimo accesso al file è avvenuto più di un certo periodo di tempo fa (6 ore per impostazione predefinita). L'utilizzo dell'`atime`opzione `relatime` o ottimizzerà i processi di rilascio dei file.

> **Note**
>
> Se il carico di lavoro richiede una precisione precisa nel tempo di accesso, puoi montarlo con l'opzione di `atime` montaggio. Tuttavia, ciò può influire sulle prestazioni del carico di lavoro aumentando il traffico di rete necessario per mantenere valori precisi del tempo di accesso.
> Se il carico di lavoro non richiede tempi di accesso ai metadati, l'utilizzo dell'opzione di `noatime` montaggio per disabilitare gli aggiornamenti al tempo di accesso può fornire un miglioramento delle prestazioni. Tieni presente che `atime` processi specifici come il rilascio dei file o il rilascio della validità dei dati saranno imprecisi al momento del rilascio.

- `flock`— Abilita il blocco dei file per il file system. Se non vuoi abilitare il blocco dei file, usa il `mount` comando without. `flock`

3. Verificate che il comando mount abbia avuto successo elencando il contenuto della directory in cui avete montato il file system`/mnt/fsx`, utilizzando il comando seguente.

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

È inoltre possibile utilizzare il `df` comando seguente.

```
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
```

I risultati mostrano che il FSx file system Amazon è stato montatoon /mnt/fsx.

Fase 4: Esegui il tuo flusso di lavoro

Ora che il file system è stato creato e montato su un'istanza di calcolo, puoi utilizzarlo per eseguire il tuo carico di lavoro di elaborazione ad alte prestazioni.

Puoi creare un'associazione di repository di dati per collegare il tuo file system a un repository di dati Amazon S3. Per ulteriori informazioni, consulta. Collegamento del file system a un bucket Amazon S3

Dopo aver collegato il file system a un repository di dati Amazon S3, puoi esportare i dati che hai scritto nel file system nel tuo bucket Amazon S3 in qualsiasi momento. Da un terminale su una delle tue istanze di calcolo, esegui il comando seguente per esportare un file nel tuo bucket Amazon S3.

```
sudo lfs hsm_archive file_name
```

Per ulteriori informazioni su come eseguire rapidamente questo comando su una cartella o su una grande raccolta di file, consulta. Esportazione di file utilizzando i comandi HSM

Fase 5: eliminazione delle risorse

Dopo aver terminato questo esercizio, segui questi passaggi per ripulire le tue risorse e proteggere il tuo AWS account.

Per eliminare le risorse

1. Se desideri eseguire un'esportazione finale, esegui il comando seguente.

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

2. Sulla EC2 console Amazon, interrompi l'istanza. Per ulteriori informazioni, consulta Terminate Your Instance nella Amazon EC2 User Guide.
3. Sulla console Amazon FSx for Lustre, elimina il file system con la seguente procedura:

   a. Nel pannello di navigazione, scegli File system.
   b. Scegli il file system che desideri eliminare dall'elenco dei file system sulla dashboard.
   c. In Azioni, seleziona Elimina file system.
   d. Nella finestra di dialogo che appare, scegli se desideri eseguire un backup finale del file system. Fornisci quindi l'ID del file system per confermare l'eliminazione. Scegli Elimina file system.

4. Se hai creato un bucket Amazon S3 per questo esercizio e non desideri conservare i dati che hai esportato, ora puoi eliminarlo. Per ulteriori informazioni, consulta Eliminare un bucket nella Guida per l'utente di Amazon Simple Storage Service.

Opzioni di implementazione e classe di archiviazione FSx per i file system Lustre

Amazon FSx for Lustre offre due opzioni di implementazione del file system: persistente e scratch. Fornisce tre classi di archiviazione: SSD (unità a stato solido), Intelligent-Tiering e HDD (unità disco rigido).

Scegli il tipo di distribuzione del file system e la classe di storage quando crei un nuovo file system AWS Management Console, utilizzando l'API, the AWS Command Line Interface (AWS CLI) o Amazon FSx for Lustre. Per ulteriori informazioni, consulta Passaggio 1: crea il tuo FSx file system for Lustre e CreateFileSystemnell'Amazon FSx API Reference.

File system persistenti

I file system persistenti sono progettati per lo storage e i carichi di lavoro a lungo termine e i file server offrono un'elevata disponibilità. Per i file system basati su SSD e HDD, i dati vengono replicati automaticamente all'interno della stessa zona di disponibilità in cui si trova il file system. Per i file system Intelligent-Tiering, i dati vengono replicati su più zone di disponibilità. I volumi di dati collegati ai file server vengono replicati indipendentemente dai file server a cui sono collegati.

Amazon monitora FSx continuamente i file system persistenti per individuare eventuali guasti hardware e sostituisce automaticamente i componenti dell'infrastruttura in caso di guasto. Su un file system persistente, se un file server non è disponibile, viene sostituito automaticamente entro pochi minuti dall'errore. Durante questo periodo, le richieste di dati dei client su quel server riprovano in modo trasparente e alla fine hanno esito positivo dopo la sostituzione del file server. I dati sui file system persistenti vengono replicati su dischi e tutti i dischi guasti vengono sostituiti automaticamente in modo trasparente.

Utilizza file system persistenti per lo storage a lungo termine e per carichi di lavoro incentrati sulla velocità effettiva che vengono eseguiti per periodi prolungati o indefinitamente e che potrebbero essere sensibili alle interruzioni della disponibilità.

I tipi di distribuzione persistenti crittografano automaticamente i dati in transito quando vi si accede da EC2 istanze Amazon che supportano la crittografia in transito.

Amazon FSx for Lustre supporta due tipi di distribuzione persistente: Persistent 1 e Persistent 2.

Tipo di distribuzione Persistent 2

Persistent 2 è il tipo di distribuzione Persistent di ultima generazione ed è più adatto per i casi d'uso che richiedono storage a lungo termine e che richiedono i massimi livelli di IOPS e throughput. I file system Persistent 2 supportano le classi di storage SSD e Intelligent-Tiering.

Puoi creare file system Persistent 2 con una configurazione di metadati e EFA abilitati utilizzando la FSx console Amazon e AWS Command Line Interface l'API Amazon FSx .

Tipo di distribuzione persistente 1

Il tipo di distribuzione Persistent 1 è ideale per i casi d'uso che richiedono uno storage a lungo termine. I tipi di distribuzione Persistent 1 supportano le classi di archiviazione SSD (unità a stato solido) e HDD (unità disco rigido).

Puoi creare tipi di distribuzione Persistent 1 solo utilizzando AWS CLI e l' FSx API Amazon.

File system Scratch

I file system Scratch sono progettati per l'archiviazione temporanea e l'elaborazione a breve termine dei dati. I dati non vengono replicati e non persistono in caso di guasto di un file server. I file system Scratch offrono un throughput di burst elevato fino a sei volte il throughput di base di 200 per MBps TiB di capacità di storage. Per ulteriori informazioni, consulta Caratteristiche prestazionali delle classi di storage SSD e HDD.

Utilizza i file system scratch quando hai bisogno di uno storage ottimizzato in termini di costi per carichi di lavoro a breve termine e con elevati livelli di elaborazione.

In un file system scratch, i file server non vengono sostituiti in caso di guasto e i dati non vengono replicati. Se un file server o un disco di archiviazione non è disponibile su un file system di memoria virtuale, i file archiviati su altri server sono ancora accessibili. Se i client tentano di accedere ai dati presenti sul server o sul disco non disponibile, riscontrano un errore di I/O immediato.

La tabella seguente illustra la disponibilità o la durabilità per cui sono progettati i file system scratch di dimensioni esemplificative, nel corso di un giorno e di una settimana. Poiché i file system più grandi dispongono di più file server e più dischi, le probabilità di errore aumentano.

Dimensioni del file system (TiB)	Numero di file server	Disponibilità/durata nell'arco di un giorno	Disponibilità/durata nell'arco di una settimana
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%

Indirizzi IP per file system

Ogni file system FSx for Lustre richiede un indirizzo IP per ogni server di metadati (MDS) e un indirizzo IP per ogni server di storage (OSS).

File system che utilizzano una classe di archiviazione SSD o HDD

Tipo di file system	Produttività, /TiB MBps	Archiviazione per sistema operativo
Persistente 2 EFA*	125	38,4 TiB/OSS
	250	19,2 TiB per sistema operativo
	500	9,6 TiB per sistema operativo
	1000	4,8 TiB per sistema operativo
Persistente 2 non EFA*	125, 250, 500, 1000	2,4 TiB per sistema operativo
1 SSD persistente	50, 100, 200	2,4 TiB per sistema operativo

Tipo di file system	Produttività, /TiB MBps	Archiviazione per sistema operativo
HDD persistente	12	6 TiB per sistema operativo
	40	1,8 TiB per sistema operativo
Scratch 2	200	2,4 TiB per sistema operativo
Scratch 1	200	3,6 TiB per sistema operativo

File system che utilizzano la classe di storage Intelligent-Tiering

Tipo di file system	Velocità effettiva per OSS
Suddivisione in più livelli intelligente*	4000 per sistema operativo MBps

> **Note**
>
> * Amazon fornisce un FSx server di metadati per ogni 12.000 IOPS di metadati su file system SSD Persistent 2 e Intelligent-Tiering configurati con la configurazione dei metadati.
> I file system Amazon FSx for Lustre Intelligent-Tiering supportano un massimo di 512 TiB di storage per sistema operativo.

FSx per le classi di storage Lustre

Amazon FSx for Lustre offre classi di storage per unità a stato solido (SSD), Intelligent-Tiering e unità disco rigido (HDD) ottimizzate per diversi requisiti di elaborazione dei dati:

- La classe di archiviazione SSD offre un accesso a bassa latenza (inferiore al millisecondo) all'intero set di dati. La classe di storage SSD viene fornita, il che significa che si specifica una dimensione del file system e si pagano i costi di storage per la quantità di storage fornita. Utilizza la classe di

storage SSD per carichi di lavoro sensibili alla latenza che richiedono le prestazioni dello storage all-flash su tutti i dati.

I file system Persistent 2 con storage SSD supportano livelli più elevati di throughput per unità di storage (ovvero 250, 500 o 1000 per MBps TIB) rispetto ai file system Persistent 1. Per un file system Persistent 1 con storage SSD, il throughput per unità di storage è di 50, 100 o 200 per MBps TiB. Per un file system Scratch con storage SSD, il throughput per unità di storage è di 200 per MBps TiB.

- La classe di storage Intelligent-Tiering offre uno storage completamente elastico e intelligente su più livelli. Elasticità significa che si paga per la quantità di dati archiviati e non è necessario specificare la dimensione del file system. Il tiering intelligente significa che paghi automaticamente meno per archiviare dati a cui non hai avuto accesso di recente. Questa classe di storage ottimizza automaticamente i costi suddividendo i dati «cold» su livelli di storage più economici. È possibile fornire una cache di lettura SSD opzionale per l'accesso a bassa latenza (inferiore al millisecondo) ai dati a cui si accede di frequente. La classe di storage Intelligent-Tiering offre il miglior equilibrio tra prezzo e prestazioni per la maggior parte dei carichi di lavoro. Utilizza la classe di storage Intelligent-Tiering per carichi di lavoro compatibili con la cache e che non richiedono le prestazioni dello storage all-flash su tutti i dati. I file system Intelligent-Tiering supportano capacità di throughput con incrementi di 4000. MBps
- La classe di storage HDD può essere utilizzata con carichi di lavoro che richiedono una latenza ms costante a una cifra per tutti i dati. È possibile fornire una cache di lettura SSD opzionale con dimensioni pari al 20% della capacità di archiviazione dell'HDD per fornire un accesso a bassa latenza ai dati a cui si accede di frequente. Con lo storage su HDD, è possibile specificare la dimensione del file system e pagare per la quantità di storage fornita. Per un file system Persistent 1 con storage su HDD, il throughput per unità di storage è 12 o 40 per MBps TiB.

Per ulteriori informazioni sulle prestazioni di queste classi di archiviazione, vedere e. Caratteristiche prestazionali delle classi di storage SSD e HDD Caratteristiche prestazionali della classe di storage Intelligent-Tiering

In che modo la classe di storage Intelligent-Tiering suddivide i dati su più livelli

La classe di storage Amazon FSx Intelligent-Tiering archivia automaticamente i dati in tre livelli di accesso. È progettata per ottimizzare i costi di storage spostando automaticamente i dati sul livello di accesso più conveniente, senza impatto sulle prestazioni o costi operativi. La classe di storage

Intelligent-Tiering suddivide automaticamente i dati in base all'ora dell'ultimo accesso, ottimizzando così automaticamente i costi per i dati meno attivi:

- I dati a cui si accede negli ultimi 30 giorni vengono archiviati nel livello Frequent Access.
- I dati a cui non è stato effettuato l'accesso per 30 giorni consecutivi passano automaticamente al livello Accesso infrequente e costano meno dei dati nel livello Accesso frequente.
- I dati a cui non è stato effettuato l'accesso per 90 giorni consecutivi passano automaticamente al livello Archive Instant Access e costano meno dei dati nel livello Infrequent Access.

Quando si accede ai dati nei livelli Infrequent Access o Archive Instant Access, i dati tornano automaticamente al livello Frequent Access. Tutti gli accessi ai dati non memorizzati nella cache hanno le stesse caratteristiche prestazionali, indipendentemente dal livello dei dati, e non vi sono costi di IOPS, recupero o transizione aggiuntivi oltre ai normali costi operativi di lettura/scrittura.

Disponibilità del tipo di implementazione

I tipi di distribuzione Scratch 2, Persistent 1 e Persistent 2 sono disponibili nei seguenti casi Regioni AWS:

Regione AWS	Persistente 2	Persistente 1	Scratch 2
Stati Uniti orientali (Ohio)	✓	✓	✓
Stati Uniti orientali (Virginia settentrionale)	✓	✓	✓
Zona locale degli Stati Uniti orientali (Atlanta)	✓ *		
Zona locale degli Stati Uniti orientali (Dallas)	✓ *		
Stati Uniti occidentali (California settentrionale)	✓	✓	✓
Zona locale degli Stati Uniti occidentali (Los Angeles)		✓	✓

Regione AWS	Persistente 2	Persistente 1	Scratch 2
US West (Oregon)	✓	✓	✓
Africa (Città del Capo)		✓	✓
Asia Pacifico (Hong Kong)	✓	✓	✓
Asia Pacific (Hyderabad)		✓	✓
Asia Pacifico (Giacarta)		✓	✓
Asia Pacifico (Malesia)	✓ *		
Asia Pacifico (Melbourne)		✓	✓
Asia Pacifico (Mumbai)	✓	✓	✓
Asia Pacific (Osaka)		✓	✓
Asia Pacific (Seul)	✓	✓	✓
Asia Pacifico (Singapore)	✓	✓	✓
Asia Pacifico (Sydney)	✓	✓	✓
Asia Pacifico (Tailandia)	✓ *		
Asia Pacifico (Tokyo)	✓	✓	✓
Canada (Centrale)	✓	✓	✓
Canada occidentale (Calgary)	✓ *		
Europa (Francoforte)	✓	✓	✓
Europa (Irlanda)	✓	✓	✓
Europa (Londra)	✓	✓	✓
Europa (Milano)		✓	✓

Regione AWS	Persistente 2	Persistente 1	Scratch 2
Europa (Parigi)		✓	✓
Europa (Spagna)		✓	✓
Europa (Stoccolma)	✓	✓	✓
Europa (Zurigo)		✓	✓
Israele (Tel Aviv)	✓ *		✓
Messico (centrale)	✓ *		
Medio Oriente (Bahrein)		✓	✓
Medio Oriente (Emirati Arabi Uniti)		✓	✓
Sud America (San Paolo)		✓	✓
AWS GovCloud (Stati Uniti orientali)		✓	✓
AWS GovCloud (Stati Uniti occidentali)		✓	✓

Note

* Questi Regioni AWS supportano i file system Persistent-125 e Persistent-250 con classe di archiviazione SSD senza EFA.

Utilizzo di repository di dati con Amazon FSx for Lustre

Amazon FSx for Lustre fornisce file system ad alte prestazioni ottimizzati per l'elaborazione rapida dei carichi di lavoro. Può supportare carichi di lavoro come l'apprendimento automatico, l'High Performance Computing (HPC), l'elaborazione video, la modellazione finanziaria e l'automazione della progettazione elettronica (EDA). Questi carichi di lavoro richiedono in genere che i dati vengano presentati utilizzando un'interfaccia di file system scalabile e ad alta velocità per l'accesso ai dati. Spesso, i set di dati utilizzati per questi carichi di lavoro sono archiviati in repository di dati a lungo termine in Amazon S3. FSx for Lustre è integrato nativamente con Amazon S3, semplificando l'elaborazione dei set di dati con il file system. Lustre

> **Note**
>
> - I backup dei file system non sono supportati sui file system collegati a un repository di dati Amazon S3. Per ulteriori informazioni, consulta Protezione dei dati con backup.
> - I file system Intelligent-Tiering non supportano il collegamento a repository di dati Amazon S3.

Argomenti

Panoramica degli archivi di dati

Quando usi Amazon FSx for Lustre con repository di dati, puoi importare ed elaborare grandi volumi di dati di file in un file system ad alte prestazioni utilizzando attività automatiche di importazione e importazione di archivi di dati. Allo stesso tempo, puoi scrivere risultati nei tuoi repository di dati utilizzando attività automatiche di esportazione o esportazione degli archivi di dati. Con queste funzionalità, puoi riavviare il carico di lavoro in qualsiasi momento utilizzando i dati più recenti archiviati nel tuo repository di dati.

> **Note**
>
> Le associazioni di archivi di dati, l'esportazione automatica e il supporto per più archivi di dati non sono disponibili sui file system o sui FSx file system Lustre 2.10. `Scratch 1`

FSx for Lustre è profondamente integrato con Amazon S3. Questa integrazione significa che puoi accedere senza problemi agli oggetti archiviati nei bucket Amazon S3 dalle applicazioni che montano FSx il file system for Lustre. Puoi anche eseguire carichi di lavoro ad alta intensità di calcolo su EC2 istanze Amazon in Cloud AWS ed esportare i risultati nel tuo repository di dati una volta completato il carico di lavoro.

Per accedere agli oggetti nel repository di dati di Amazon S3 come file e directory sul file system, i metadati di file e directory devono essere caricati nel file system. Puoi caricare i metadati da un repository di dati collegato quando crei un'associazione di repository di dati.

Inoltre, è possibile importare i metadati di file e directory dai repository di dati collegati al file system utilizzando l'importazione automatica o utilizzando un'attività di importazione di archivi di dati. Quando attivi l'importazione automatica per un'associazione di repository di dati, il file system importa automaticamente i metadati dei file man mano che i file vengono creati, modificati e/o eliminati nell'archivio di dati S3. In alternativa, puoi importare i metadati per file e directory nuovi o modificati utilizzando un'attività di importazione del repository di dati.

> **Note**
>
> Le attività automatiche di importazione e importazione dell'archivio di dati possono essere utilizzate contemporaneamente su un file system.

È inoltre possibile esportare i file e i metadati associati presenti nel file system nel repository di dati utilizzando l'esportazione automatica o un'attività di esportazione dell'archivio di dati. Quando si attiva l'esportazione automatica su un'associazione di repository di dati, il file system esporta automaticamente i dati e i metadati dei file man mano che i file vengono creati, modificati o eliminati. In alternativa, è possibile esportare file o directory utilizzando un'attività di esportazione del repository di dati. Quando si utilizza un'operazione di esportazione di un archivio di dati, vengono esportati i dati e i metadati dei file creati o modificati dopo l'ultima operazione di questo tipo.

> **Note**
>
> - Le attività automatiche di esportazione ed esportazione del repository di dati non possono essere utilizzate contemporaneamente su un file system.
> - Le associazioni di archivi di dati esportano solo file, collegamenti simbolici e directory regolari. Ciò significa che tutti gli altri tipi di file (FIFO special, block special, character special e socket) non verranno esportati come parte dei processi di esportazione come l'esportazione automatica e le attività di archiviazione dei dati di esportazione.

FSx for Lustre supporta anche carichi di lavoro di cloud bursting con file system locali, consentendoti di copiare dati da client locali utilizzando o VPN. AWS Direct Connect

> **Important**
>
> Se hai collegato uno o più file system FSx for Lustre a un repository di dati su Amazon S3, non eliminare il bucket Amazon S3 prima di aver eliminato o scollegato tutti i file system collegati.

Supporto per regione e account per i bucket S3 collegati

Quando crei link ai bucket S3, tieni presente le seguenti limitazioni relative al supporto per regione e account:

- L'esportazione automatica supporta configurazioni interregionali. Il FSx file system Amazon e il bucket S3 collegato possono trovarsi nello stesso Regione AWS o in modo diverso. Regioni AWS
- L'importazione automatica non supporta configurazioni interregionali. Sia il FSx file system Amazon che il bucket S3 collegato devono trovarsi nello stesso. Regione AWS

- Sia l'esportazione automatica che l'importazione automatica supportano configurazioni tra account. Il FSx file system Amazon e il bucket S3 collegato possono appartenere allo stesso Account AWS o a diversi. Account AWS

Supporto per metadati POSIX per archivi di dati

Amazon FSx for Lustre trasferisce automaticamente i metadati POSIX (Portable Operating System Interface) per file, directory e collegamenti simbolici (collegamenti simbolici) durante l'importazione e l'esportazione di dati da e verso un repository di dati collegato su Amazon S3. Quando esporti le modifiche nel tuo file system nel relativo repository di dati collegato, FSx for Lustre esporta anche le modifiche ai metadati POSIX come metadati di oggetti S3. Ciò significa che se un altro file system FSx for Lustre importa gli stessi file da S3, i file avranno gli stessi metadati POSIX in quel file system, incluse proprietà e autorizzazioni.

FSx for Lustre importa solo oggetti S3 con chiavi oggetto conformi a POSIX, come le seguenti.

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

FSx for Lustre memorizza le directory e i collegamenti simbolici come oggetti separati nel repository di dati collegato su S3, For directories, FSx for Lustre crea un oggetto S3 con un nome chiave che termina con una barra («/»), come segue:

- La chiave dell'oggetto S3 viene mappata alla directory for Lustre. `mydir/` FSx `mydir/`
- La chiave oggetto S3 viene `mydir/mysubdir/` mappata alla directory FSx for Lustre. `mydir/mysubdir/`

Per i collegamenti simbolici, FSx for Lustre utilizza il seguente schema Amazon S3:

- Chiave dell'oggetto S3: il percorso del link, relativo alla directory di montaggio for Lustre FSx
- Dati dell'oggetto S3: il percorso di destinazione di questo collegamento simbolico
- Metadati degli oggetti S3: i metadati per il collegamento simbolico

FSx for Lustre archivia i metadati POSIX, tra cui proprietà, autorizzazioni e timestamp per file, directory e collegamenti simbolici, negli oggetti S3 come segue:

- `Content-Type`— L'intestazione dell'entità HTTP utilizzata per indicare il tipo di supporto della risorsa per i browser Web.
- `x-amz-meta-file-permissions`— Il tipo di file e le autorizzazioni nel formato`<octal file type><octal permission mask>`, coerenti con la `st_mode` pagina man di Linux stat (2).

  > **Note**
  >
  > FSx for Lustre non importa né conserva informazioni. `setuid`

- `x-amz-meta-file-owner`— L'ID utente del proprietario (UID) espresso come numero intero.
- `x-amz-meta-file-group`— L'ID del gruppo (GID) espresso come numero intero.
- `x-amz-meta-file-atime`— L'ora dell'ultimo accesso, espressa in nanosecondi, dall'inizio dell'epoca Unix. Termina il valore temporale `conns`; altrimenti FSx for Lustre interpreta il valore come millisecondi.
- `x-amz-meta-file-mtime`— L'ora dell'ultima modifica, espressa in nanosecondi, dall'inizio dell'epoca Unix. Termina il valore temporale `conns`; in caso contrario, FSx for Lustre interpreta il valore come millisecondi.
- `x-amz-meta-user-agent`— L'agente utente, ignorato durante l'importazione di Lustre. FSx Durante l'esportazione, FSx for Lustre imposta questo valore su. `aws-fsx-lustre`

Quando si importano oggetti da S3 a cui non sono associati permessi POSIX, l'autorizzazione POSIX predefinita che FSx Lustre assegna a un file è. `755` Questa autorizzazione consente l'accesso in lettura ed esecuzione per tutti gli utenti e l'accesso in scrittura per il proprietario del file.

> **Note**
>
> FSx for Lustre non conserva alcun metadato personalizzato definito dall'utente sugli oggetti S3.

Collegamenti fisici ed esportazione su Amazon S3

Se l'esportazione automatica (con politiche NUOVE e MODIFICATE) è abilitata su un DRA nel file system, ogni collegamento fisico contenuto nel DRA viene esportato su Amazon S3 come oggetto S3 separato per ogni collegamento rigido. Se un file con più collegamenti fisici viene modificato sul file

system, tutte le copie in S3 vengono aggiornate, indipendentemente dal collegamento fisico utilizzato per modificare il file.

Se gli hard link vengono esportati in S3 utilizzando le attività di data repository (DRTs), ogni collegamento fisico contenuto nei percorsi specificati per il DRT viene esportato in S3 come oggetto S3 separato per ogni collegamento fisico. Se un file con più collegamenti fisici viene modificato sul file system, ogni copia in S3 viene aggiornata al momento dell'esportazione del rispettivo collegamento fisico, indipendentemente dal collegamento fisico utilizzato per modificare il file.

> **Important**
>
> Quando un nuovo file system FSx for Lustre viene collegato a un bucket S3 in cui gli hard link erano stati precedentemente esportati da un altro file system FSx for Lustre AWS DataSync o Amazon FSx File Gateway, gli hard link vengono successivamente importati come file separati nel nuovo file system.

Collegamenti fisici e file rilasciati

Un file rilasciato è un file i cui metadati sono presenti nel file system, ma il cui contenuto è archiviato solo in S3. Per ulteriori informazioni sui file rilasciati, vedi. Rilascio di file

> **Important**
>
> L'uso di collegamenti fisici in un file system con associazioni di archivi di dati (DRAs) è soggetto alle seguenti limitazioni:
>
> - L'eliminazione e la ricreazione di un file rilasciato che contiene più collegamenti fisici possono causare la sovrascrittura del contenuto di tutti i collegamenti fisici.
> - L'eliminazione di un file rilasciato comporta l'eliminazione del contenuto di tutti gli hard link che risiedono al di fuori di un'associazione di repository di dati.
> - La creazione di un collegamento fisico a un file rilasciato il cui oggetto S3 corrispondente si trova nelle classi di archiviazione S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive non creerà un nuovo oggetto in S3 per il collegamento fisico.

Procedura dettagliata: allegare le autorizzazioni POSIX durante il caricamento di oggetti in un bucket Amazon S3

La procedura seguente illustra il processo di caricamento degli oggetti in Amazon S3 con autorizzazioni POSIX. In questo modo puoi importare le autorizzazioni POSIX quando crei un FSx file system Amazon collegato a quel bucket S3.

Per caricare oggetti con autorizzazioni POSIX su Amazon S3

1. Dal tuo computer o macchina locale, usa i seguenti comandi di esempio per creare una directory di test (`s3cptestdir`) e un file (`s3cptest.txt`) che verranno caricati nel bucket S3.

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

   Il file e la directory appena creati hanno un ID utente (UID) del proprietario del file e un ID di gruppo (GID) pari a 500 e autorizzazioni, come mostrato nell'esempio precedente.

2. Chiama l'API Amazon S3 per creare la directory `s3cptestdir` con le autorizzazioni per i metadati. È necessario specificare il nome della directory con una barra finale (). / Per informazioni sui metadati POSIX supportati, vedere. Supporto per metadati POSIX per archivi di dati

   *bucket_name*Sostituiscilo con il nome effettivo del tuo bucket S3.

   ```
   $ 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. Verifica che le autorizzazioni POSIX siano contrassegnate con i metadati degli oggetti S3.

   ```
   $ aws s3api head-object --bucket bucket_name --key s3cptestdir/
   {
       "AcceptRanges": "bytes",
       "LastModified": "Fri, 08 Jan 2021 17:32:27 GMT",
       "ContentLength": 0,
   ```

```
    "ETag": "\"d41d8cd98f00b204e9800998ecf8427e\"",
    "VersionId": "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. Carica il file di test (creato nel passaggio 1) dal tuo computer al bucket S3 con le autorizzazioni per i metadati.

```
$ 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. Verifica che le autorizzazioni POSIX siano contrassegnate con i metadati degli oggetti S3.

```
$ aws s3api head-object --bucket bucket_name --key s3cptestdir/s3cptest.txt
{
    "AcceptRanges": "bytes",
    "LastModified": "Fri, 08 Jan 2021 17:33:35 GMT",
    "ContentLength": 26,
    "ETag": "\"eb33f7e1f44a14a8e2f9475ae3fc45d3\"",
    "VersionId": "w9ztRoEhB832m8NC3a_JTlTyIx7Uzql6",
    "ContentType": "text/plain",
    "Metadata": {
        "user-agent": "aws-fsx-lustre",
        "file-atime": "1595002920000000000ns",
        "file-owner": "500",
        "file-permissions": "0100664",
        "file-group": "500",
        "file-mtime": "1595002920000000000ns"
    }
}
```

6. Verifica le autorizzazioni sul FSx file system Amazon collegato al bucket S3.

```
$ 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
```

Sia la `s3cptestdir` directory che il `s3cptest.txt` file hanno i permessi POSIX importati.

Collegamento del file system a un bucket Amazon S3

Puoi collegare il tuo file system Amazon FSx for Lustre ai repository di dati in Amazon S3. Puoi creare il link durante la creazione del file system o in qualsiasi momento dopo la creazione del file system.

Un collegamento tra una directory sul file system e un bucket o prefisso S3 è chiamato associazione di repository di dati (DRA). È possibile configurare un massimo di 8 associazioni di repository di dati su un file system for Lustre. FSx È possibile mettere in coda un massimo di 8 richieste DRA, ma è possibile elaborare solo una richiesta alla volta per il file system. Ogni DRA deve avere una directory del file system univoca FSx per Lustre e un bucket o prefisso S3 univoco ad essa associato.

> **Note**
>
> Le associazioni di archivi di dati, l'esportazione automatica e il supporto per più archivi di dati non sono disponibili sui file system o sui file system Lustre FSx 2.10. `Scratch 1`

Per accedere agli oggetti nell'archivio di dati S3 come file e directory sul file system, i metadati di file e directory devono essere caricati nel file system. È possibile caricare i metadati da un archivio di dati collegato quando si crea il DRA o caricare i metadati per batch di file e directory a cui si desidera accedere utilizzando il file system FSx for Lustre in un secondo momento utilizzando

un'attività di importazione dell'archivio dati oppure utilizzare l'esportazione automatica per caricare automaticamente i metadati quando gli oggetti vengono aggiunti, modificati o eliminati dall'archivio dati.

È possibile configurare un DRA solo per l'importazione automatica, solo per l'esportazione automatica o per entrambi. Un'associazione di repository di dati configurata sia con l'importazione automatica che con l'esportazione automatica propaga i dati in entrambe le direzioni tra il file system e il bucket S3 collegato. Quando apporti modifiche ai dati nel tuo repository di dati S3, FSx for Lustre rileva le modifiche e quindi importa automaticamente le modifiche nel tuo file system. Quando crei, modifichi o elimini file, FSx for Lustre esporta automaticamente le modifiche in Amazon S3 in modo asincrono una volta che l'applicazione ha terminato la modifica del file.

⚠ Important

- Se modifichi lo stesso file sia nel file system che nel bucket S3, devi garantire il coordinamento a livello di applicazione per evitare conflitti. FSx for Lustre non impedisce scritture in conflitto in più posizioni.
- Per i file contrassegnati con un attributo immutabile, FSx for Lustre non è in grado di sincronizzare le modifiche tra il file system FSx for Lustre e un bucket S3 collegato al file system. L'impostazione di un flag immutabile per un periodo di tempo prolungato può causare un peggioramento delle prestazioni dello spostamento dei dati tra Amazon FSx e S3.

Quando crei un'associazione di repository di dati, puoi configurare le seguenti proprietà:

- Percorso del file system: immettere un percorso locale sul file system che punti a una directory (ad esempio`/ns1/`) o sottodirectory (ad esempio`/ns1/subdir/`) che verrà mappata one-to-one con il percorso del repository di dati specificato di seguito. La barra che precede il nome è obbligatoria. Due associazioni di repository di dati non possono avere percorsi di file system sovrapposti. Se ad esempio un repository di dati è associato al percorso del file system `/ns1`, non è possibile collegare un altro repository di dati al percorso del file system `/ns1/ns2`.

> **Note**
>
> Se indichi solo una barra (/) come percorso del file system, puoi collegare solo un repository di dati al file system. Puoi specificare solo "/" come percorso del file system per il primo repository di dati associato a un file system.

- Percorso dell'archivio dati: inserisci un percorso nell'archivio dati S3. Il percorso può essere un prefisso o un bucket S3 nel formato `s3://bucket-name/prefix/`. Questa proprietà specifica da dove verranno importati o esportati i file nel repository di dati S3. FSx for Lustre aggiungerà un «/» finale al percorso del tuo repository di dati se non ne fornisci uno. Ad esempio, se fornite un percorso di archivio dati di`s3://amzn-s3-demo-bucket/my-prefix`, FSx for Lustre lo interpreterà come. `s3://amzn-s3-demo-bucket/my-prefix/`

  Due associazioni di repository di dati non possono avere percorsi di repository di dati sovrapposti. Ad esempio, se un archivio di dati con percorso `s3://amzn-s3-demo-bucket/my-prefix/` è collegato al file system, non è possibile creare un'altra associazione di repository di dati con il percorso dell'archivio di dati. `s3://amzn-s3-demo-bucket/my-prefix/my-sub-prefix`
- Importa metadati dal repository: è possibile selezionare questa opzione per importare i metadati dall'intero repository di dati subito dopo aver creato l'associazione del repository di dati. In alternativa, è possibile eseguire un'attività di importazione dell'archivio di dati per caricare tutti o un sottoinsieme dei metadati dall'archivio di dati collegato nel file system in qualsiasi momento dopo la creazione dell'associazione all'archivio di dati.
- Impostazioni di importazione: scegliete una politica di importazione che specifichi il tipo di oggetti aggiornati (qualsiasi combinazione di oggetti nuovi, modificati ed eliminati) che verranno importati automaticamente dal bucket S3 collegato al file system. L'importazione automatica (nuova, modificata, eliminata) è attivata per impostazione predefinita quando aggiungi un repository di dati dalla console, ma è disabilitata per impostazione predefinita quando si utilizza l' FSx API AWS CLI o Amazon.
- Impostazioni di esportazione: scegli una politica di esportazione che specifichi il tipo di oggetti aggiornati (qualsiasi combinazione di nuovi, modificati ed eliminati) che verranno esportati automaticamente nel bucket S3. L'esportazione automatica (nuova, modificata, eliminata) è attivata per impostazione predefinita quando aggiungi un repository di dati dalla console, ma è disabilitata per impostazione predefinita quando si utilizza l' FSx API AWS CLI o Amazon.

Le impostazioni del percorso del file system e del percorso del repository dei dati forniscono una mappatura 1:1 tra i percorsi in Amazon FSx e le chiavi degli oggetti in S3.

Argomenti

Creazione di un link a un bucket S3

Le seguenti procedure illustrano il processo di creazione di un'associazione di repository di dati per un file system FSx for Lustre a un bucket S3 esistente, utilizzando and (). AWS Management Console AWS Command Line Interface AWS CLI Per informazioni sull'aggiunta di autorizzazioni a un bucket S3 per collegarlo al file system, consulta. Aggiungere le autorizzazioni per utilizzare gli archivi di dati in Amazon S3

> **Note**
>
> Gli archivi di dati non possono essere collegati a file system su cui sono abilitati i backup del file system. Disabilita i backup prima di collegarti a un archivio di dati.

Per collegare un bucket S3 durante la creazione di un file system (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo file system descritta Passaggio 1: crea il tuo FSx file system for Lustre nella sezione Guida introduttiva.
3. Apri la sezione Import/Export del repository di dati - opzionale. La funzionalità è disattivata per impostazione predefinita.
4. Scegli Importa dati da ed esporta dati su S3.
5. Nella finestra di dialogo Informazioni sull'associazione del repository di dati, fornisci informazioni per i seguenti campi.

- Percorso del file system: inserisci il nome di una directory di alto livello (ad esempio`/ns1`) o sottodirectory (ad esempio`/ns1/subdir`) all'interno del FSx file system Amazon che verrà associata al repository di dati S3. La barra anteriore del percorso è obbligatoria. Due associazioni di repository di dati non possono avere percorsi di file system sovrapposti. Se ad esempio un repository di dati è associato al percorso del file system `/ns1`, non è possibile collegare un altro repository di dati al percorso del file system `/ns1/ns2`. L'impostazione del percorso del file system deve essere univoca per tutte le associazioni di repository di dati per il file system.
- Percorso dell'archivio dati: inserisci il percorso di un bucket o prefisso S3 esistente da associare al tuo file system (ad esempio,). `s3://amzn-s3-demo-bucket/my-prefix` Due associazioni di repository di dati non possono avere percorsi di repository di dati sovrapposti. L'impostazione del percorso dell'archivio dati deve essere univoca per tutte le associazioni di archivi di dati per il file system.
- Importa metadati dal repository: seleziona questa proprietà per eseguire, facoltativamente, un'attività di importazione dell'archivio di dati per importare i metadati subito dopo la creazione del collegamento.

6. Per le impostazioni di importazione, facoltativo, imposta una politica di importazione che determini il modo in cui gli elenchi di file e directory vengono mantenuti aggiornati quando aggiungi, modifichi o elimini oggetti nel tuo bucket S3. Ad esempio, scegli Nuovo per importare i metadati nel tuo file system per i nuovi oggetti creati nel bucket S3. Per ulteriori informazioni sulle politiche di importazione, consulta. Importa automaticamente gli aggiornamenti dal tuo bucket S3
7. Per la politica di esportazione, imposta una politica di esportazione che determini il modo in cui i file vengono esportati nel bucket S3 collegato quando aggiungi, modifichi o elimini oggetti nel tuo file system. Ad esempio, scegli Modificato per esportare oggetti il cui contenuto o metadati sono stati modificati sul tuo file system. Per ulteriori informazioni sulle politiche di esportazione, consultateEsporta automaticamente gli aggiornamenti nel tuo bucket S3.
8. Continuare con la sezione successiva della procedura guidata per la creazione del file system.

Per collegare un bucket S3 a un file system esistente (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard, scegli File system, quindi seleziona il file system per cui desideri creare un'associazione di repository di dati.
3. Scegli la scheda Archivio dati.

4. Nel riquadro Associazioni di archivi di dati, scegli Crea associazione di archivi di dati.
5. Nella finestra di dialogo Informazioni sull'associazione agli archivi di dati, fornisci informazioni per i seguenti campi.

   - Percorso del file system: inserisci il nome di una directory di alto livello (ad esempio`/ns1`) o sottodirectory (ad esempio`/ns1/subdir`) all'interno del FSx file system Amazon che verrà associata al repository di dati S3. La barra anteriore del percorso è obbligatoria. Due associazioni di repository di dati non possono avere percorsi di file system sovrapposti. Se ad esempio un repository di dati è associato al percorso del file system `/ns1`, non è possibile collegare un altro repository di dati al percorso del file system `/ns1/ns2`. L'impostazione del percorso del file system deve essere univoca per tutte le associazioni di repository di dati per il file system.
   - Percorso dell'archivio dati: inserisci il percorso di un bucket o prefisso S3 esistente da associare al tuo file system (ad esempio,). `s3://amzn-s3-demo-bucket/my-prefix` Due associazioni di repository di dati non possono avere percorsi di repository di dati sovrapposti. L'impostazione del percorso dell'archivio dati deve essere univoca per tutte le associazioni di archivi di dati per il file system.
   - Importa metadati dal repository: seleziona questa proprietà per eseguire, facoltativamente, un'attività di importazione dell'archivio di dati per importare i metadati subito dopo la creazione del collegamento.
6. Per le impostazioni di importazione, facoltativo, imposta una politica di importazione che determini il modo in cui gli elenchi di file e directory vengono mantenuti aggiornati quando aggiungi, modifichi o elimini oggetti nel tuo bucket S3. Ad esempio, scegli Nuovo per importare i metadati nel tuo file system per i nuovi oggetti creati nel bucket S3. Per ulteriori informazioni sulle politiche di importazione, consulta. Importa automaticamente gli aggiornamenti dal tuo bucket S3
7. Per la politica di esportazione, imposta una politica di esportazione che determini il modo in cui i file vengono esportati nel bucket S3 collegato quando aggiungi, modifichi o elimini oggetti nel tuo file system. Ad esempio, scegli Modificato per esportare oggetti il cui contenuto o metadati sono stati modificati sul tuo file system. Per ulteriori informazioni sulle politiche di esportazione, consultateEsporta automaticamente gli aggiornamenti nel tuo bucket S3.
8. Scegli Create (Crea).

Per collegare un file system a un bucket S3 ()AWS CLI

L'esempio seguente crea un'associazione di repository di dati che collega un FSx file system Amazon a un bucket S3, con una politica di importazione che importa qualsiasi file nuovo o modificato nel

file system e una politica di esportazione che esporta file nuovi, modificati o eliminati nel bucket S3 collegato.

- Per creare un'associazione di repository di dati, usa il `create-data-repository-association` comando Amazon FSx CLI, come illustrato di seguito.

```
$ 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 restituisce immediatamente la descrizione JSON del DRA. Il DRA viene creato in modo asincrono.

È possibile utilizzare questo comando per creare un'associazione di archivi di dati anche prima che il file system abbia terminato la creazione. La richiesta verrà messa in coda e l'associazione all'archivio dati verrà creata una volta che il file system sarà disponibile.

Aggiornamento delle impostazioni di associazione agli archivi di dati

Puoi aggiornare le impostazioni di un'associazione di repository di dati esistente utilizzando l' AWS Management Console AWS CLI, la e l' FSx API Amazon, come illustrato nelle seguenti procedure.

> **Note**
>
> Non è possibile aggiornare l'`File system path`hor `Data repository path` di un DRA dopo la sua creazione. Se si desidera modificare l'`File system path`hor`Data repository path`, è necessario eliminare il DRA e crearlo nuovamente.

Per aggiornare le impostazioni per un'associazione di archivi di dati esistente (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard, scegli File system, quindi seleziona il file system che desideri gestire.
3. Scegli la scheda Archivio dati.

4. Nel riquadro Associazioni agli archivi di dati, scegli l'associazione agli archivi di dati che desideri modificare.
5. Scegli Aggiorna. Viene visualizzata una finestra di dialogo di modifica per l'associazione all'archivio di dati.
6. Per le impostazioni di importazione, facoltativo, puoi aggiornare la tua politica di importazione. Per ulteriori informazioni sulle politiche di importazione, consultaImporta automaticamente gli aggiornamenti dal tuo bucket S3.
7. Per le impostazioni di esportazione, facoltativo, puoi aggiornare la tua politica di esportazione. Per ulteriori informazioni sulle politiche di esportazione, consultaEsporta automaticamente gli aggiornamenti nel tuo bucket S3.
8. Scegli Aggiorna.

Per aggiornare le impostazioni per un'associazione di archivi di dati (CLI) esistente

- Per aggiornare un'associazione di repository di dati, usa il `update-data-repository-association` comando Amazon FSx CLI, come illustrato di seguito.

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

Dopo aver aggiornato correttamente le politiche di importazione ed esportazione dell'associazione di repository di dati, Amazon FSx restituisce la descrizione dell'associazione di repository di dati aggiornata come JSON.

Eliminazione di un'associazione a un bucket S3

Le seguenti procedure illustrano il processo di eliminazione di un'associazione di repository di dati da un FSx file system Amazon esistente a un bucket S3 esistente, utilizzando and (). AWS Management Console AWS Command Line Interface AWS CLI L'eliminazione dell'associazione del data repository scollega il file system dal bucket S3.

Per eliminare un collegamento da un file system a un bucket S3 (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.

2. Dalla dashboard, scegli File system, quindi seleziona il file system da cui desideri eliminare un'associazione di repository di dati.
3. Scegli la scheda Archivio dati.
4. Nel riquadro Associazioni agli archivi di dati, scegli l'associazione di archivi di dati che desideri eliminare.
5. Per Azioni, scegli Elimina associazione.
6. Nella finestra di dialogo Elimina, puoi scegliere Elimina dati nel file system per eliminare fisicamente i dati nel file system che corrispondono all'associazione del repository di dati.

   Scegliete questa opzione se intendete creare una nuova associazione di repository di dati utilizzando lo stesso percorso del file system ma puntando a un prefisso di bucket S3 diverso o se non avete più bisogno dei dati nel file system.
7. Scegli Elimina per rimuovere l'associazione del repository di dati dal file system.

Per eliminare un collegamento da un file system a un bucket S3 ()AWS CLI

L'esempio seguente elimina un'associazione di repository di dati che collega un FSx file system Amazon a un bucket S3. Il `--association-id` parametro specifica l'ID dell'associazione di repository di dati da eliminare.

- Per eliminare un'associazione di repository di dati, utilizza il `delete-data-repository-association` comando Amazon FSx CLI, come illustrato di seguito.

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

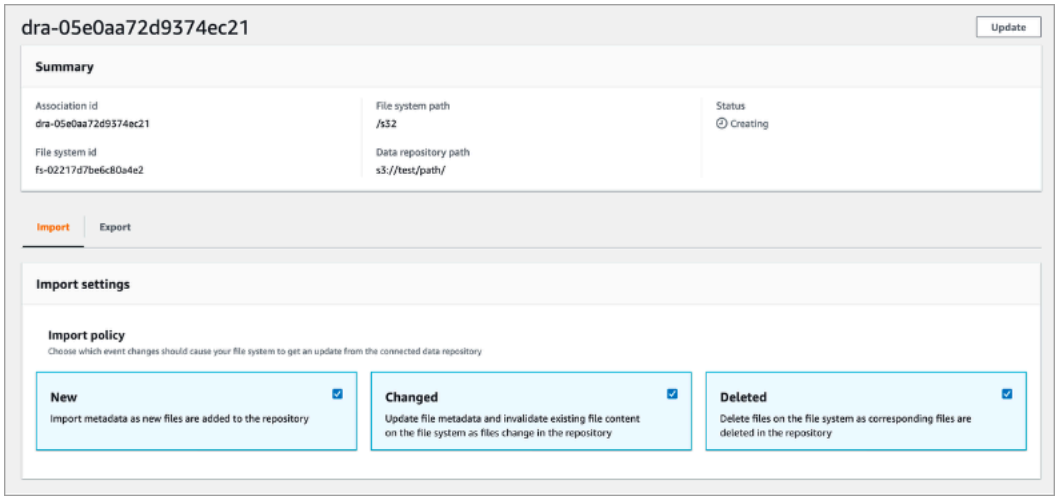
Dopo aver eliminato con successo l'associazione del repository di dati, Amazon FSx restituisce la sua descrizione come JSON.

Visualizzazione dei dettagli dell'associazione ai repository di dati

È possibile visualizzare i dettagli di un'associazione di repository di dati utilizzando la console FSx for Lustre AWS CLI, l'e l'API. I dettagli includono l'ID di associazione del DRA, il percorso del file system, il percorso dell'archivio dati, le impostazioni di importazione, le impostazioni di esportazione, lo stato e l'ID del file system associato.

Per visualizzare i dettagli del DRA (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard, scegli File system, quindi seleziona il file system per cui desideri visualizzare i dettagli di un'associazione di repository di dati.
3. Scegli la scheda Archivio dati.
4. Nel riquadro Associazioni agli archivi di dati, scegli l'associazione di archivi di dati che desideri visualizzare. Viene visualizzata la pagina di riepilogo, che mostra i dettagli del DRA.



Per visualizzare i dettagli DRA (CLI)

- Per visualizzare i dettagli di una specifica associazione di repository di dati, utilizza il `describe-data-repository-associations` comando Amazon FSx CLI, come illustrato di seguito.

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

  Amazon FSx restituisce la descrizione dell'associazione del repository di dati come JSON.

Stato del ciclo di vita dell'associazione al repository di dati

Lo stato del ciclo di vita dell'associazione del data repository fornisce informazioni sullo stato di uno specifico DRA. Un'associazione di repository di dati può avere i seguenti stati del ciclo di vita:

- Creazione: Amazon FSx sta creando l'associazione del repository di dati tra il file system e il repository di dati collegato. L'archivio di dati non è disponibile.

- Disponibile: l'associazione dell'archivio di dati è disponibile per l'uso.
- Aggiornamento: l'associazione dell'archivio di dati è in corso di un aggiornamento avviato dal cliente che potrebbe influire sulla sua disponibilità.
- Eliminazione: l'associazione all'archivio di dati è in fase di eliminazione avviata dal cliente.
- Configurato erroneamente: Amazon FSx non può importare automaticamente gli aggiornamenti dal bucket S3 o esportare automaticamente gli aggiornamenti nel bucket S3 finché la configurazione dell'associazione del repository di dati non viene corretta.

  Un DRA può essere configurato in modo errato a causa di quanto segue:

  - Amazon FSx non dispone delle autorizzazioni IAM necessarie per accedere al bucket S3.
  - La configurazione della notifica FSx degli eventi sul bucket S3 viene eliminata o modificata.
  - Il bucket S3 contiene notifiche di eventi esistenti che si sovrappongono ai tipi di eventi. FSx

  Dopo aver risolto il problema sottostante, il DRA torna automaticamente allo stato Disponibile entro 15 minuti oppure è possibile attivare immediatamente la modifica dello stato utilizzando il comando. AWS CLI update-data-repository-association
- Fallita: l'associazione del repository di dati si trova in uno stato terminale che non può essere ripristinato (ad esempio, perché il percorso del file system viene eliminato o il bucket S3 viene eliminato).

Puoi visualizzare lo stato del ciclo di vita di un'associazione di repository di dati utilizzando la FSx console Amazon, e l' AWS Command Line Interface API Amazon. FSx Per ulteriori informazioni, consulta Visualizzazione dei dettagli dell'associazione ai repository di dati.

Utilizzo di bucket Amazon S3 crittografati lato server

FSx for Lustre supporta i bucket Amazon S3 che utilizzano la crittografia lato server con chiavi gestite da S3 (SSE-S3) e con storage in (SSE-KMS). AWS KMS keys AWS Key Management Service

Se desideri che Amazon FSx crittografi i dati durante la scrittura nel tuo bucket S3, devi impostare la crittografia predefinita sul bucket S3 su SSE-S3 o SSE-KMS. Per ulteriori informazioni, consulta Configurazione della crittografia predefinita nella Guida per l'utente di Amazon S3. Quando scrivi file nel tuo bucket S3, Amazon FSx segue la politica di crittografia predefinita del tuo bucket S3.

Per impostazione predefinita, Amazon FSx supporta i bucket S3 crittografati tramite SSE-S3. Se desideri collegare il tuo FSx file system Amazon a un bucket S3 crittografato utilizzando la crittografia

SSE-KMS, devi aggiungere una dichiarazione alla politica delle chiavi gestite dai clienti che consenta ad Amazon di crittografare e FSx decrittografare gli oggetti nel tuo bucket S3 utilizzando la tua chiave KMS.

La seguente dichiarazione consente a uno specifico FSx file system Amazon di crittografare e decrittografare oggetti per uno specifico bucket S3,. *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

Se utilizzi un KMS con CMK per crittografare il tuo bucket S3 con le chiavi del bucket S3 abilitate, impostalo sull'ARN del bucket, non sull'ARN `EncryptionContext` dell'oggetto, come in questo esempio:

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

```
    }
```

La seguente informativa sulla politica consente a tutti i FSx file system Amazon del tuo account di collegarsi a un bucket S3 specifico.

```
{
      "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-*"
        }
      }
}
```

Accesso a bucket Amazon S3 crittografati lato server da un VPC Account AWS diverso o condiviso

Dopo aver creato un file system FSx for Lustre collegato a un bucket Amazon S3 crittografato, devi quindi concedere al ruolo collegato al servizio (SLR)

`AWSServiceRoleForFSxS3Access_`*`fs-01234567890`* l'accesso alla chiave KMS utilizzata per crittografare il bucket S3 prima di leggere o scrivere dati dal bucket S3 collegato. Puoi utilizzare un ruolo IAM che dispone già delle autorizzazioni per la chiave KMS.

> **Note**
>
> Questo ruolo IAM deve trovarsi nell'account in cui è stato creato il file system FSx for Lustre (che è lo stesso account della SLR S3), non nell'account a cui appartiene la chiave KMS/ bucket S3.

Utilizzi il ruolo IAM per chiamare la seguente AWS KMS API per creare una concessione per S3 SLR in modo che la SLR ottenga l'autorizzazione per gli oggetti S3. Per trovare l'ARN associato alla tua reflex, cerca i ruoli IAM utilizzando l'ID del file system come stringa di ricerca.

```
$ 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"
```

Per ulteriori informazioni sui ruoli collegati al servizio, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

Importazione delle modifiche dal tuo archivio di dati

Puoi importare modifiche ai dati e ai metadati POSIX da un repository di dati collegato al tuo file system Amazon FSx. I metadati POSIX associati includono proprietà, autorizzazioni e timestamp.

Per importare le modifiche al file system, utilizzate uno dei seguenti metodi:

- Configurate il file system per importare automaticamente file nuovi, modificati o eliminati dal repository di dati collegato. Per ulteriori informazioni, consulta Importa automaticamente gli aggiornamenti dal tuo bucket S3.
- Seleziona l'opzione per importare i metadati quando crei un'associazione di repository di dati. Ciò avvierà un'attività di importazione dell'archivio di dati subito dopo la creazione dell'associazione dell'archivio di dati.

- Utilizza un'attività di importazione di repository di dati su richiesta. Per ulteriori informazioni, consulta Utilizzo delle attività di archiviazione dei dati per importare le modifiche.

Le attività automatiche di importazione e importazione dell'archivio di dati possono essere eseguite contemporaneamente.

Quando attivi l'importazione automatica per un'associazione di repository di dati, il file system aggiorna automaticamente i metadati dei file man mano che gli oggetti vengono creati, modificati o eliminati in S3. Quando selezioni l'opzione per importare i metadati durante la creazione di un'associazione di repository di dati, il file system importa i metadati per tutti gli oggetti nel repository di dati. Quando si esegue l'importazione utilizzando un'attività di importazione del repository di dati, il file system importa solo i metadati per gli oggetti che sono stati creati o modificati dopo l'ultima importazione.

FSx for Lustre copia automaticamente il contenuto di un file dal repository di dati e lo carica nel file system quando l'applicazione accede per la prima volta al file nel file system. Questo movimento di dati è gestito da FSx for Lustre ed è trasparente per le applicazioni. Le letture successive di questi file vengono fornite direttamente dal file system con latenze inferiori al millisecondo.

Potete anche precaricare l'intero file system o una directory all'interno del file system. Per ulteriori informazioni, consulta Precaricamento dei file nel file system. Se richiedi il precaricamento di più file contemporaneamente, FSx for Lustre carica i file dal tuo repository di dati Amazon S3 in parallelo.

FSx for Lustre importa solo oggetti S3 con chiavi oggetto conformi a POSIX. Sia le attività automatiche di importazione che quelle di importazione del repository di dati importano i metadati POSIX. Per ulteriori informazioni, consulta Supporto per metadati POSIX per archivi di dati.

> **Note**
>
> FSx for Lustre non supporta l'importazione di metadati per i link simbolici (collegamenti simbolici) dalle classi di archiviazione S3 Glacier Flexible Retrieval e S3 Glacier Deep Archive. È possibile importare i metadati per gli oggetti S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive che non sono collegamenti simbolici (ovvero, viene creato un inode sul file system for Lustre con i metadati corretti). FSx Tuttavia, per leggere questi dati dal file system, è necessario prima ripristinare l'oggetto S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. L'importazione di dati di file direttamente da oggetti Amazon S3 nella classe di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive in for Lustre non è supportata. FSx

Importa automaticamente gli aggiornamenti dal tuo bucket S3

Puoi configurare FSx Lustre in modo che aggiorni automaticamente i metadati nel file system man mano che gli oggetti vengono aggiunti, modificati o eliminati dal tuo bucket S3. FSx for Lustre crea, aggiorna o elimina l'elenco di file e directory, corrispondente alla modifica in S3. Se l'oggetto modificato nel bucket S3 non contiene più i relativi metadati, FSx for Lustre mantiene i valori correnti dei metadati del file, incluse le autorizzazioni correnti.

> **Note**
>
> Il file system FSx for Lustre e il bucket S3 collegato devono trovarsi nello stesso per importare automaticamente gli aggiornamenti. Regione AWS

È possibile configurare l'importazione automatica quando si crea l'associazione del repository di dati e aggiornare le impostazioni di importazione automatica in qualsiasi momento utilizzando la console di FSx gestione, l'o l'API AWS CLI. AWS

> **Note**
>
> È possibile configurare sia l'importazione automatica che l'esportazione automatica sulla stessa associazione di repository di dati. Questo argomento descrive solo la funzionalità di importazione automatica.

> **Important**
>
> - Se un oggetto viene modificato in S3 con tutte le politiche di importazione automatiche abilitate e l'esportazione automatica disabilitata, il contenuto di quell'oggetto viene sempre importato in un file corrispondente nel file system. Se un file esiste già nella posizione di destinazione, il file viene sovrascritto.
> - Se un file viene modificato sia nel file system che in S3, con tutte le politiche di importazione ed esportazione automatiche abilitate, il file nel file system o l'oggetto in S3 potrebbero essere sovrascritti dall'altro. Non è garantito che una modifica successiva in una posizione sovrascriva una modifica precedente in un'altra posizione. Se modifichi lo stesso file sia nel file system che nel bucket S3, dovresti garantire il coordinamento a livello

di applicazione per prevenire tali conflitti. FSx for Lustre non impedisce scritture in conflitto in più posizioni.

La politica di importazione specifica come desiderate che FSx Lustre aggiorni il file system man mano che il contenuto cambia nel bucket S3 collegato. Un'associazione di archivi di dati può avere una delle seguenti politiche di importazione:

- Nuovo: FSx for Lustre aggiorna automaticamente i metadati di file e directory solo quando vengono aggiunti nuovi oggetti al repository di dati S3 collegato.
- Modificato: FSx for Lustre aggiorna automaticamente i metadati di file e directory solo quando viene modificato un oggetto esistente nel repository di dati.
- Eliminato — FSx for Lustre aggiorna automaticamente i metadati di file e directory solo quando viene eliminato un oggetto nel data repository.
- Qualsiasi combinazione di New, Changed ed Deleted — FSx for Lustre aggiorna automaticamente i metadati di file e directory quando si verifica una delle azioni specificate nell'archivio di dati S3. Ad esempio, puoi specificare che il file system venga aggiornato quando un oggetto viene aggiunto a (Nuovo) o rimosso da (Eliminato) dal repository S3, ma non aggiornato quando un oggetto viene modificato.
- Nessuna policy configurata: FSx for Lustre non aggiorna i metadati di file e directory sul file system quando gli oggetti vengono aggiunti, modificati o eliminati dal repository di dati S3. Se non configuri una politica di importazione, l'importazione automatica è disabilitata per l'associazione del repository di dati. È comunque possibile importare manualmente le modifiche ai metadati utilizzando un'attività di importazione dell'archivio dati, come descritto in. Utilizzo delle attività di archiviazione dei dati per importare le modifiche

Important

L'importazione automatica non sincronizzerà le seguenti azioni S3 con il file system Linked FSx for Lustre:

- Eliminazione di un oggetto utilizzando le scadenze del ciclo di vita degli oggetti S3
- Eliminazione permanente della versione corrente dell'oggetto in un bucket abilitato al controllo delle versioni
- Annullamento di un oggetto in un bucket abilitato al controllo delle versioni

Nella maggior parte dei casi d'uso, si consiglia di configurare una politica di importazione di Nuovo, Modificato ed Eliminato. Questa politica garantisce che tutti gli aggiornamenti effettuati nel repository di dati S3 collegato vengano importati automaticamente nel file system.

Quando imposti una politica di importazione per aggiornare i metadati dei file e delle directory del file system in base alle modifiche nel repository di dati S3 collegato, FSx for Lustre crea una configurazione di notifica degli eventi sul bucket S3 collegato. La configurazione della notifica degli eventi è denominata. `FSx` Non modificare o eliminare la configurazione della notifica `FSx` degli eventi nel bucket S3: in questo modo si impedirà l'importazione automatica di metadati aggiornati di file e directory nel file system.

Quando FSx for Lustre aggiorna un elenco di file che è stato modificato nel repository di dati S3 collegato, sovrascrive il file locale con la versione aggiornata, anche se il file è bloccato in scrittura.

FSx for Lustre fa del suo meglio per aggiornare il file system. FSx for Lustre non è in grado di aggiornare il file system nelle seguenti situazioni:

- Se FSx for Lustre non dispone dell'autorizzazione per aprire l'oggetto S3 nuovo o modificato. In questo caso, FSx for Lustre salta l'oggetto e continua. Lo stato del ciclo di vita DRA non è influenzato.
- Se FSx for Lustre non dispone di autorizzazioni a livello di bucket, ad esempio for. `GetBucketAcl` Ciò causerà una configurazione errata dello stato del ciclo di vita del repository di dati. Per ulteriori informazioni, consulta Stato del ciclo di vita dell'associazione al repository di dati.
- Se la configurazione di notifica `FSx` degli eventi sul bucket S3 collegato viene eliminata o modificata. Ciò causerà una configurazione errata dello stato del ciclo di vita del repository di dati. Per ulteriori informazioni, consulta Stato del ciclo di vita dell'associazione al repository di dati.

Ti consigliamo di attivare la registrazione in CloudWatch Logs per registrare le informazioni su file o directory che non possono essere importati automaticamente. Gli avvisi e gli errori nel registro contengono informazioni sul motivo dell'errore. Per ulteriori informazioni, consulta Registri degli eventi del data repository.

Prerequisiti

FSx Affinché Lustre importi automaticamente file nuovi, modificati o eliminati dal bucket S3 collegato, sono necessarie le seguenti condizioni:

- Il file system e il bucket S3 collegato si trovano nello stesso. Regione AWS

- Il bucket S3 non ha uno stato del ciclo di vita configurato in modo errato. Per ulteriori informazioni, consulta Stato del ciclo di vita dell'associazione al repository di dati.
- Il tuo account dispone delle autorizzazioni necessarie per configurare e ricevere notifiche di eventi sul bucket S3 collegato.

Tipi di modifiche ai file supportati

FSx for Lustre supporta l'importazione delle seguenti modifiche ai file e alle directory che si verificano nel bucket S3 collegato:

- Modifiche al contenuto dei file.
- Modifiche ai metadati di file o directory.
- Modifiche alla destinazione o ai metadati del collegamento simbolico.
- Eliminazioni di file e cartelle. Se elimini un oggetto nel bucket S3 collegato che corrisponde a una directory nel file system (ovvero un oggetto con un nome chiave che termina con una barra), FSx for Lustre elimina la directory corrispondente sul file system solo se è vuota.

Aggiornamento delle impostazioni di importazione

Puoi configurare le impostazioni di importazione di un file system per un bucket S3 collegato quando crei l'associazione del repository di dati. Per ulteriori informazioni, consulta Creazione di un link a un bucket S3.

Puoi anche aggiornare le impostazioni di importazione in qualsiasi momento, inclusa la politica di importazione. Per ulteriori informazioni, consulta Aggiornamento delle impostazioni di associazione agli archivi di dati.

Monitoraggio dell'importazione automatica

Se la velocità di modifica nel bucket S3 supera la velocità con cui l'importazione automatica può elaborare queste modifiche, le corrispondenti modifiche ai metadati importate nel file system FSx for Lustre vengono ritardate. In tal caso, puoi utilizzare la `AgeOfOldestQueuedMessage` metrica per monitorare l'età della modifica più vecchia in attesa di essere elaborata mediante importazione automatica. Per ulteriori informazioni su questa metrica, consulta. FSx per le metriche del repository Lustre S3

Se il ritardo nell'importazione delle modifiche ai metadati supera i 14 giorni (in base alla `AgeOfOldestQueuedMessage` metrica), le modifiche nel bucket S3 che non sono state elaborate

mediante l'importazione automatica non vengono importate nel file system. Inoltre, il ciclo di vita dell'associazione al repository di dati è contrassegnato come MAL CONFIGURATO e l'importazione automatica viene interrotta. Se hai abilitato l'esportazione automatica, l'esportazione automatica continua a monitorare le modifiche del file system FSx for Lustre. Tuttavia, le modifiche aggiuntive non vengono sincronizzate dal file system FSx for Lustre a S3.

Per riportare l'associazione del repository di dati dallo stato del ciclo di vita ERRONEAMENTE CONFIGURATO allo stato del ciclo di vita DISPONIBILE, è necessario aggiornare l'associazione del repository di dati. È possibile aggiornare l'associazione del repository di dati utilizzando il comando update-data-repository-associationCLI (o l'operazione API UpdateDataRepositoryAssociationcorrispondente). L'unico parametro di richiesta di cui hai bisogno è l'associazione `AssociationID` di repository di dati che desideri aggiornare.

Dopo che lo stato del ciclo di vita dell'associazione al repository di dati è passato a AVAILABLE, l'importazione automatica (e l'esportazione automatica se abilitata) si riavvia. Al riavvio, l'esportazione automatica riprende la sincronizzazione delle modifiche del file system su S3. Per sincronizzare i metadati degli oggetti nuovi e modificati in S3 con il file system FSx for Lustre che non sono stati importati o che provengono da quando l'associazione dell'archivio di dati era in uno stato configurato erroneamente, esegui un'attività di importazione dell'archivio di dati. Le attività di importazione del repository di dati non sincronizzano le eliminazioni nel bucket S3 con il file system for Lustre. FSx Se desideri sincronizzare completamente S3 con il tuo file system (incluse le eliminazioni), devi ricreare il file system.

Per garantire che i ritardi nell'importazione delle modifiche ai metadati non superino i 14 giorni, ti consigliamo di impostare un allarme sulla `AgeOfOldestQueuedMessage` metrica e di ridurre l'attività nel tuo bucket S3 se la metrica supera la soglia di allarme. `AgeOfOldestQueuedMessage` Per un file system FSx for Lustre collegato a un bucket S3 con un singolo shard che invia continuamente il numero massimo di modifiche possibili da S3, con la sola importazione automatica in esecuzione sul file system FSx for Lustre, l'importazione automatica può elaborare un arretrato di 7 ore di modifiche S3 entro 14 giorni.

Inoltre, con una singola azione S3, puoi generare più modifiche di quante ne possa mai elaborare l'importazione automatica in 14 giorni. Esempi di questi tipi di azioni includono, a titolo esemplificativo, i AWS Snowball caricamenti su S3 e le eliminazioni su larga scala. Se apporti una modifica su larga scala al tuo bucket S3 che desideri sincronizzare con il file system FSx for Lustre, per evitare che le modifiche automatiche all'importazione superino i 14 giorni, dovresti eliminare il file system e ricrearlo una volta completata la modifica a S3.

Se la tua `AgeOfOldestQueuedMessage` metrica è in crescita, esamina il bucket `GetRequests` S3 e le `DeleteRequests` metriche per verificare se ci sono cambiamenti di attività che potrebbero causare un aumento della frequenza e/o del numero di modifiche inviate all'importazione automatica. `PutRequests` `PostRequests` Per informazioni sui parametri S3 disponibili, consulta Monitoring Amazon S3 nella Amazon S3 User Guide.

Per un elenco di tutte le metriche disponibili FSx per Lustre, consulta. Monitoraggio con Amazon CloudWatch

Utilizzo delle attività di archiviazione dei dati per importare le modifiche

L'attività di importazione dell'archivio di dati importa i metadati degli oggetti nuovi o modificati nel tuo repository di dati S3, creando un nuovo elenco di file o directory per ogni nuovo oggetto nell'archivio di dati S3. Per ogni oggetto che è stato modificato nel repository di dati, l'elenco di file o directory corrispondente viene aggiornato con i nuovi metadati. Non viene intrapresa alcuna azione per gli oggetti che sono stati eliminati dal data repository.

Utilizza le seguenti procedure per importare le modifiche ai metadati utilizzando la FSx console Amazon e la CLI. Tieni presente che puoi utilizzare un'attività di archivio dati per più attività. DRAs

Per importare le modifiche ai metadati (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione, scegli File system, quindi scegli il tuo Lustre file system.
3. Scegli la scheda Archivio dati.
4. Nel riquadro Associazioni agli archivi di dati, scegli le associazioni degli archivi di dati per cui desideri creare l'attività di importazione.
5. Dal menu Azioni, scegli Importa attività. Questa scelta non è disponibile se il file system non è collegato a un archivio di dati. Viene visualizzata la pagina dell'attività Crea archivio dati di importazione.
6. (Facoltativo) Specificate fino a 32 directory o file da importare dai bucket S3 collegati fornendo i percorsi di tali directory o file nei percorsi del repository di dati da importare.

> **Note**
>
> Se un percorso fornito non è valido, l'attività ha esito negativo.

7. (Facoltativo) Scegliete Abilita in Rapporto di completamento per generare un rapporto sul completamento dell'attività dopo il completamento dell'attività. Un rapporto sul completamento dell'attività fornisce dettagli sui file elaborati dall'attività che soddisfano l'ambito fornito in Ambito del rapporto. Per specificare la posizione in cui Amazon FSx deve recapitare il report, inserisci un percorso relativo su un repository di dati S3 collegato per Report path.
8. Scegli Create (Crea).

   Una notifica nella parte superiore della pagina File system mostra l'attività che hai appena creato in corso.

Per visualizzare lo stato e i dettagli dell'attività, scorri verso il basso fino al riquadro Attività del data Repository nella scheda Data Repository per il file system. L'ordinamento predefinito mostra l'attività più recente nella parte superiore dell'elenco.

Per visualizzare un riepilogo dell'attività da questa pagina, scegli Task ID per l'attività appena creata. Viene visualizzata la pagina di riepilogo dell'attività.

Per importare modifiche ai metadati (CLI)

- Utilizzate il comando `create-data-repository-task`CLI per importare le modifiche ai metadati sul file system FSx for Lustre. L'operazione API corrispondente è. `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
  ```

  Dopo aver creato correttamente l'attività di archiviazione dei dati, Amazon FSx restituisce la descrizione dell'attività come JSON.

Dopo aver creato l'attività per importare i metadati dall'archivio di dati collegato, puoi controllare lo stato dell'attività di importazione dell'archivio di dati. Per ulteriori informazioni sulla visualizzazione delle attività del data repository, vedere. Accesso alle attività del repository di dati

Precaricamento dei file nel file system

Facoltativamente, puoi precaricare contenuti, singoli file o directory nel tuo file system.

Importazione di file tramite comandi HSM

Amazon FSx copia i dati dal tuo repository di dati Amazon S3 al primo accesso a un file. Grazie a questo approccio, la lettura o scrittura iniziale su un file comporta una piccola latenza. Se l'applicazione è sensibile a questa latenza e sapete a quali file o directory deve accedere, potete facoltativamente precaricare il contenuto di singoli file o directory. A tale scopo, utilizzare il comando seguente. `hsm_restore`

È possibile utilizzare il `hsm_action` comando (rilasciato con l'utilità `lfs` utente) per verificare che il contenuto del file abbia terminato il caricamento nel file system. Il valore restituito da `NOOP` indica che il file è stato caricato correttamente. Esegui i seguenti comandi da un'istanza di calcolo con il file system montato. Sostituiscilo *`path/to/file`* con il percorso del file che stai precaricando nel file system.

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

È possibile precaricare l'intero file system o un'intera directory all'interno del file system utilizzando i seguenti comandi. (La e commerciale finale esegue un comando come processo in background). Se richiedi il precaricamento di più file contemporaneamente, Amazon FSx carica i file dal tuo repository di dati Amazon S3 in parallelo. Se un file è già stato caricato nel file system, il `hsm_restore` comando non lo ricarica.

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

> **Note**
>
> Se il bucket S3 collegato è più grande del file system, dovresti essere in grado di importare tutti i metadati dei file nel tuo file system. Tuttavia, puoi caricare solo la quantità effettiva di dati di file che rientra nello spazio di archiviazione rimanente del file system. Riceverai un errore se tenti di accedere ai dati dei file quando non c'è più spazio di archiviazione sul file system. In tal caso, è possibile aumentare la quantità di capacità di archiviazione in base alle esigenze. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione.

Fase di convalida

Puoi eseguire lo script bash elencato di seguito per aiutarti a scoprire quanti file o oggetti si trovano in uno stato di archiviazione (rilasciato).

Per migliorare le prestazioni dello script, in particolare su file system con un numero elevato di file, i thread della CPU vengono determinati automaticamente in base al file. `/proc/cpuproc` Cioè, vedrai prestazioni più veloci con un'istanza Amazon EC2 con un numero di vCPU più elevato.

1. Configura lo script bash.

```
#!/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
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. Rendi eseguibile lo script:

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

3. Esegui lo script, come nell'esempio seguente:

```
$ ./find_lustre_released_files.sh /fsx1/sample
Searching in /fsx1/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
```

Se sono presenti oggetti rilasciati, esegui un ripristino in blocco nelle directory desiderate per importare i file in FSx for Lustre da S3, come nell'esempio seguente:

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

Nota che ci `hsm_restore` vorrà del tempo se ci sono milioni di file.

Esportazione delle modifiche nel repository di dati

È possibile esportare le modifiche ai dati e alle modifiche ai metadati POSIX dal file system FSx for Lustre a un repository di dati collegato. I metadati POSIX associati includono proprietà, autorizzazioni e timestamp.

Per esportare le modifiche dal file system, utilizzate uno dei seguenti metodi.

- Configura il tuo file system per esportare automaticamente file nuovi, modificati o eliminati nel tuo repository di dati collegato. Per ulteriori informazioni, consulta Esporta automaticamente gli aggiornamenti nel tuo bucket S3.
- Utilizza un'attività di esportazione di repository di dati su richiesta. Per ulteriori informazioni, consulta Utilizzo delle attività dell'archivio dati per esportare le modifiche

Le attività automatiche di esportazione ed esportazione dell'archivio di dati non possono essere eseguite contemporaneamente.

> **Important**
>
> L'esportazione automatica non sincronizzerà le seguenti operazioni sui metadati sul file system con S3 se gli oggetti corrispondenti sono archiviati in S3 Glacier Flexible Retrieval:
>
> - chmod
> - masticato
> - rinominare

Quando si attiva l'esportazione automatica per un'associazione di archivi di dati, il file system esporta automaticamente i dati dei file e le modifiche ai metadati man mano che i file vengono creati, modificati o eliminati. Quando esportate file o directory utilizzando un'operazione di esportazione di un archivio di dati, il file system esporta solo i file di dati e i metadati che sono stati creati o modificati dopo l'ultima esportazione.

Sia le attività di esportazione automatica che quelle di esportazione del repository di dati esportano i metadati POSIX. Per ulteriori informazioni, consulta Supporto per metadati POSIX per archivi di dati.

> **Important**
>
> - Per garantire che FSx for Lustre possa esportare i dati nel bucket S3, è necessario archiviarli in un formato compatibile con UTF-8.
> - Le chiavi oggetto S3 hanno una lunghezza massima di 1.024 byte. FSx for Lustre non esporterà file la cui chiave oggetto S3 corrispondente sarebbe più lunga di 1.024 byte.

> **Note**
>
> Tutti gli oggetti creati dalle attività automatiche di esportazione ed esportazione del repository dei dati vengono scritti utilizzando la classe di archiviazione S3 Standard.

Argomenti

Esporta automaticamente gli aggiornamenti nel tuo bucket S3

È possibile configurare il file system FSx for Lustre per aggiornare automaticamente il contenuto di un bucket S3 collegato man mano che i file vengono aggiunti, modificati o eliminati dal file system. FSx for Lustre crea, aggiorna o elimina l'oggetto in S3, corrispondente alla modifica nel file system.

> **Note**
>
> L'esportazione automatica non è disponibile FSx per i file system o i file system Lustre 2.10. `Scratch 1`

È possibile esportare in un archivio di dati che si trova nello Regione AWS stesso file system o in un altro. Regione AWS

È possibile configurare l'esportazione automatica quando si crea l'associazione del repository di dati e aggiornare le impostazioni di esportazione automatica in qualsiasi momento utilizzando la console di FSx gestione AWS CLI, l'API e l' AWS API.

> **Important**
>
> - Se un file viene modificato nel file system con tutte le politiche di esportazione automatiche abilitate e l'importazione automatica disabilitata, il contenuto di quel file viene sempre esportato in un oggetto corrispondente in S3. Se un oggetto esiste già nella posizione di destinazione, l'oggetto viene sovrascritto.

- Se un file viene modificato sia nel file system che in S3, con tutte le politiche di importazione ed esportazione automatiche abilitate, il file nel file system o l'oggetto in S3 potrebbero essere sovrascritti dall'altro. Non è garantito che una modifica successiva in una posizione sovrascriva una modifica precedente in un'altra posizione. Se modifichi lo stesso file sia nel file system che nel bucket S3, dovresti garantire il coordinamento a livello di applicazione per prevenire tali conflitti. FSx for Lustre non impedisce scritture in conflitto in più posizioni.

La politica di esportazione specifica come desiderate che FSx Lustre aggiorni il bucket S3 collegato man mano che il contenuto cambia nel file system. Un'associazione di archivi di dati può avere una delle seguenti politiche di esportazione automatiche:

- Nuovo: FSx for Lustre aggiorna automaticamente l'archivio di dati S3 solo quando viene creato un nuovo file, directory o collegamento simbolico sul file system.
- Modificato: FSx for Lustre aggiorna automaticamente l'archivio di dati S3 solo quando viene modificato un file esistente nel file system. Per le modifiche al contenuto del file, il file deve essere chiuso prima di essere propagato nell'archivio S3. Le modifiche ai metadati (ridenominazione, proprietà, autorizzazioni e timestamp) vengono propagate al termine dell'operazione. Per rinominare le modifiche (incluse le mosse), l'oggetto S3 esistente (precedentemente rinominato) viene eliminato e viene creato un nuovo oggetto S3 con il nuovo nome.
- Eliminato — FSx for Lustre aggiorna automaticamente l'archivio di dati S3 solo quando un file, una directory o un collegamento simbolico viene eliminato dal file system.
- Qualsiasi combinazione di Nuovo, Modificato ed Eliminato — FSx for Lustre aggiorna automaticamente l'archivio di dati S3 quando si verifica una delle azioni specificate nel file system. Ad esempio, puoi specificare che l'archivio S3 venga aggiornato quando un file viene aggiunto a (Nuovo) o rimosso da (Eliminato) dal file system, ma non quando un file viene modificato.
- Nessuna policy configurata: FSx for Lustre non aggiorna automaticamente l'archivio di dati S3 quando i file vengono aggiunti, modificati o eliminati dal file system. Se non configuri una politica di esportazione, l'esportazione automatica è disabilitata. È comunque possibile esportare manualmente le modifiche utilizzando un'attività di esportazione dell'archivio dati, come descritto inUtilizzo delle attività dell'archivio dati per esportare le modifiche.

Nella maggior parte dei casi d'uso, si consiglia di configurare una politica di esportazione di Nuovo, Modificato ed Eliminato. Questa politica garantisce che tutti gli aggiornamenti effettuati sul file system vengano esportati automaticamente nel repository di dati S3 collegato.

Ti consigliamo di attivare la registrazione in CloudWatch Logs per registrare le informazioni su file o directory che non possono essere esportati automaticamente. Gli avvisi e gli errori nel registro contengono informazioni sul motivo dell'errore. Per ulteriori informazioni, consulta Registri degli eventi del data repository.

> **Note**
>
> Sebbene l'ora di accesso (`atime`) e l'ora di modifica (`mtime`) siano sincronizzate con S3 durante le operazioni di esportazione, le modifiche a questi timestamp da sole non attivano l'esportazione automatica. Solo le modifiche al contenuto dei file o ad altri metadati (come la proprietà o le autorizzazioni) attiveranno un'esportazione automatica in S3.

Aggiornamento delle impostazioni di esportazione

Puoi configurare le impostazioni di esportazione di un file system su un bucket S3 collegato quando crei l'associazione del repository di dati. Per ulteriori informazioni, consulta Creazione di un link a un bucket S3.

Puoi anche aggiornare le impostazioni di esportazione in qualsiasi momento, inclusa la politica di esportazione. Per ulteriori informazioni, consulta Aggiornamento delle impostazioni di associazione agli archivi di dati.

Monitoraggio dell'esportazione automatica

Puoi monitorare le associazioni di repository di dati abilitate all'esportazione automatica utilizzando una serie di metriche pubblicate su Amazon. CloudWatch La `AgeOfOldestQueuedMessage` metrica rappresenta l'età dell'aggiornamento più vecchio apportato al file system che non è stato ancora esportato in S3. Se `AgeOfOldestQueuedMessage` è maggiore di zero per un periodo di tempo prolungato, consigliamo di ridurre temporaneamente il numero di modifiche (in particolare la ridenominazione delle directory) che vengono apportate attivamente al file system fino a ridurre la coda dei messaggi. Per ulteriori informazioni, consulta FSx per le metriche del repository Lustre S3.

> **Important**
>
> Quando si elimina un'associazione di archivio di dati o un file system con l'esportazione automatica abilitata, è innanzitutto necessario assicurarsi che `AgeOfOldestQueuedMessage` sia zero, ovvero che non vi siano modifiche non ancora

esportate. Se `AgeOfOldestQueuedMessage` è maggiore di zero quando elimini l'associazione al repository di dati o il file system, le modifiche che non erano ancora state esportate non raggiungeranno il bucket S3 collegato. Per evitare ciò, attendi che `AgeOfOldestQueuedMessage` raggiunga lo zero prima di eliminare l'associazione al repository di dati o il file system.

Utilizzo delle attività dell'archivio dati per esportare le modifiche

L'attività di esportazione del repository dei dati esporta i file nuovi o modificati nel file system. Crea un nuovo oggetto in S3 per ogni nuovo file sul file system. Per ogni file che è stato modificato sul file system o i cui metadati sono stati modificati, l'oggetto corrispondente in S3 viene sostituito con un nuovo oggetto con i nuovi dati e metadati. Non viene intrapresa alcuna azione per i file che sono stati eliminati dal file system.

> **Note**
>
> Tieni presente quanto segue quando utilizzi le attività di esportazione del repository di dati:
>
> - L'uso di caratteri jolly per includere o escludere file da esportare non è supportato.
> - Durante l'esecuzione `mv` delle operazioni, il file di destinazione dopo lo spostamento verrà esportato in S3 anche se non sono presenti UID, GID, autorizzazioni o modifiche al contenuto.

Utilizza le seguenti procedure per esportare le modifiche ai dati e ai metadati sul file system in bucket S3 collegati utilizzando la console Amazon FSx e la CLI. Tieni presente che puoi utilizzare un'attività di archivio dati per più attività. DRAs

Per esportare le modifiche (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione, scegli File system, quindi scegli il tuo Lustre file system.
3. Scegli la scheda Archivio dati.
4. Nel riquadro Associazioni tra archivi di dati, scegli l'associazione di archivi di dati per cui desideri creare l'attività di esportazione.

5. Per Azioni, scegli Esporta attività. Questa scelta non è disponibile se il file system non è collegato a un archivio di dati su S3. Viene visualizzata la finestra di dialogo Crea attività di esportazione dell'archivio dei dati.
6. (Facoltativo) Specificate fino a 32 cartelle o file da esportare dal vostro FSx file system Amazon fornendo i percorsi di tali directory o file in Percorsi del file system da esportare. I percorsi forniti devono essere relativi al punto di montaggio del file system. Se il punto di montaggio è `/mnt/fsx` ed `/mnt/fsx/path1` è una directory o un file sul file system che si desidera esportare, il percorso da fornire è`path1`.

   > **Note**
   >
   > Se un percorso fornito non è valido, l'operazione ha esito negativo.

7. (Facoltativo) Scegliete Abilita in Rapporto di completamento per generare un rapporto sul completamento dell'attività dopo il completamento dell'attività. Un rapporto sul completamento dell'attività fornisce dettagli sui file elaborati dall'attività che soddisfano l'ambito fornito in Ambito del rapporto. Per specificare la posizione in cui Amazon FSx deve recapitare il report, inserisci un percorso relativo nel repository di dati S3 collegato al file system per Report path.
8. Scegli Create (Crea).

   Una notifica nella parte superiore della pagina File system mostra l'attività che hai appena creato in corso.

Per visualizzare lo stato e i dettagli dell'attività, scorri verso il basso fino al riquadro Attività del data Repository nella scheda Data Repository per il file system. L'ordinamento predefinito mostra l'attività più recente nella parte superiore dell'elenco.

Per visualizzare un riepilogo dell'attività da questa pagina, scegli Task ID per l'attività appena creata. Viene visualizzata la pagina di riepilogo dell'attività.

Per esportare le modifiche (CLI)

- Utilizzate il comando `create-data-repository-task`CLI per esportare le modifiche ai dati e ai metadati sul file system FSx for Lustre. L'operazione API corrispondente è. `CreateDataRepositoryTask`

```
$ aws fsx create-data-repository-task \
    --file-system-id fs-0123456789abcdef0 \
```

```
    --type EXPORT_TO_REPOSITORY \
    --paths path1,path2/file1 \
    --report Enabled=true
```

Dopo aver creato correttamente l'attività di data repository, Amazon FSx restituisce la descrizione dell'attività come JSON, come mostrato nell'esempio seguente.

```
{
    "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"
    }
}
```

Dopo aver creato l'attività per esportare i dati nel repository di dati collegato, puoi verificare lo stato dell'attività di esportazione dell'archivio di dati. Per ulteriori informazioni sulla visualizzazione delle attività del data repository, vedere. Accesso alle attività del repository di dati

Esportazione di file utilizzando i comandi HSM

> **Note**
>
> Per esportare le modifiche ai dati e ai metadati del file system FSx for Lustre in un repository di dati durevole su Amazon S3, utilizza la funzionalità di esportazione automatica descritta in. Esporta automaticamente gli aggiornamenti nel tuo bucket S3 Puoi anche utilizzare le attività

di esportazione del repository di dati, descritte in. Utilizzo delle attività dell'archivio dati per esportare le modifiche

Per esportare un singolo file nel tuo repository di dati e verificare che il file sia stato esportato correttamente nel tuo repository di dati, puoi eseguire i comandi mostrati di seguito. Il valore restituito da `states: (0x00000009) exists archived` indica che il file è stato esportato correttamente.

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

> **Note**
>
> È necessario eseguire i comandi HSM (ad esempio`hsm_archive`) come utente root o utilizzando. `sudo`

Per esportare l'intero file system o un'intera directory del file system, eseguite i seguenti comandi. Se esporti più file contemporaneamente, Amazon FSx for Lustre esporta i file nel tuo repository di dati Amazon S3 in parallelo.

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

Per determinare se l'esportazione è stata completata, esegui il comando seguente.

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

Se il comando restituisce zero file rimanenti, l'esportazione è completa.

Attività di archiviazione dei dati

Utilizzando le attività di importazione ed esportazione dell'archivio di dati, puoi gestire il trasferimento di dati e metadati tra il file system FSx for Lustre e uno qualsiasi dei suoi repository di dati durevoli su Amazon S3.

Le attività di archiviazione dei dati ottimizzano i trasferimenti di dati e metadati tra il file system FSx for Lustre e un repository di dati su S3. Un modo per farlo è tenere traccia delle modifiche

tra il tuo FSx file system Amazon e il suo repository di dati collegato. Lo fanno anche utilizzando tecniche di trasferimento parallelo per trasferire dati a velocità fino a centinaia di GBps. Puoi creare e visualizzare attività di repository di dati utilizzando la FSx console Amazon AWS CLI, e l' FSx API Amazon.

Le attività di archiviazione dei dati mantengono i metadati POSIX (Portable Operating System Interface) del file system, inclusi proprietà, autorizzazioni e timestamp. Poiché le attività mantengono questi metadati, è possibile implementare e gestire i controlli di accesso tra il file system FSx for Lustre e i relativi repository di dati collegati.

Puoi utilizzare un'attività di repository dei dati di rilascio per liberare spazio nel file system per nuovi file rilasciando i file esportati in Amazon S3. Il contenuto del file rilasciato viene rimosso, ma i metadati del file rilasciato rimangono nel file system. Gli utenti e le applicazioni possono comunque accedere a un file rilasciato leggendo nuovamente il file. Quando l'utente o l'applicazione legge il file rilasciato, FSx for Lustre recupera in modo trasparente il contenuto del file da Amazon S3.

Tipi di attività di archiviazione dei dati

Esistono tre tipi di attività di archiviazione dei dati:

- Esporta le attività del repository di dati, esporta dal tuo Lustre file system a un bucket S3 collegato.
- Importa le attività del repository di dati: importa da un bucket S3 collegato al tuo file system. Lustre
- Le attività di release data repository rilasciano i file esportati in un bucket S3 collegato dal tuo file system. Lustre

Per ulteriori informazioni, consulta Creazione di un'attività di repository di dati.

Argomenti

- Comprendere lo stato e i dettagli di un'attività
- Utilizzo delle attività dell'archivio dati
- Utilizzo dei report sul completamento delle attività
- Risoluzione dei problemi relativi alle attività del data repository

Comprendere lo stato e i dettagli di un'attività

Un'attività di archivio dati contiene informazioni descrittive e uno stato del ciclo di vita.

Dopo aver creato un'attività, puoi visualizzare le seguenti informazioni dettagliate per un'attività di repository di dati utilizzando la FSx console Amazon, la CLI o l'API:

- Il tipo di attività:
  - `EXPORT_TO_REPOSITORY`indica un'attività di esportazione.
  - `IMPORT_METADATA_FROM_REPOSITORY`indica un'attività di importazione.
  - `RELEASE_DATA_FROM_FILESYSTEM`indica un'attività di rilascio.
- Il file system su cui è stata eseguita l'operazione.
- L'ora di creazione dell'attività.
- Lo stato dell'attività.
- Il numero totale di file elaborati dall'operazione.
- Il numero totale di file elaborati con successo dall'attività.
- Il numero totale di file che l'operazione non è riuscita a elaborare. Questo valore è maggiore di zero quando lo stato dell'attività è FALLITO. Informazioni dettagliate sui file che hanno avuto esito negativo sono disponibili in un rapporto sul completamento dell'attività. Per ulteriori informazioni, consulta Utilizzo dei report sul completamento delle attività.
- L'ora in cui è iniziata l'attività.
- L'ora dell'ultimo aggiornamento dello stato dell'attività. Lo stato dell'attività viene aggiornato ogni 30 secondi.

Un'attività di archivio dati può avere uno dei seguenti stati:

- PENDING indica che Amazon non FSx ha avviato l'attività.
- EXECUTING indica che Amazon FSx sta elaborando l'operazione.
- FAILED indica che Amazon FSx non ha elaborato correttamente l'operazione. Ad esempio, potrebbero esserci dei file che l'operazione non è riuscita a elaborare. I dettagli dell'attività forniscono ulteriori informazioni sull'errore. Per ulteriori informazioni sulle attività non riuscite, vedereRisoluzione dei problemi relativi alle attività del data repository.
- SUCCEEDED indica che Amazon FSx ha completato l'attività con successo.
- ANNULLATO indica che l'attività è stata annullata e non completata.
- ANNULLAMENTO indica che Amazon FSx sta annullando l'operazione.

Per ulteriori informazioni sull'accesso alle attività esistenti nell'archivio di dati, consulta. Accesso alle attività del repository di dati

Utilizzo delle attività dell'archivio dati

Nelle sezioni seguenti, è possibile trovare informazioni dettagliate sulla gestione delle attività del repository di dati. Puoi creare, duplicare, visualizzare i dettagli e annullare le attività del repository di dati utilizzando la FSx console Amazon, la CLI o l'API.

Argomenti

Creazione di un'attività di repository di dati

Puoi creare un'attività di repository di dati utilizzando la FSx console Amazon, la CLI o l'API. Dopo aver creato un'attività, puoi visualizzarne l'avanzamento e lo stato utilizzando la console, la CLI o l'API.

È possibile creare tre tipi di attività nell'archivio dati:

- L'attività Esporta archivio dati esporta dal Lustre file system in un bucket S3 collegato. Per ulteriori informazioni, consulta Utilizzo delle attività dell'archivio dati per esportare le modifiche.
- L'attività Importa archivio dati importa da un bucket S3 collegato al file system. Lustre Per ulteriori informazioni, consulta Utilizzo delle attività di archiviazione dei dati per importare le modifiche.
- L'attività Release data repository rilascia i file dal Lustre file system che sono stati esportati in un bucket S3 collegato. Per ulteriori informazioni, consulta Utilizzo delle attività di archiviazione dei dati per rilasciare file.

Duplicazione di un'attività

Puoi duplicare un'attività di repository di dati esistente nella console Amazon FSx . Quando si duplica un'attività, una copia esatta dell'operazione esistente viene visualizzata nella pagina Create import data repository o Create export data repository. È possibile apportare modifiche ai percorsi di esportazione o importazione, in base alle esigenze, prima di creare ed eseguire la nuova attività.

> **Note**
>
> Una richiesta di esecuzione di un'attività duplicata avrà esito negativo se una copia esatta di tale attività è già in esecuzione. Una copia esatta di un'operazione già in esecuzione contiene lo stesso percorso o gli stessi percorsi del file system nel caso di un'attività di esportazione o gli stessi percorsi dell'archivio dati nel caso di un'attività di importazione.

È possibile duplicare un'attività dalla visualizzazione dei dettagli dell'attività, dal riquadro Attività dell'archivio dati nella scheda Data Repository per il file system o dalla pagina Attività dell'archivio dati.

Per duplicare un'attività esistente

1. Scegli un'attività nel riquadro Attività dell'archivio dati nella scheda Archivio dati per il file system.
2. Scegli Duplica attività. A seconda del tipo di attività scelto, viene visualizzata la pagina Crea archivio dati di importazione o Crea archivio dati di esportazione. Tutte le impostazioni per la nuova attività sono identiche a quelle per l'attività che stai duplicando.
3. Modifica o aggiungi i percorsi da cui desideri importare o esportare.
4. Scegli Create (Crea).

Accesso alle attività del repository di dati

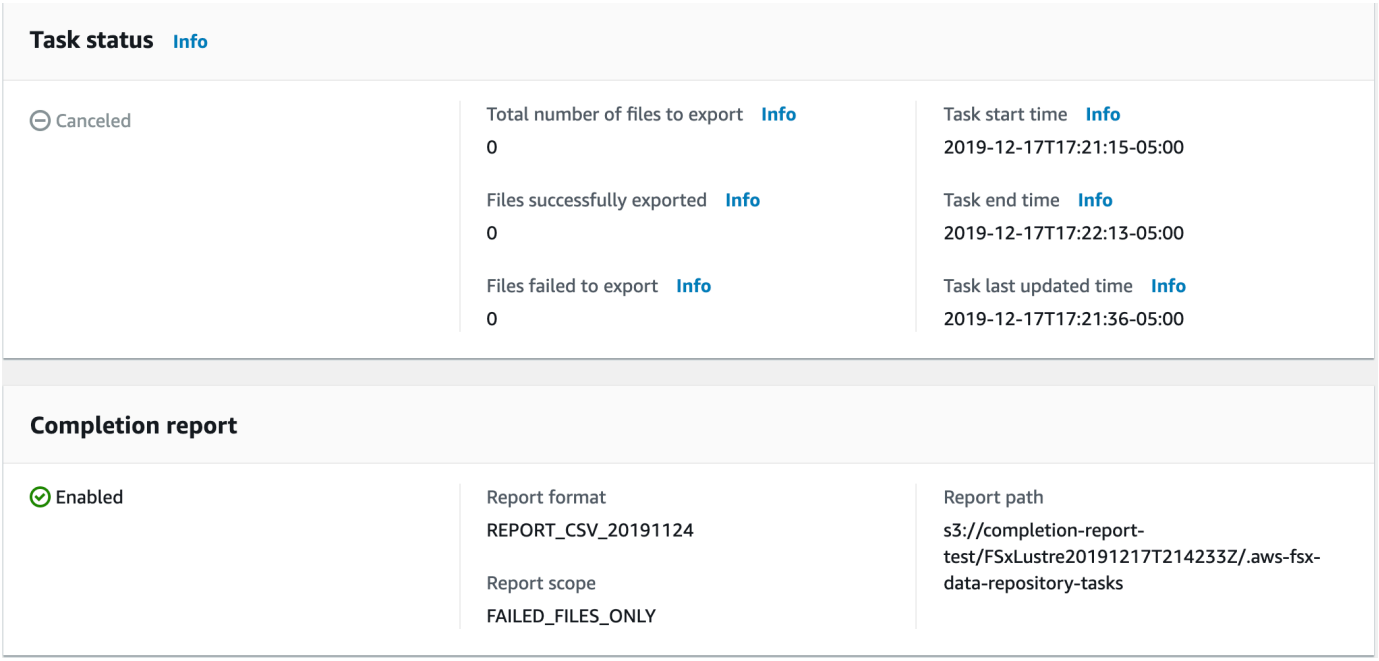
Dopo aver creato un'attività di archivio dati, puoi accedere all'attività e a tutte le attività esistenti nel tuo account utilizzando la FSx console Amazon, la CLI e l'API. Amazon FSx fornisce le seguenti informazioni dettagliate sulle attività:

- Tutte le attività esistenti.
- Tutte le attività relative a un file system specifico.
- Tutte le attività relative a una specifica associazione di archivi di dati.
- Tutte le attività con uno stato del ciclo di vita specifico. Per ulteriori informazioni sui valori dello stato del ciclo di vita delle attività, vedere. Comprendere lo stato e i dettagli di un'attività

Puoi accedere a tutte le attività di data repository esistenti nel tuo account utilizzando la FSx console Amazon, la CLI o l'API, come descritto di seguito.

Per visualizzare le attività e i dettagli delle attività nell'archivio di dati (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione, scegli il file system per cui desideri visualizzare le attività del data repository. Viene visualizzata la pagina dei dettagli del file system.
3. Nella pagina dei dettagli del file system, scegli la scheda Archivio dati. Tutte le attività per questo file system vengono visualizzate nel pannello Attività dell'archivio dati.
4. Per visualizzare i dettagli di un'attività, scegliete ID attività o Nome attività nel pannello Attività dell'archivio dati. Viene visualizzata la pagina dei dettagli dell'attività.



Per recuperare le attività dell'archivio di dati e i dettagli delle attività (CLI)

Utilizzando il comando Amazon FSx `describe-data-repository-tasks`CLI, puoi visualizzare tutte le attività del repository di dati e i relativi dettagli nel tuo account. `DescribeDataRepositoryTasks`è il comando API equivalente.

- Usa il comando seguente per visualizzare tutti gli oggetti dell'attività del data repository nel tuo account.

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

  Se il comando ha esito positivo, Amazon FSx restituisce la risposta in formato JSON.

```
{
    "DataRepositoryTasks": [
        {
            "Lifecycle": "EXECUTING",
            "Paths": [],
            "Report": {
                "Path":"s3://dataset-01/reports",
                "Format":"REPORT_CSV_20191124",
                "Enabled":true,
                "Scope":"FAILED_FILES_ONLY"
            },
            "StartTime": 1591863862.288,
            "EndTime": ,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef3",
            "Status": {
                "SucceededCount": 4255,
                "TotalCount": 4200,
                "FailedCount": 55,
                "LastUpdatedTime": 1571863875.289
            },
            "FileSystemId": "fs-0123456789a7",
            "CreationTime": 1571863850.075,
            "ResourceARN": "arn:aws:fsx:us-east-1:1234567890:task/
task-0123456789abcdef3"
        },
        {
            "Lifecycle": "FAILED",
            "Paths": [],
            "Report": {
                "Enabled": false,
            },
            "StartTime": 1571863862.288,
            "EndTime": 1571863905.292,
            "Type": "EXPORT_TO_REPOSITORY",
            "Tags": [],
            "TaskId": "task-0123456789abcdef1",
            "Status": {
                "SucceededCount": 1153,
                "TotalCount": 1156,
                "FailedCount": 3,
                "LastUpdatedTime": 1571863875.289
```

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


Visualizzazione delle attività per file system

Puoi visualizzare tutte le attività per un file system specifico utilizzando la FSx console Amazon, la CLI o l'API, come descritto di seguito.

Per visualizzare le attività per file system (console)

1. Scegli File system nel pannello di navigazione. Viene visualizzata la pagina File system.

2. Scegliete il file system per il quale desiderate visualizzare le attività del data repository. Viene visualizzata la pagina dei dettagli del file system.
3. Nella pagina dei dettagli del file system, scegli la scheda Archivio dati. Tutte le attività per questo file system vengono visualizzate nel pannello Attività dell'archivio dati.

Per recuperare le attività tramite file system (CLI)

- Utilizzare il comando seguente per visualizzare tutte le attività di archiviazione dei dati per il file system. `fs-0123456789abcdef0`

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

Se il comando ha esito positivo, Amazon FSx restituisce la risposta in formato JSON.

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

Annullamento di un'attività di archiviazione dati

È possibile annullare un'attività dell'archivio dati mentre si trova nello stato PENDING o EXECUTING. Quando si annulla un'attività, si verifica quanto segue:

- Amazon FSx non elabora i file in coda per l'elaborazione.
- Amazon FSx continua a elaborare tutti i file attualmente in corso.
- Amazon FSx non ripristina i file che l'attività ha già elaborato.

Per annullare un'attività di archiviazione dati (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Fai clic sul file system per il quale desideri annullare un'attività di archiviazione dei dati.

3. Apri la scheda Data Repository e scorri verso il basso per visualizzare il pannello Data Repository Tasks.
4. Scegliete ID attività o Nome attività per l'attività che desiderate annullare.
5. Scegli Annulla attività per annullare l'attività.
6. Inserisci l'ID dell'attività per confermare la richiesta di annullamento.

Per annullare un'attività di archiviazione dati (CLI)

Utilizza il comando Amazon FSx `cancel-data-repository-task`CLI per annullare un'attività. `CancelDataRepositoryTask`è il comando API equivalente.

- Utilizzare il comando seguente per annullare un'attività di archiviazione dati.

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

Se il comando ha esito positivo, Amazon FSx restituisce la risposta in formato JSON.

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

Utilizzo dei report sul completamento delle attività

Un rapporto sul completamento di un'attività fornisce dettagli sui risultati di un'attività di esportazione, importazione o rilascio di un archivio di dati. Il rapporto include i risultati dei file elaborati dall'attività che corrispondono all'ambito del rapporto. È possibile specificare se generare un rapporto per un'attività utilizzando il `Enabled` parametro.

Amazon FSx invia il report al repository di dati collegato del file system in Amazon S3, utilizzando il percorso specificato quando abiliti il report per un'attività. Il nome del file del report serve `report.csv` per le attività di importazione e `failures.csv` per le attività di esportazione o rilascio.

Il formato del report è un file con valori separati da virgole (CSV) che contiene tre campi:`FilePath`, e. `FileStatus` `ErrorCode`

I report vengono codificati utilizzando la codifica in formato RFC-4180 come segue:

- I percorsi che iniziano con uno dei seguenti caratteri sono contenuti tra virgolette singole: `@ + - =`
- Le stringhe che contengono almeno uno dei seguenti caratteri sono contenute tra virgolette doppie: `" ,`
- A tutte le virgolette doppie viene aggiunta una virgoletta doppia aggiuntiva.

Di seguito sono riportati alcuni esempi di codifica dei report:

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

Per ulteriori informazioni sulla codifica RFC-4180, vedere RFC-4180 - Common Format and MIME Type for Comma-Separated Values (CSV) sul sito Web IETF.

Di seguito è riportato un esempio delle informazioni fornite in un rapporto di completamento delle attività che include solo i file non riusciti.

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

Per ulteriori informazioni sugli errori delle attività e su come risolverli, vedereRisoluzione dei problemi relativi alle attività del data repository.

Risoluzione dei problemi relativi alle attività del data repository

Puoi attivare la registrazione in CloudWatch Logs per registrare le informazioni su eventuali errori riscontrati durante l'importazione o l'esportazione di file utilizzando le attività del repository di dati. Per informazioni sui registri degli eventi di Logs, vedere CloudWatch . Registri degli eventi del data repository

Quando un'attività di data repository non riesce, puoi trovare il numero di file che Amazon FSx non è riuscito a elaborare in File non riusciti a esportare nella pagina di stato dell'attività della console. Oppure puoi utilizzare la CLI o l'API e visualizzare la proprietà dell'`Status: FailedCount`attività. Per informazioni sull'accesso a queste informazioni, consultaAccesso alle attività del repository di dati.

Per le attività di archiviazione dei dati, Amazon fornisce FSx anche facoltativamente informazioni su file e directory specifici che non sono stati compilati in un rapporto di completamento. Il report sul completamento dell'attività contiene il percorso del file o della directory sul Lustre file system in cui si è verificato l'errore, lo stato e il motivo dell'errore. Per ulteriori informazioni, consulta Utilizzo dei report sul completamento delle attività.

Un'operazione di archiviazione dei dati può fallire per diversi motivi, inclusi quelli elencati di seguito.

Codice di errore	Spiegazione
`FileSizeTooLarge`	La dimensione massima dell'oggetto supportata da Amazon S3 è di 5 TiB.
`InternalError`	Si è verificato un errore nel FSx file system di Amazon per un'attività di importazione, esportazione o rilascio. In genere, questo codice di errore indica che il FSx file system Amazon su cui è stata eseguita l'operazi one non riuscita si trova in uno stato del ciclo di vita FAILED. In questo caso, i file interessati potrebbero non essere recuperab ili a causa della perdita di dati. Altrimenti, puoi utilizzare i comandi HSM (Hierarchical Storage Management) per esportare i file e le directory nel repository di dati su S3. Per ulteriori informazioni, consulta Esportazione di file utilizzando i comandi HSM.
`OperationNotPermitted`	Amazon FSxnon è riuscito a rilasciare il file perché non è stato esportato in un bucket S3 collegato. È necessario utilizzare le attività automatiche di esportazione o esportazione dell'archivio di dati per garantire che i file vengano prima esportati nel bucket Amazon S3 collegato.

Codice di errore	Spiegazione
`PathSizeTooLong`	Il percorso di esportazione è troppo lungo. La lunghezza massima della chiave dell'oggetto supportata da S3 è di 1.024 caratteri.
`ResourceBusy`	Amazon FSxnon è riuscito a esportare o rilasciare il file perché un altro client del file system vi stava accedendo. È possibile riprovare DataRepositoryTask dopo che il flusso di lavoro ha terminato la scrittura sul file.

Codice di errore	Spiegazione
`S3AccessDenied`	L'accesso ad Amazon S3 è stato negato per un'attività di esportazione o importazione di un repository di dati. Per le attività di esportazione, il FSx file system Amazon deve disporre dell'autorizzazione per eseguire l'`S3:PutObject` operazione di esportazione in un repository di dati collegato su S3. Questa autorizzazione viene concessa nel ruolo collegato al `AWSServiceRoleForFSxS3Access_` *`fs-0123456789abcdef0`* servizio. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx. Per le attività di esportazione, poiché l'attività di esportazione richiede che i dati fluiscano all'esterno del VPC di un file system, questo errore può verificarsi se il repository di destinazione ha una policy bucket che contiene una delle chiavi di condizione globali `aws:SourceVpc` o `aws:SourceVpce` IAM. Per le attività di importazione, il FSx file system Amazon deve disporre dell'autorizzazione per eseguire le `S3:GetObject` operazioni `S3:HeadObject` e importare da un repository di dati collegato su S3. Per le attività di importazione, se il bucket S3 utilizza la crittografia lato server con chiavi gestite dal cliente archiviate in AWS Key Management Service (SSE-KMS), è necessario seguire le configurazioni delle policy riportate in. Utilizzo di bucket Amazon S3 crittografati lato server

Codice di errore	Spiegazione
	Se il tuo bucket S3 contiene oggetti caricati da un account bucket S3 Account AWS diverso da quello collegato al file system, puoi assicurarti che le attività di repository dei dati possano modificare i metadati S3 o sovrascrivere gli oggetti S3 indipendentemente dall'account che li ha caricati. Ti consigliamo di abilitare la funzionalità S3 Object Ownership per il tuo bucket S3. Questa funzionalità ti consente di assumere la proprietà di nuovi oggetti che altri Account AWS caricano nel tuo bucket, forzando i caricamenti a fornire l'ACL predefinito. `-/-acl bucket-owner-full-control` Puoi abilitare S3 Object Ownership scegliendo l'opzione preferita del proprietario del bucket nel tuo bucket S3. Per ulteriori informazioni, consulta Controllare la proprietà degli oggetti caricati utilizzando S3 Object Ownership nella Amazon S3 User Guide.
`S3Error`	Amazon FSx ha riscontrato un errore relativo a S3 che non lo era. `S3AccessDenied`
`S3FileDeleted`	Amazon non FSx è riuscito a esportare un file hard link perché il file sorgente non esiste nell'archivio dati.

Codice di errore	Spiegazione
`S3ObjectInUnsupportedTier`	Amazon FSx ha importato con successo un oggetto non symlink da una classe di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Sarà `succeeded with warning` incluso nel rapporto sul completamento dell'atti vità. `FileStatus` L'avviso indica che per recuperare i dati, è necessario ripristinare prima l'oggetto S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive e quindi utilizzare un comando per importare l'oggetto. `hsm_resto re`
`S3ObjectNotFound`	Amazon non FSx è riuscito a importare o esportare il file perché non esiste nell'archivio dati.
`S3ObjectPathNotPosixCompliant`	L'oggetto Amazon S3 esiste ma non può essere importato perché non è un oggetto conforme a POSIX. Per informazioni sui metadati POSIX supportati, consulta. Supporto per metadati POSIX per archivi di dati
`S3ObjectUpdateInProgressFro mFileRename`	Amazon FSxnon è riuscito a rilasciare il file perché l'esportazione automatica sta elaborand o una ridenominazione del file. Il processo di ridenominazione automatica dell'esportazione deve essere completato prima che il file possa essere rilasciato.

Codice di errore	Spiegazione
`S3SymlinkInUnsupportedTier`	Amazon non FSx è riuscito a importare un oggetto symlink perché si trova in una classe di storage Amazon S3 non supportata, ad esempio una classe di storage S3 Glacier Flexible Retrieval o S3 Glacier Deep Archive. Sarà incluso nel rapporto sul completamento dell'attività. `FileStatus failed`
`SourceObjectDeletedBeforeReleasing`	Amazon non FSx è stato in grado di rilasciare il file dal file system perché il file è stato eliminato dall'archivio dati prima che potesse essere rilasciato.

Rilascio di file

Le attività di rilascio del data repository rilasciano i dati dei file dal file system FSx for Lustre per liberare spazio per nuovi file. Il rilascio di un file mantiene l'elenco dei file e i metadati, ma rimuove la copia locale del contenuto del file. Se un utente o un'applicazione accede a un file rilasciato, i dati vengono caricati automaticamente e in modo trasparente sul file system dal bucket Amazon S3 collegato.

> **Note**
>
> Le attività relative al repository dei dati di rilascio non sono disponibili sui file system Lustre FSx 2.10.

I parametri Percorsi di rilascio del file system e Durata minima dall'ultimo accesso determinano quali file verranno rilasciati.

- Percorsi del file system da rilasciare: specifica il percorso da cui verranno rilasciati i file.
- Durata minima dall'ultimo accesso: specifica la durata, in giorni, di modo che tutti i file a cui non si accede durante tale periodo debbano essere rilasciati. La durata dall'ultimo accesso a un file viene calcolata prendendo la differenza tra l'ora di creazione dell'attività di rilascio e l'ultima volta in cui è stato effettuato l'accesso a un file (valore massimo di `atimemtime`, `ectime`).

I file verranno rilasciati lungo il percorso del file solo se sono stati esportati in S3 e hanno una durata dall'ultimo accesso superiore al valore minimo di durata dall'ultimo accesso. Fornendo una durata minima dall'ultimo accesso di `0` giorni, i file verranno rilasciati indipendentemente dalla loro durata dall'ultimo accesso.

> **Note**
>
> L'uso di caratteri jolly per includere o escludere file da rilasciare non è supportato.

Le attività del repository di dati di rilascio rilasceranno solo i dati dai file che sono già stati esportati in un repository di dati S3 collegato. Puoi esportare i dati in S3 utilizzando la funzione di esportazione automatica, un'attività di esportazione del repository di dati o i comandi HSM. Per verificare che un file sia stato esportato nel tuo repository di dati, puoi eseguire il seguente comando. Il valore restituito da `states: (0x00000009) exists archived` indica che il file è stato esportato correttamente.

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

> **Note**
>
> È necessario eseguire il comando HSM come utente root o utilizzando. `sudo`

Per rilasciare i dati dei file a intervalli regolari, puoi pianificare un'attività di repository di dati di rilascio ricorrente utilizzando Amazon Scheduler. EventBridge Per ulteriori informazioni, consulta la sezione Guida introduttiva a EventBridge Scheduler nella Amazon EventBridge Scheduler User Guide.

Argomenti

- Utilizzo delle attività di archiviazione dei dati per rilasciare file

Utilizzo delle attività di archiviazione dei dati per rilasciare file

Utilizza le seguenti procedure per creare attività che rilasciano file dal file system utilizzando la FSx console Amazon e la CLI. Il rilascio di un file mantiene l'elenco dei file e i metadati, ma rimuove la copia locale del contenuto del file.

Per rilasciare file (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli File system, quindi scegli il tuo Lustre file system.
3. Scegli la scheda Archivio dati.
4. Nel riquadro Associazioni tra archivi di dati, scegli l'associazione di repository di dati per cui desideri creare l'attività di rilascio.
5. Per Azioni, scegli Crea attività di rilascio. Questa scelta è disponibile solo se il file system è collegato a un archivio di dati su S3. Viene visualizzata la finestra di dialogo Create release data repository task.
6. In Percorsi del file system da rilasciare, specifica fino a 32 directory o file da rilasciare dal tuo FSx file system Amazon fornendo i percorsi di tali directory o file. I percorsi che fornisci devono essere relativi al punto di montaggio del file system. Ad esempio, se il punto di montaggio `/mnt/fsx/path1` è `/mnt/fsx` ed è un file sul file system che si desidera rilasciare, il percorso da fornire è`path1`. Per rilasciare tutti i file del file system, specificate una barra (/) come percorso.

   > **Note**
   >
   > Se un percorso fornito non è valido, l'operazione ha esito negativo.

7. Per la durata minima dall'ultimo accesso, specifica la durata, in giorni, in modo che tutti i file a cui non si accede durante tale periodo debbano essere rilasciati. L'ora dell'ultimo accesso viene calcolata utilizzando il valore massimo di `atimemtime`, `ectime`. I file con un periodo di durata dell'ultimo accesso superiore alla durata minima dall'ultimo accesso (relativa all'ora di creazione dell'attività) verranno rilasciati. I file con un periodo di durata dell'ultimo accesso inferiore a questo numero di giorni non verranno rilasciati, anche se si trovano nel campo Percorsi di rilascio del file system. Fornisci una durata di `0` giorni per il rilascio dei file indipendentemente dalla durata dell'ultimo accesso.
8. (Facoltativo) In Rapporto di completamento, scegli Abilita per generare un rapporto sul completamento delle attività che fornisca dettagli sui file che soddisfano l'ambito fornito nell'ambito fornito nell'ambito del rapporto. Per specificare una posizione in FSx cui Amazon deve recapitare il report, inserisci un percorso relativo nel repository di dati S3 collegato al file system per Report path.
9. Scegli l'attività Crea archivio dati.

Una notifica nella parte superiore della pagina File system mostra l'attività appena creata in corso.

Per visualizzare lo stato e i dettagli dell'attività, nella scheda Data Repository, scorri verso il basso fino a Data Repository Tasks. L'ordinamento predefinito mostra l'attività più recente nella parte superiore dell'elenco.

Per visualizzare un riepilogo dell'attività da questa pagina, scegli Task ID per l'attività appena creata.

Per rilasciare file (CLI)

- Utilizzate il comando `create-data-repository-task`CLI per creare un'attività che rilasci file sul file system FSx for Lustre. L'operazione API corrispondente è. `CreateDataRepositoryTask`

  Imposta i seguenti parametri:

  - `--file-system-id`Imposta l'ID del file system da cui stai rilasciando i file.
  - Imposta `--paths` i percorsi sul file system da cui verranno rilasciati i dati. Se viene specificata una directory, i file all'interno della directory vengono rilasciati. Se viene specificato un percorso di file, viene rilasciato solo quel file. Per rilasciare tutti i file del file system che sono stati esportati in un bucket S3 collegato, specifica una barra (/) per il percorso.
  - Imposta `--type` su `RELEASE_DATA_FROM_FILESYSTEM`.
  - Imposta le opzioni come segue`--release-configuration` `DurationSinceLastAccess`:
    - `Unit`: impostato su `DAYS`.
    - `Value`— Specificate un numero intero che rappresenti la durata, espressa in giorni, in modo che tutti i file a cui non si accede durante tale periodo debbano essere rilasciati. I file a cui è stato effettuato l'accesso durante un periodo inferiore a questo numero di giorni non verranno rilasciati, anche se sono inclusi nel `--paths` parametro. Fornisci una durata di `0` giorni per il rilascio dei file indipendentemente dalla durata dell'ultimo accesso.

  Questo comando di esempio specifica che i file che sono stati esportati in un bucket S3 collegato e soddisfano i `--release-configuration` criteri verranno rilasciati dalle directory nei percorsi specificati.

```
$ 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
```

Dopo aver creato correttamente l'attività di archiviazione dei dati, Amazon FSx restituisce la descrizione dell'attività come JSON.

Dopo aver creato l'attività per rilasciare i file, puoi controllare lo stato dell'attività. Per ulteriori informazioni sulla visualizzazione delle attività del repository di dati, vedereAccesso alle attività del repository di dati.

Usare Amazon FSx con i tuoi dati locali

Puoi utilizzare Lustre FSx per elaborare i tuoi dati locali con istanze di elaborazione in-cloud. FSx for Lustre supporta l'accesso tramite AWS Direct Connect e la VPN, che consentono di montare i file system da client locali.

Da utilizzare FSx per Lustre con i dati locali

1. Creare un file system. Per ulteriori informazioni, consulta l'Passaggio 1: crea il tuo FSx file system for Lustreesercizio introduttivo.
2. Installa il file system dai client locali. Per ulteriori informazioni, consulta Montaggio di FSx file system Amazon da un ambiente locale o da un Amazon VPC peer-to-peer.
3. Copia i dati che desideri elaborare nel file system FSx for Lustre.
4. Esegui il tuo carico di lavoro ad alta intensità di calcolo su EC2 istanze Amazon nel cloud montando il tuo file system.
5. Al termine, copia i risultati finali dal file system nella posizione dei dati locale ed elimina il file system for Lustre. FSx

Registri degli eventi del data repository

Puoi attivare la registrazione su CloudWatch Logs per registrare le informazioni su eventuali errori riscontrati durante l'importazione o l'esportazione di file utilizzando le attività di importazione automatica, esportazione automatica e archiviazione dei dati. Per ulteriori informazioni, consulta Registrazione con Amazon CloudWatch Logs.

> **Note**
>
> Quando un'attività di data repository fallisce, Amazon scrive FSx anche le informazioni sull'errore nel report di completamento dell'attività. Per ulteriori informazioni sulle informazioni sugli errori nei report di completamento, consultaRisoluzione dei problemi relativi alle attività del data repository.

Le attività automatiche di importazione, esportazione automatica e archivio dati possono avere esito negativo per diversi motivi, inclusi quelli elencati di seguito. Per informazioni sulla visualizzazione di questi registri, vedere. Visualizzazione dei registri

Importazione di eventi

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ImportListObjectError`	ERROR	Impossibile elencare gli oggetti S3 nel bucket *`bucket_name`* S3 con prefisso. *`prefix`*	Amazon FSx non è riuscito a elencare gli oggetti S3 nel bucket S3. Questo può accadere se la policy del bucket S3 non fornisce autorizzazioni	N/D

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
			sufficienti ad Amazon. FSx	
`S3ImportUnsupportedTierWarning`	WARN	Impossibile importare un oggetto S3 con chiave *`key_value`* nel bucket S3 a *`bucket_name`* causa di un oggetto S3 in un livello non supportato. *`S3_tier_name`*	Amazon non FSx è riuscito a importare un oggetto S3 perché si trova in una classe di storage Amazon S3 non supportata, come la classe di storage S3 Glacier Flexible Retrieval o la classe di storage S3 Glacier Deep Archive.	`S3ObjectInUnsupportedTier`

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ImportSymlinkInUnsupportedTierWarning`	WARN	Impossibile importare un oggetto S3 con chiave *`key_value`* nel bucket S3 a causa di un oggetto S3 symlink in un livello non supportato. *`bucket_name S3_tier_name`*	Amazon non FSx è riuscito a importare un oggetto symlink perché si trova in una classe di storage Amazon S3 non supportata, come la classe di storage S3 Glacier Flexible Retrieval o la classe di storage S3 Glacier Deep Archive.	`S3SymlinkInUnsupportedTier`

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ImportAccessDenied`	ERROR	Impossibile importare l'oggetto S3 con chiave *`key_value`* nel bucket S3 perché l'accesso all'oggetto S3 è stato negato. *`bucket_name`*	L'accesso è stato negato ad Amazon S3 per un'attività di importazione di esportazione di un repository di dati. Per le attività di importazione, il FSx file system Amazon deve disporre dell'autorizzazione per eseguire le `s3:GetObject` operazioni `s3:HeadObject` e importare da un repository di dati collegato su S3. Per le attività di importazione, se il bucket S3 utilizza la crittografia	`S3AccessDenied`

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
			lato server con chiavi gestite dal cliente archiviate in AWS Key Management Service (SSE-KMS), è necessario seguire le configurazioni delle policy riportate in. Utilizzo di bucket Amazon S3 crittografati lato server	
`S3ImportDeleteAccessDenied`	ERROR	Impossibile eliminare il file locale per l'oggetto S3 con chiave *`key_value`* nel bucket S3 perché l'accesso all'oggetto S3 è stato negato. *`bucket_name`*	All'importazione automatica è stato negato l'accesso a un oggetto S3.	N/D

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ImportObjectPathNotPosixCompliant`	ERROR	Impossibile importare l'oggetto S3 con la chiave *`key_value`* nel bucket S3 *`bucket_name`* perché l'oggetto S3 non è conforme a POSIX.	L'oggetto Amazon S3 esiste ma non può essere importato perché non è un oggetto conforme a POSIX. Per informazioni sui metadati POSIX supportati, consulta. Supporto per metadati POSIX per archivi di dati	`S3ObjectPathNotPosixCompliant`

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ImportObjectTypeMismatch`	ERROR	Impossibile importare l'oggetto S3 con la chiave *`key_value`* nel bucket S3 *`bucket_name`* perché un oggetto S3 con lo stesso nome è già stato importato nel file system.	L'oggetto S3 da importare è di un tipo diverso (file o directory) rispetto a un oggetto esistente con lo stesso nome nel file system.	`S3ObjectTypeMismatch`
`S3ImportDirectoryMetadataUpdateError`	ERROR	Impossibile aggiornare i metadati della directory locale a causa di un errore interno.	Impossibile importare i metadati delle directory a causa di un errore interno.	N/D
`S3ImportObjectDeleted`	ERROR	Impossibile importare l'oggetto S3 con la chiave *`key_value`* perché non è stato trovato nel bucket S3. *`bucket_name`*	Amazon non FSx è stato in grado di importare i metadati dei file perché l'oggetto corrispondente non esiste nel repository di dati.	`S3FileDeleted`

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ImportBucketDoesNotExist`	ERROR	Impossibile importare l'oggetto S3 con la chiave *`key_value`* nel bucket S3 *`bucket_name`* perché il bucket non esiste.	Amazon FSx non può importare automaticamente un oggetto S3 nel file system perché il bucket S3 non esiste più.	N/D
`S3ImportDeleteBucketDoesNotExist`	ERROR	Impossibile eliminare il file locale per l'oggetto S3 con chiave *`key_value`* nel bucket S3 *`bucket_name`* perché il bucket non esiste.	Amazon FSx non può eliminare un file collegato a un oggetto S3 sul file system perché il bucket S3 non esiste più.	N/D

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ImportDirectoryCreateError`	ERROR	Impossibile creare la directory locale a causa di un errore interno.	Amazon FSx non è riuscito a importare automaticamente la creazione di una directory sul file system a causa di un errore interno.	N/D
`NoDiskSpace`	ERROR	Impossibile importare l'oggetto S3 con la chiave *`key_value`* nel bucket S3 *`bucket_name`* perché il file system è pieno.	Il file system ha esaurito lo spazio su disco sui server di metadati durante la creazione del file o della directory.	N/D

Esporta eventi

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ExportInternalError`	ERRORE	Impossibile esportare l'oggetto S3 con la chiave	L'oggetto non è stato esportato a causa di un errore interno.	`INTERNAL_ERROR`

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
		key_value nel bucket S3 a *bucket_name* causa di un errore interno.		

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ExportAccessDenied`	ERRORE	Impossibile esportare il file perché è stato negato l'accesso all'oggetto S3 con chiave *`key_value`* nel bucket S3. *`bucket_name`*	L'accesso ad Amazon S3 è stato negato per un'attività di esportazione di un repository di dati. Per le attività di esportazione, il FSx file system Amazon deve disporre dell'autorizzazione per eseguire l'`s3:PutObject` operazione di esportazione in un repository di dati collegato su S3. Questa autorizzazione viene concessa nel ruolo collegato al `AWSServiceRoleForFSxS3Access_` *`fs-0123456789abcdef0`* servizio. Per ulteriori informazioni,	`S3AccessDenied`

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
			consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx. Poiché l'attività di esportazione richiede che i dati fluiscano all'esterno del VPC di un file system, questo errore può verificarsi se il repository di destinazione ha una policy bucket che contiene una delle chiavi di condizione globali `aws:SourceVpc` o `aws:SourceVpce` IAM. Se il tuo bucket S3 contiene oggetti caricati da un account bucket S3 Account AWS	

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
			diverso da quello collegato al file system, puoi assicurarti che le attività del repository di dati possano modificare i metadati S3 o sovrascri vere gli oggetti S3 indipende ntemente dall'account che li ha caricati. Ti consiglia mo di abilitare la funzional ità S3 Object Ownership per il tuo bucket S3. Questa funzional ità ti consente di assumere la proprietà di nuovi oggetti che altri Account AWS caricano nel tuo bucket, forzando i caricamenti a fornire l'ACL predefinito. `--acl bucket-`	

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
			`owner-full-control` Puoi abilitare S3 Object Ownership scegliendo l'opzione preferita del proprietario del bucket nel tuo bucket S3. Per ulteriori informazioni, consulta Controllare la proprietà degli oggetti caricati utilizzando S3 Object Ownership nella Amazon S3 User Guide.	
`S3ExportPathSizeTooLong`	ERRORE	Impossibile esportare il file perché la dimensione del percorso del file locale supera la lunghezza massima della chiave dell'oggetto supportata da S3.	Il percorso di esportazione è troppo lungo. La lunghezza massima della chiave dell'oggetto supportata da S3 è di 1.024 caratteri.	`PathSizeTooLong`

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ExportFileSizeTooLarge`	ERRORE	Impossibile esportare il file perché la dimensione del file supera la dimensione massima supportata degli oggetti S3.	La dimensione massima dell'oggetto supportata da Amazon S3 è di 5 TiB.	`FileSizeTooLarge`
`S3ExportKMSKeyNotFound`	ERRORE	Impossibile esportare il file per l'oggetto S3 con chiave *`key_value`* nel bucket S3 *`bucket_name`* perché la chiave KMS del bucket non è stata trovata.	Amazon non FSx è riuscito a esportare il file perché AWS KMS key non è stato trovato. Assicurati di utilizzare una chiave che sia Regione AWS uguale a quella del bucket S3. Per ulteriori informazioni sulla creazione di chiavi KMS, consulta Creating keys nella Developer Guide. AWS Key Management Service	`N/A`

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ExportResourceBusy`	ERRORE	Impossibile esportare il file perché è utilizzato da un altro processo.	Amazon non FSx è stato in grado di esportare il file perché era stato modificato da un altro client sul file system. Puoi riprovare l'operazione dopo che il flusso di lavoro ha terminato la scrittura sul file.	`ResourceBusy`
`S3ExportLocalObjectReleaseWithoutS3Source`	WARN	Esportazione ignorata: il file locale è in stato di rilascio e un oggetto S3 collegato con chiave non *`key_value`* è stato trovato nel bucket. *`bucket_name`*	Amazon non FSx è stato in grado di esportare il file perché era in uno stato rilasciato sul file system.	N/D

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3ExportLocalObjectNotMatchDra`	WARN	Esportazione ignorata: il file locale non appartiene a un percorso del file system collegato a un archivio di dati.	Amazon non FSx è riuscito a esportare perché l'oggetto non appartiene a un percorso del file system collegato a un repository di dati.	N/D
`InternalAutoExportError`	ERRORE	L'esportazione automatica ha rilevato un errore interno durante l'esportazione di un oggetto del file system	L'esportazione non è riuscita a causa di un errore interno (esportazione automatica o a livello di lustre).	N/D
`S3CompletionReportUploadFailure`	ERRORE	Impossibile caricare il rapporto di completamento delle attività del repository di dati in *`bucket_name`*	Amazon non FSx è stato in grado di caricare il rapporto di completamento.	N/D

Codice di errore	Livello di log	Messaggio di registro	Causa principale	Codice di errore nel rapporto di completamento
`S3CompletionReportValidateFailure`	ERRORE	Impossibile caricare il report di completamento delle attività dell'archivio dati nel bucket *`bucket_name`* perché il percorso del report di completamento *`report_path`* non appartiene a un archivio di dati associato a questo file system	Amazon non FSx è stato in grado di caricare il report di completamento perché il percorso S3 fornito dal cliente non appartiene a un repository di dati collegato.	N/D

Utilizzo di tipi di distribuzione precedenti

Questa sezione si applica ai file system con tipo di distribuzione Scratch 1 e anche ai file system con `Scratch 2` o tipi di `Persistent 1` distribuzione che non utilizzano associazioni di repository di dati. Tieni presente che l'esportazione automatica e il supporto per più archivi di dati non sono disponibili sui FSx file system Lustre che non utilizzano associazioni di repository di dati.

Argomenti

- Collega il tuo file system a un bucket Amazon S3
- Importa automaticamente gli aggiornamenti dal tuo bucket S3

Collega il tuo file system a un bucket Amazon S3

Quando crei un file system Amazon FSx for Lustre, puoi collegarlo a un repository di dati durevole in Amazon S3. Prima di creare il file system, assicurati di aver già creato il bucket Amazon S3 a cui ti stai collegando. Nella procedura guidata per la creazione del file system, si impostano le seguenti proprietà di configurazione del repository di dati nel riquadro opzionale Import/Export dell'archivio dati.

- Scegli in che modo Amazon FSx mantiene aggiornato il tuo elenco di file e directory man mano che aggiungi o modifichi oggetti nel tuo bucket S3 dopo la creazione del file system. Per ulteriori informazioni, consulta Importa automaticamente gli aggiornamenti dal tuo bucket S3.
- Bucket di importazione: inserisci il nome del bucket S3 che stai utilizzando per il repository collegato.
- Prefisso di importazione: inserisci un prefisso di importazione opzionale se desideri importare nel tuo file system solo alcuni elenchi di file e directory di dati nel tuo bucket S3. Il prefisso di importazione definisce da dove importare i dati nel bucket S3.
- Prefisso di esportazione: definisce dove Amazon FSx esporta il contenuto del tuo file system nel bucket S3 collegato.

Puoi creare una mappatura 1:1 in cui Amazon FSx esporta i dati dal tuo file system FSx for Lustre nelle stesse directory del bucket S3 da cui sono stati importati. Per avere una mappatura 1:1, specifica un percorso di esportazione verso il bucket S3 senza prefissi quando crei il file system.

- Quando crei un file system utilizzando la console, scegli l'opzione Esporta prefisso > Un prefisso che specifichi e mantieni vuoto il campo del prefisso.
- Quando crei un file system utilizzando la AWS CLI o l'API, specifica il percorso di esportazione come nome del bucket S3 senza prefissi aggiuntivi, ad esempio. `ExportPath=s3://amzn-s3-demo-bucket/`

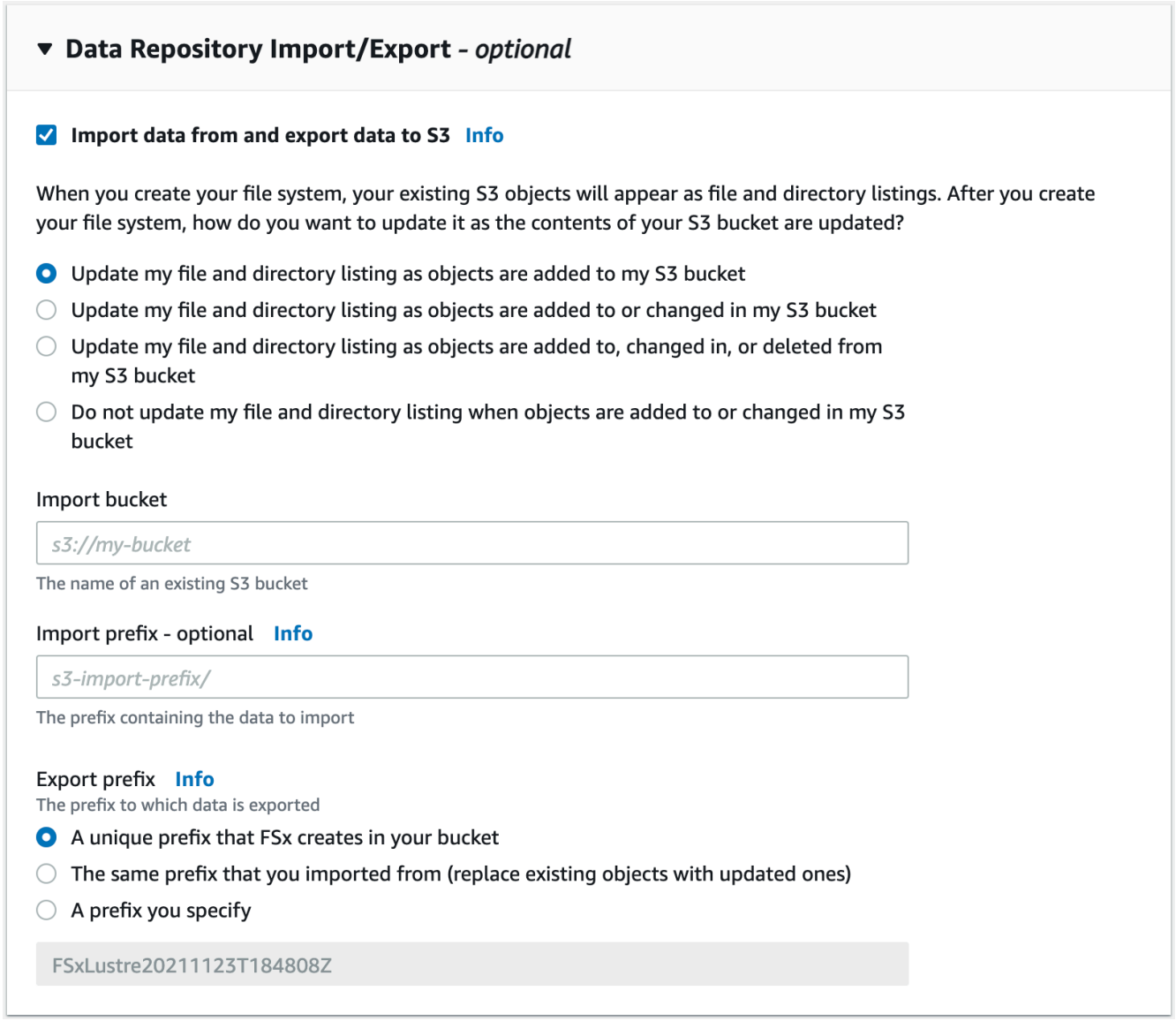
Utilizzando questo metodo, puoi includere un prefisso di importazione quando specifichi il percorso di importazione e ciò non influisce sulla mappatura 1:1 per le esportazioni.

Creazione di file system collegati a un bucket S3

Le seguenti procedure illustrano il processo di creazione di un FSx file system Amazon collegato a un bucket S3 utilizzando la console di AWS gestione e l'interfaccia a riga di AWS comando (CLI AWS).

Console

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard, scegli Crea file system.
3. Per il tipo di file system, scegliete FSx Lustre, quindi scegliete Avanti.
4. Fornite le informazioni richieste per le sezioni Dettagli del file system e Rete e sicurezza. Per ulteriori informazioni, consulta Passaggio 1: crea il tuo FSx file system for Lustre.
5. Utilizza il pannello di importazione/esportazione del repository di dati per configurare un repository di dati collegato in Amazon S3. Seleziona Importa dati da ed esporta dati su S3 per espandere la sezione Import/Export dell'archivio dati e configurare le impostazioni dell'archivio di dati.



6. Scegli in che modo Amazon FSx mantiene aggiornato il tuo elenco di file e directory man mano che aggiungi o modifichi oggetti nel tuo bucket S3. Quando crei il file system, gli oggetti S3 esistenti vengono visualizzati come elenchi di file e directory.

   - Aggiorna il mio elenco di file e directory man mano che gli oggetti vengono aggiunti al mio bucket S3: (impostazione predefinita) Amazon aggiorna FSx automaticamente gli elenchi di file e directory di tutti i nuovi oggetti aggiunti al bucket S3 collegato che non esistono attualmente nel file system. FSx Amazon FSx non aggiorna gli elenchi di oggetti che sono stati modificati nel bucket S3. Amazon FSx non elimina gli elenchi di oggetti eliminati nel bucket S3.

     > **Note**
     >
     > L'impostazione predefinita delle preferenze di importazione per l'importazione di dati da un bucket S3 collegato utilizzando la CLI e l'API è. `NONE` L'impostazione predefinita delle preferenze di importazione quando si utilizza la console è l'aggiornamento Lustre man mano che vengono aggiunti nuovi oggetti al bucket S3.

   - Aggiorna il mio elenco di file e directory man mano che gli oggetti vengono aggiunti o modificati nel mio bucket S3: Amazon aggiorna FSx automaticamente gli elenchi di file e directory di tutti i nuovi oggetti aggiunti al bucket S3 e di tutti gli oggetti esistenti che vengono modificati nel bucket S3 dopo aver scelto questa opzione. Amazon FSx non elimina gli elenchi di oggetti eliminati nel bucket S3.
   - Aggiorna il mio elenco di file e directory man mano che gli oggetti vengono aggiunti, modificati o eliminati dal mio bucket S3: Amazon aggiorna FSx automaticamente gli elenchi di file e directory di tutti i nuovi oggetti aggiunti al bucket S3, di tutti gli oggetti esistenti che vengono modificati nel bucket S3 e di tutti gli oggetti esistenti che vengono eliminati nel bucket S3 dopo aver scelto questa opzione.
   - Non aggiornare il mio file e la mia lista direttamente quando gli oggetti vengono aggiunti, modificati o eliminati dal mio bucket S3: Amazon aggiorna gli elenchi di file e directory dal bucket S3 collegato FSx solo quando viene creato il file system. FSx non aggiorna gli elenchi di file e directory per oggetti nuovi, modificati o eliminati dopo aver scelto questa opzione.

7. Inserisci un prefisso di importazione opzionale se desideri importare solo alcuni degli elenchi di file e directory dei dati nel tuo bucket S3 nel tuo file system. Il prefisso di importazione definisce da dove importare i dati nel bucket S3. Per ulteriori informazioni, consulta Importa automaticamente gli aggiornamenti dal tuo bucket S3.

8. Scegli una delle opzioni di prefisso di esportazione disponibili:

   - Un prefisso unico che Amazon FSx crea nel tuo bucket: scegli questa opzione per esportare oggetti nuovi e modificati utilizzando un prefisso generato da FSx for Lustre. Il prefisso è simile al seguente:. `/FSxLustre`*`file-system-creation- timestamp`* Il timestamp è in formato UTC, ad esempio `FSxLustre20181105T222312Z`.
   - Lo stesso prefisso da cui hai importato (sostituisci gli oggetti esistenti con quelli aggiornati): Scegli questa opzione per sostituire gli oggetti esistenti con quelli aggiornati.
   - Un prefisso specificato: scegliete questa opzione per conservare i dati importati ed esportare oggetti nuovi e modificati utilizzando un prefisso specificato dall'utente. Per ottenere una mappatura 1:1 durante l'esportazione dei dati nel bucket S3, scegli questa opzione e lascia vuoto il campo del prefisso. FSx esporterà i dati nelle stesse directory da cui sono stati importati.
9. (Facoltativo) Imposta le preferenze di manutenzione o utilizza le impostazioni predefinite del sistema.
10. Scegliete Avanti e controllate le impostazioni del file system. Apportate eventuali modifiche, se necessario.
11. Scegliere Create file system (Crea file system).

AWS CLI

L'esempio seguente crea un FSx file system Amazon collegato a`amzn-s3-demo-bucket`, con una preferenza di importazione che importa tutti i file nuovi, modificati ed eliminati nel repository di dati collegato dopo la creazione del file system.

> **Note**
>
> L'impostazione delle preferenze di importazione predefinita per l'importazione di dati da un bucket S3 collegato utilizzando la CLI e l'API è`NONE`, che è diversa dal comportamento predefinito quando si utilizza la console.

Per creare un file system FSx for Lustre, usa il `create-file-system`comando Amazon FSx CLI, come illustrato di seguito. L'operazione API corrispondente è. `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
```

Dopo aver creato correttamente il file system, Amazon FSx restituisce la descrizione del file system come JSON, come mostrato nell'esempio seguente.

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

Visualizzazione del percorso di esportazione di un file system

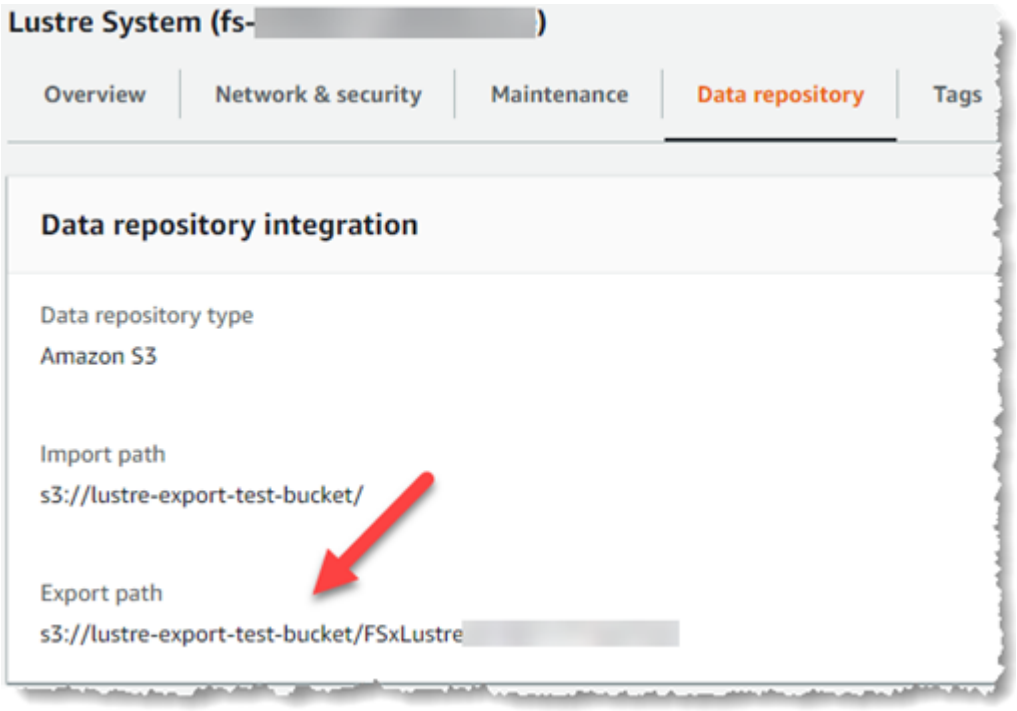
È possibile visualizzare il percorso di esportazione di un file system utilizzando la console FSx for Lustre, la AWS CLI e l'API.

Console

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/
2. Scegli il nome del file system o l'ID del file system FSx for Lustre per il quale desideri visualizzare il percorso di esportazione.

   Viene visualizzata la pagina dei dettagli del file system per quel file system.
3. Scegli la scheda Archivio dati.

   Viene visualizzato il pannello di integrazione dell'archivio dati, che mostra i percorsi di importazione ed esportazione.



CLI

Per determinare il percorso di esportazione per il file system, utilizzate il comando [describe-file-systems](#) AWS CLI.

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

Cerca la `ExportPath` proprietà sotto `LustreConfiguration` nella risposta.

```
{
    "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"
}
```

Stato del ciclo di vita del repository di dati

Lo stato del ciclo di vita del data repository fornisce informazioni sullo stato del repository di dati collegato al file system. Un repository di dati può avere i seguenti stati del ciclo di vita.

- Creazione: Amazon FSx sta creando la configurazione del repository di dati tra il file system e il repository di dati collegato. L'archivio di dati non è disponibile.
- Disponibile: l'archivio di dati è disponibile per l'uso.
- Aggiornamento: la configurazione dell'archivio dati è in fase di aggiornamento avviato dal cliente che potrebbe influire sulla sua disponibilità.
- Configurato erroneamente: Amazon FSx non può importare automaticamente gli aggiornamenti dal bucket S3 finché la configurazione del repository di dati non viene corretta. Per ulteriori informazioni, consulta Risoluzione dei problemi relativi a un bucket S3 collegato non correttamente configurato.

Puoi visualizzare lo stato del ciclo di vita del repository di dati collegato di un file system utilizzando la FSx console Amazon, l'interfaccia a riga di AWS comando e l'API Amazon. FSx Nella FSx

console Amazon, puoi accedere allo stato del ciclo di vita del repository di dati nel riquadro Data Repository Integration della scheda Data Repository per il file system. La `Lifecycle` proprietà si trova nell'`DataRepositoryConfiguration`oggetto nella risposta di un comando `describe-file-systems`CLI (l'azione API equivalente è `DescribeFileSystems`).

Importa automaticamente gli aggiornamenti dal tuo bucket S3

Per impostazione predefinita, quando crei un nuovo file system, Amazon FSx importa i metadati dei file (nome, proprietà, timestamp e autorizzazioni) degli oggetti nel bucket S3 collegato al momento della creazione del file system. Puoi configurare il file system FSx for Lustre per importare automaticamente i metadati degli oggetti aggiunti, modificati o eliminati dal bucket S3 dopo la creazione del file system. FSx for Lustre aggiorna l'elenco di file e directory di un oggetto modificato dopo la creazione nello stesso modo in cui importa i metadati dei file durante la creazione del file system. Quando Amazon FSx aggiorna l'elenco di file e directory di un oggetto modificato, se l'oggetto modificato nel bucket S3 non contiene più i relativi metadati, Amazon FSx mantiene i valori correnti dei metadati del file, anziché utilizzare le autorizzazioni predefinite.

> **Note**
>
> Le impostazioni di importazione sono disponibili FSx per i file system Lustre creati dopo le 15:00 EDT del 23 luglio 2020.

È possibile impostare le preferenze di importazione quando si crea un nuovo file system e aggiornare le impostazioni sui file system esistenti utilizzando la console di FSx gestione, la AWS CLI e l' AWS API. Quando crei il file system, gli oggetti S3 esistenti vengono visualizzati come elenchi di file e directory. Dopo aver creato il file system, come vuoi aggiornarlo man mano che i contenuti del tuo bucket S3 vengono aggiornati? Un file system può avere una delle seguenti preferenze di importazione:

> **Note**
>
> Il file system FSx for Lustre e il bucket S3 collegato devono trovarsi nella stessa AWS regione per importare automaticamente gli aggiornamenti.

- Aggiorna il mio elenco di file e directory man mano che gli oggetti vengono aggiunti al mio bucket S3: (impostazione predefinita) Amazon aggiorna FSx automaticamente gli elenchi di file e directory

di tutti i nuovi oggetti aggiunti al bucket S3 collegato che non esistono attualmente nel file system. FSx Amazon FSx non aggiorna gli elenchi di oggetti che sono stati modificati nel bucket S3. Amazon FSx non elimina gli elenchi di oggetti eliminati nel bucket S3.

> **Note**
>
> L'impostazione predefinita delle preferenze di importazione per l'importazione di dati da un bucket S3 collegato utilizzando la CLI e l'API è. `NONE` L'impostazione predefinita delle preferenze di importazione quando si utilizza la console è l'aggiornamento Lustre man mano che vengono aggiunti nuovi oggetti al bucket S3.

- Aggiorna il mio elenco di file e directory man mano che gli oggetti vengono aggiunti o modificati nel mio bucket S3: Amazon aggiorna FSx automaticamente gli elenchi di file e directory di tutti i nuovi oggetti aggiunti al bucket S3 e di tutti gli oggetti esistenti che vengono modificati nel bucket S3 dopo aver scelto questa opzione. Amazon FSx non elimina gli elenchi di oggetti eliminati nel bucket S3.
- Aggiorna il mio elenco di file e directory man mano che gli oggetti vengono aggiunti, modificati o eliminati dal mio bucket S3: Amazon aggiorna FSx automaticamente gli elenchi di file e directory di tutti i nuovi oggetti aggiunti al bucket S3, di tutti gli oggetti esistenti che vengono modificati nel bucket S3 e di tutti gli oggetti esistenti che vengono eliminati nel bucket S3 dopo aver scelto questa opzione.
- Non aggiornare il mio file e la mia lista direttamente quando gli oggetti vengono aggiunti, modificati o eliminati dal mio bucket S3: Amazon aggiorna gli elenchi di file e directory dal bucket S3 collegato FSx solo quando viene creato il file system. FSx non aggiorna gli elenchi di file e directory per oggetti nuovi, modificati o eliminati dopo aver scelto questa opzione.

Quando imposti le preferenze di importazione per aggiornare gli elenchi dei file system e delle directory in base alle modifiche nel bucket S3 collegato, Amazon FSx crea una configurazione di notifica degli eventi sul bucket S3 collegato denominato. `FSx` Non modificare o eliminare la configurazione di notifica degli `FSx` eventi sul bucket S3: in questo modo si evita l'importazione automatica di elenchi di file e directory nuovi o modificati nel file system.

Quando Amazon FSx aggiorna un elenco di file che è stato modificato nel bucket S3 collegato, sovrascrive il file locale con la versione aggiornata, anche se il file è bloccato in scrittura. Allo stesso modo, quando Amazon FSx aggiorna un elenco di file quando l'oggetto corrispondente è stato eliminato dal bucket S3 collegato, elimina il file locale, anche se il file è bloccato in scrittura.

Amazon FSx fa del suo meglio per aggiornare il file system. Amazon FSx non può aggiornare il file system apportando modifiche nelle seguenti situazioni:

- Quando Amazon FSx non dispone dell'autorizzazione per aprire l'oggetto S3 nuovo o modificato.
- Quando la configurazione di notifica `FSx` degli eventi sul bucket S3 collegato viene eliminata o modificata.

Entrambe queste condizioni causano una configurazione errata dello stato del ciclo di vita del repository di dati. Per ulteriori informazioni, consulta Stato del ciclo di vita del repository di dati.

Prerequisiti

Le seguenti condizioni sono necessarie per consentire FSx ad Amazon di importare automaticamente file nuovi, modificati o eliminati dal bucket S3 collegato:

- Il file system e il bucket S3 collegato devono trovarsi nella stessa regione. AWS
- Il bucket S3 non ha uno stato del ciclo di vita configurato in modo errato. Per ulteriori informazioni, consulta Stato del ciclo di vita del repository di dati.
- Il tuo account deve disporre delle autorizzazioni necessarie per configurare e ricevere notifiche di eventi sul bucket S3 collegato.

Tipi di modifiche ai file supportati

Amazon FSx supporta l'importazione delle seguenti modifiche a file e cartelle che si verificano nel bucket S3 collegato:

- Modifiche al contenuto dei file
- Modifiche ai metadati di file o cartelle
- Modifiche alla destinazione o ai metadati del collegamento simbolico

Aggiornamento delle preferenze di importazione

È possibile impostare le preferenze di importazione di un file system quando si crea un nuovo file system. Per ulteriori informazioni, consulta Collegamento del file system a un bucket Amazon S3.

Puoi anche aggiornare le preferenze di importazione di un file system dopo averlo creato utilizzando la Console di AWS gestione, la AWS CLI e l' FSx API Amazon, come illustrato nella procedura seguente.

Console

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard, scegli File system.
3. Seleziona il file system che desideri gestire per visualizzare i dettagli del file system.
4. Scegli Archivio dati per visualizzare le impostazioni dell'archivio dati. È possibile modificare le preferenze di importazione se lo stato del ciclo di vita è DISPONIBILE o NON È CONFIGURATO CORRETTAMENTE. Per ulteriori informazioni, consulta Stato del ciclo di vita del repository di dati.
5. Scegliete Azioni, quindi scegliete Aggiorna preferenze di importazione per visualizzare la finestra di dialogo Aggiorna preferenze di importazione.
6. Selezionate la nuova impostazione, quindi scegliete Aggiorna per apportare la modifica.

CLI

Per aggiornare le preferenze di importazione, utilizzate il `update-file-system`comando CLI. L'operazione API corrispondente è `UpdateFileSystem`.

Dopo aver aggiornato correttamente il file system`AutoImportPolicy`, Amazon FSx restituisce la descrizione del file system aggiornato come JSON, come mostrato di seguito:

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

Prestazioni FSx di Amazon for Lustre

Questo capitolo fornisce argomenti sulle prestazioni di Amazon FSx for Lustre, inclusi alcuni importanti suggerimenti e raccomandazioni per massimizzare le prestazioni del file system.

Argomenti

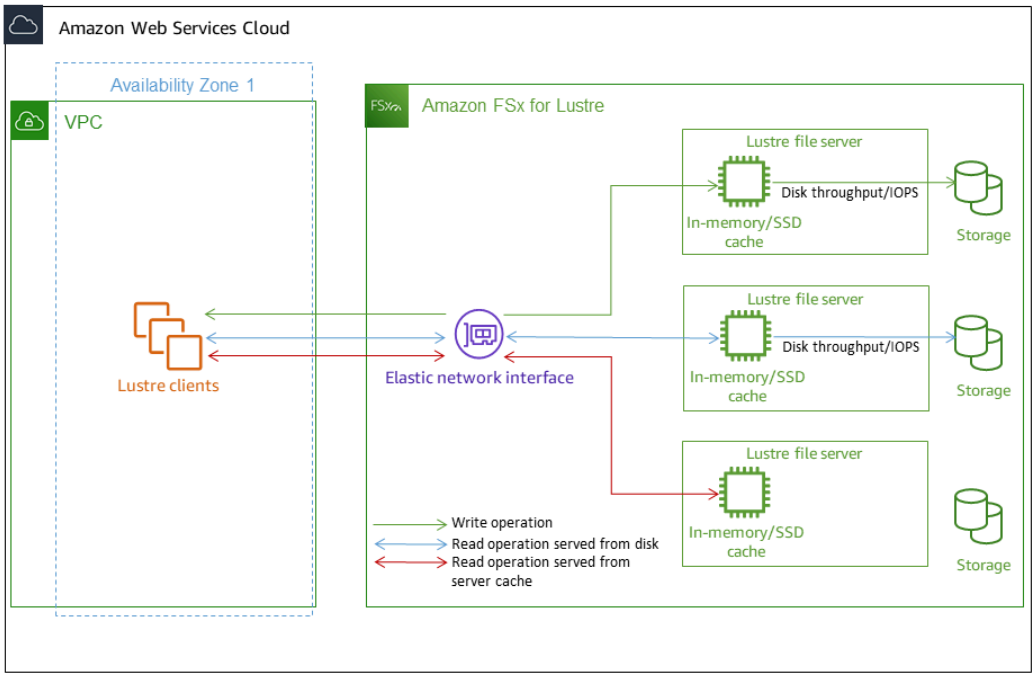
Panoramica

Amazon FSx for Lustre, basato sul popolare file system ad alte prestazioniLustre, offre prestazioni di scalabilità orizzontale che aumentano linearmente con le dimensioni di un file system. Lustrei file system si scalano orizzontalmente su più file server e dischi. Questa scalabilità offre a ciascun client l'accesso diretto ai dati archiviati su ciascun disco per eliminare molti dei colli di bottiglia presenti nei file system tradizionali. Amazon FSx for Lustre si basa sull'architettura Lustre scalabile per supportare alti livelli di prestazioni su un gran numero di client.

Come funzionano i file FSx system di For Lustre

Ogni file system FSx for Lustre è costituito dai file server con cui i client comunicano e da un set di dischi collegati a ciascun file server in cui sono archiviati i dati. Ogni file server utilizza una cache veloce in memoria per migliorare le prestazioni dei dati a cui si accede più frequentemente. A seconda della classe di archiviazione, è possibile dotare il file server di una cache di lettura SSD opzionale. Quando un client accede ai dati archiviati nella cache in memoria o SSD, il file server non ha bisogno di leggerli dal disco, il che riduce la latenza e aumenta la quantità totale di throughput

che è possibile gestire. Il diagramma seguente illustra i percorsi di un'operazione di scrittura, un'operazione di lettura eseguita dal disco e un'operazione di lettura eseguita dalla cache in memoria o SSD.



Quando si leggono i dati archiviati nella cache in memoria o SSD del file server, le prestazioni del file system sono determinate dalla velocità di trasmissione della rete. Quando si scrivono dati sul file system o quando si leggono dati che non sono archiviati nella cache in memoria, le prestazioni del file system sono determinate dalla riduzione del throughput di rete e del disco.

Per ulteriori informazioni sulla velocità effettiva di rete, sulla velocità effettiva su disco e sulle caratteristiche IOPS delle classi di storage SSD e HDD, consulta e. Caratteristiche prestazionali delle classi di storage SSD e HDD Caratteristiche prestazionali della classe di storage Intelligent-Tiering

Prestazioni dei metadati del file system

Le operazioni di I/O al secondo (IOPS) dei metadati del file system determinano il numero di file e directory che è possibile creare, elencare, leggere ed eliminare al secondo.

I file system Persistent 2 consentono di effettuare il provisioning dei metadati (IOPS) indipendentemente dalla capacità di storage e offrono una maggiore visibilità sul numero e sul tipo

di metadati che le istanze client IOPS generano sul file system. Con i file system SSD, il provisioning degli IOPS dei metadati viene eseguito automaticamente in base alla capacità di storage fornita. La modalità automatica non è supportata sui file system Intelligent-Tiering.

FSx Per i file system Lustre Persistent 2, il numero di IOPS di metadati forniti e il tipo di operazione sui metadati determinano la frequenza delle operazioni sui metadati che il file system è in grado di supportare. Il livello di IOPS di metadati fornito determina il numero di IOPS assegnati per i dischi di metadati del file system.

Tipo di operazione	Operazioni che è possibile eseguire al secondo per ogni IOPS di metadati fornito
Creazione, apertura e chiusura di file	2
Eliminazione di file	1
Creazione e ridenominazione della cartella	0.1
Eliminazione della directory	0.2

Per i file system SSD, puoi scegliere di effettuare il provisioning degli IOPS dei metadati utilizzando la modalità automatica. In modalità Automatica, Amazon effettua FSx automaticamente il provisioning degli IOPS dei metadati in base alla capacità di storage del file system in base alla tabella seguente:

Capacità di storage del file system	Metadati IOPS inclusi in modalità automatica
1200 GiB	1500
2400 GiB	3000
4800—9600 GiB	6000
12000—45600 GiB	12000
≥48000 GiB	12000 IOPS per 24000 GiB

In modalità User-provisioned, puoi facoltativamente scegliere di specificare il numero di IOPS di metadati da fornire. I valori validi sono:

- Per i file system SSD, i valori validi sono`1500`,, `3000` `600012000`, e multipli fino a un massimo di. `12000` `192000`
- Per i file system Intelligent-Tiering, i valori validi sono e. `6000` `12000`

Per informazioni su come configurare Metadata IOPS, vedere. Gestione delle prestazioni dei metadati Tieni presente che paghi per gli IOPS dei metadati assegnati al di sopra del numero predefinito di IOPS di metadati per il tuo file system.

Throughput verso le singole istanze del client

Se stai creando un file system con oltre il 10% GBps della capacità di throughput, ti consigliamo di abilitare Elastic Fabric Adapter (EFA) per ottimizzare il throughput per istanza client. Per ottimizzare ulteriormente il throughput per istanza client, i file system abilitati per EFA supportano anche GPUDirect lo storage per le istanze client basate su GPU NVIDIA abilitate per EFA e ENA Express per le istanze client abilitate per ENA Express.

Il throughput che è possibile trasferire a una singola istanza client dipende dalla scelta del tipo di file system e dall'interfaccia di rete dell'istanza client.

Tipo di file system	Interfaccia di rete dell'istanza client	Velocità effettiva massima per client, Gbps
Non abilitato per EFA	Qualsiasi	100 Gbps*
Compatibile con EFA	ENA	100 Gbps*
Compatibile con EFA	ENA Express	100 Gb/s
Abilitato all'EFA	EFA	700 Gbps
Compatibile con EFA	EFA con GDS	1200 Gbps

> **Note**
>
> * Il traffico tra una singola istanza client e un singolo server di storage FSx di oggetti Lustre è limitato a 5 Gbps. Fate riferimento al Indirizzi IP per file system numero di server di storage di oggetti su cui si basa il file system FSx for Lustre.

Layout di storage del file system

Tutti i dati dei file in Lustre ingresso vengono archiviati in volumi di storage denominati object storage targets (OSTs). Tutti i metadati dei file (inclusi nomi di file, timestamp, autorizzazioni e altro) vengono archiviati in volumi di archiviazione denominati metadata target (). MDTs I file system di Amazon FSx for Lustre sono composti da uno o più MDTs file. OSTs Amazon FSx for Lustre distribuisce i dati dei file su tutti gli elementi OSTs che compongono il file system per bilanciare la capacità di storage con la velocità effettiva e il carico IOPS.

Per visualizzare l'utilizzo dello storage dell'MDT e degli elementi OSTs che costituiscono il file system, esegui il comando seguente da un client su cui è montato il file system.

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

L'output di questo comando è simile al seguente.

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 dei dati nel file system

È possibile ottimizzare le prestazioni di throughput del file system con lo striping dei file. Amazon FSx for Lustre distribuisce automaticamente i file per garantire che i dati vengano serviti da tutti i server di storage. OSTs Puoi applicare lo stesso concetto a livello di file configurando la modalità di suddivisione dei file su più file. OSTs

Lo striping significa che i file possono essere suddivisi in più blocchi che vengono poi archiviati in diversi. OSTs Quando un file viene suddiviso su più file OSTs, le richieste di lettura o scrittura al file vengono distribuite tra queste OSTs, aumentando il throughput aggregato o gli IOPS che le applicazioni possono gestire.

Di seguito sono riportati i layout predefiniti per i file system Amazon FSx for Lustre.

- Per i file system creati prima del 18 dicembre 2020, il layout predefinito specifica un numero di strisce pari a 1. Ciò significa che, a meno che non venga specificato un layout diverso, ogni file creato in Amazon FSx for Lustre utilizzando strumenti Linux standard viene archiviato su un singolo disco.
- Per i file system creati dopo il 18 dicembre 2020, il layout predefinito è un layout di file progressivo in cui i file di dimensioni inferiori a 1 GiB vengono archiviati in un'unica striscia e ai file più grandi viene assegnato un numero di strisce pari a 5.
- Per i file system creati dopo il 25 agosto 2023, il layout predefinito è un layout di file progressivo a 4 componenti, come spiegato in. Layout di file progressivi
- Per tutti i file system, indipendentemente dalla data di creazione, i file importati da Amazon S3 non utilizzano il layout predefinito, ma utilizzano invece il layout nel parametro del `ImportedFileChunkSize` file system. I file importati da S3 più grandi di quelli `ImportedFileChunkSize` verranno archiviati su più file OSTs con un numero di strisce pari a. `(FileSize / ImportedFileChunksize) + 1` Il valore predefinito di è 1GiB`ImportedFileChunkSize`.

È possibile visualizzare la configurazione del layout di un file o di una directory utilizzando il `lfs getstripe` comando.

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

Questo comando riporta il numero di strisce, la dimensione e l'offset delle strisce di un file. Il numero di strisce è il numero di strisce su cui è suddiviso OSTs il file. La dimensione dello stripe indica la quantità di dati continui archiviati su un OST. Lo stripe offset è l'indice del primo OST su cui è distribuito il file.

Modifica della configurazione dello striping

I parametri di layout di un file vengono impostati quando il file viene creato per la prima volta. Utilizzate il `lfs setstripe` comando per creare un nuovo file vuoto con un layout specificato.

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

Il `lfs setstripe` comando influisce solo sul layout di un nuovo file. Utilizzatelo per specificare il layout di un file prima di crearlo. Puoi anche definire un layout per una directory. Una volta impostato su una directory, tale layout viene applicato a ogni nuovo file aggiunto a quella directory, ma non

ai file esistenti. Ogni nuova sottodirectory creata eredita anche il nuovo layout, che viene quindi applicato a qualsiasi nuovo file o directory creato all'interno di quella sottodirectory.

Per modificare il layout di un file esistente, utilizzate il comando. `lfs migrate` Questo comando copia il file secondo necessità per distribuirne il contenuto in base al layout specificato nel comando. Ad esempio, i file che vengono aggiunti o le cui dimensioni sono aumentate non modificano il numero di strisce, quindi è necessario migrarli per modificare il layout del file. In alternativa, è possibile creare un nuovo file utilizzando il `lfs setstripe` comando per specificarne il layout, copiare il contenuto originale nel nuovo file e quindi rinominare il nuovo file per sostituire il file originale.

In alcuni casi la configurazione di layout predefinita non è ottimale per il carico di lavoro. Ad esempio, un file system con decine OSTs e un gran numero di file da più gigabyte può ottenere prestazioni migliori suddividendo i file su un numero di stripe superiore al valore predefinito di cinque. OSTs La creazione di file di grandi dimensioni con un basso numero di righe può causare problemi di I/O prestazioni e può anche causare problemi di riempimento. OSTs In questo caso, puoi creare una directory con un numero maggiore di strisce per questi file.

La configurazione di un layout a strisce per file di grandi dimensioni (in particolare file di dimensioni superiori a un gigabyte) è importante per i seguenti motivi:

- Migliora la velocità effettiva consentendo a più server OSTs e ai relativi server di contribuire con IOPS, larghezza di banda di rete e risorse della CPU durante la lettura e la scrittura di file di grandi dimensioni.
- Riduce la probabilità che un piccolo sottoinsieme di sistemi OSTs diventi un punto critico che limita le prestazioni complessive del carico di lavoro.
- Impedisce che un singolo file di grandi dimensioni riempia un OST, causando possibili errori di riempimento del disco.

Non esiste un'unica configurazione di layout ottimale per tutti i casi d'uso. Per una guida dettagliata sui layout dei file, consulta Managing File Layout (Striping) and Free Space nella documentazione di Lustre.org. Le seguenti sono linee guida generali:

- Il layout a strisce è particolarmente importante per i file di grandi dimensioni, specialmente per i casi d'uso in cui i file hanno normalmente dimensioni di centinaia di megabyte o più. Per questo motivo, il layout predefinito per un nuovo file system assegna un numero di strisce pari a cinque per i file di dimensioni superiori a 1 GiB.
- Il numero di strisce è il parametro di layout da regolare per i sistemi che supportano file di grandi dimensioni. Il numero di strisce specifica il numero di volumi OST che conterranno porzioni di un

file a strisce. Ad esempio, con un numero di strisce pari a 2 e una dimensione di banda di 1 MiB, Lustre scrive blocchi di file da 1 MiB alternativi su ciascuno di due. OSTs

- Il numero effettivo di strisce è il minore tra il numero effettivo di volumi OST e il valore di conteggio delle strisce specificato. È possibile utilizzare lo speciale valore di conteggio delle strisce `-1` per indicare che le strisce devono essere posizionate su tutti i volumi OST.
- L'impostazione di un numero elevato di strisce per file di piccole dimensioni non è ottimale perché per determinate operazioni è Lustre necessaria una connessione di rete a tutte le OST del layout, anche se il file è troppo piccolo per occupare spazio su tutti i volumi OST.
- È possibile impostare un layout progressivo dei file (PFL) che consenta di modificare il layout di un file in base alle dimensioni. Una configurazione PFL può semplificare la gestione di un file system con una combinazione di file grandi e piccoli senza dover impostare esplicitamente una configurazione per ogni file. Per ulteriori informazioni, consulta Layout di file progressivi.
- La dimensione predefinita di Stripe è 1 MiB. L'impostazione di un offset a strisce può essere utile in circostanze particolari, ma in generale è meglio non specificarlo e utilizzare l'impostazione predefinita.

Layout di file progressivi

È possibile specificare una configurazione PFL (Progressive File Layout) per una directory per specificare diverse configurazioni di stripe per file di piccole e grandi dimensioni prima di popolarla. Ad esempio, è possibile impostare un PFL nella directory di primo livello prima che i dati vengano scritti su un nuovo file system.

Per specificare una configurazione PFL, utilizzate il `lfs setstripe` comando con `-E` opzioni per specificare i componenti di layout per file di dimensioni diverse, come il comando seguente:

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

Questo comando imposta quattro componenti di layout:

- Il primo componente (`-E 100M -c 1`) indica un valore di conteggio delle strisce pari a 1 per file di dimensioni fino a 100 MiB.
- Il secondo componente (`-E 10G -c 8`) indica un numero di strisce pari a 8 per file di dimensioni fino a 10 GiB.
- Il terzo componente (`-E 100G -c 16`) indica un numero di strisce pari a 16 per file di dimensioni fino a 100 GiB.

- Il quarto componente (`-E -1 -c 32`) indica un numero di strisce pari a 32 per file di dimensioni superiori a 100 GiB.

> **Important**
>
> L'aggiunta di dati a un file creato con un layout PFL popolerà tutti i relativi componenti di layout. Ad esempio, con il comando a 4 componenti mostrato sopra, se create un file da 1 MiB e poi aggiungete dati alla fine del file, il layout del file si espanderà fino ad avere un numero di strisce pari a -1, vale a dire tutto il sistema. OSTs Ciò non significa che i dati verranno scritti su ogni OST, ma un'operazione come la lettura della lunghezza del file invierà una richiesta in parallelo a ogni OST, aggiungendo un carico di rete significativo al file system.
>
> Pertanto, fate attenzione a limitare il numero di strisce per qualsiasi file di piccola o media lunghezza a cui successivamente possono essere aggiunti dati. Poiché i file di log di solito crescono con l'aggiunta di nuovi record, Amazon FSx for Lustre assegna un numero di strisce predefinito pari a 1 a qualsiasi file creato in modalità di aggiunta, indipendentemente dalla configurazione di stripe predefinita specificata dalla directory principale.

La configurazione PFL predefinita sui file system Amazon FSx for Lustre creata dopo il 25 agosto 2023 viene impostata con questo comando:

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

I clienti con carichi di lavoro che hanno un accesso altamente simultaneo a file di medie e grandi dimensioni trarranno probabilmente vantaggio da un layout con più strisce OSTs per dimensioni più piccole e striping su tutti i file più grandi, come mostrato nel layout di esempio a quattro componenti.

Monitoraggio delle prestazioni e dell'utilizzo

Ogni minuto, Amazon FSx for Lustre invia ad Amazon i parametri di utilizzo per ogni disco (MDT e OST). CloudWatch

Per visualizzare i dettagli aggregati sull'utilizzo del file system, puoi consultare la statistica Sum di ogni metrica. Ad esempio, la somma delle `DataReadBytes` statistiche riporta la velocità di lettura totale registrata da tutti gli utenti di un file system. OSTs Analogamente, la somma delle

`FreeDataStorageCapacity` statistiche riporta la capacità di archiviazione totale disponibile per i dati dei file nel file system.

Per ulteriori informazioni sul monitoraggio delle prestazioni del file system, vedereMonitoraggio dei file system Amazon FSx for Lustre.

Caratteristiche prestazionali delle classi di storage SSD e HDD

Il throughput supportato da un file system FSx for Lustre dotato di classe di archiviazione SSD o HDD è proporzionale alla sua capacità di archiviazione. I file system Amazon FSx for Lustre si adattano a più velocità effettiva e milioni TBps di IOPS. Amazon FSx for Lustre supporta anche l'accesso simultaneo allo stesso file o directory da migliaia di istanze di calcolo. Questo accesso consente il checkpoint rapido dei dati dalla memoria dell'applicazione allo storage, una tecnica comune nell'High Performance Computing (HPC). È possibile aumentare la quantità di storage e la capacità di throughput in base alle esigenze in qualsiasi momento dopo la creazione del file system. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione.

FSx i file system for Lustre forniscono una velocità di lettura a raffica utilizzando un meccanismo di I/O credito di rete per allocare la larghezza di banda della rete in base all'utilizzo medio della larghezza di banda. I file system accumulano crediti quando l'utilizzo della larghezza di banda di rete è inferiore ai limiti di base e possono utilizzarli quando eseguono trasferimenti di dati di rete.

Le tabelle seguenti mostrano le prestazioni per cui sono progettate le opzioni di implementazione di FSx for Lustre che utilizzano classi di archiviazione SSD e HDD.

Prestazioni del file system per le opzioni di archiviazione SSD

Tipo di distribuzione	Throughput di rete (MBps/TiB di storage fornito)		IOPS di rete (IOPS/TiB di storage fornito)	Archiviazione cache (GiB RAM/TiB di storage forniti)	Latenze del disco per operazione su file (millisecondi, P50)	Throughput del disco (MBps/TiB di storage o cache SSD fornita)	
	Linea di base	Scoppio				Linea di base	Scoppio
GRATTO_2	200	1300	Decine di migliaia di valori base	6.7	Metadati: sub-ms Dati: sub-ms	200 (letto) 100 (scrittura)	-
PERSISTENTE -125	320	1300	Centinaia di migliaia sono scoppiate	3.4		125	500
PERSISTENTE-250	640	1300		6.8		250	500
PERSISTENTE-500	1300	-		13.7		500	-
PERSISTENTE - 1000	2600	-		27,3		1000	-

Prestazioni del file system per le opzioni di archiviazione su HDD

Tipo di distribuzione	Throughput di rete (MBps/TiB di storage o cache SSD fornita)		IOPS di rete (IOPS/TiB di storage fornito)	Archiviazione cache (GiB RAM/TiB di storage forniti)	Latenze del disco per operazione su file (millisecondi, P50)	Throughput del disco (MBps/TiB di storage o cache SSD fornita)	
	Linea di base	Scoppio				Linea di base	Scoppio
PERSISTENTE-12							
archiviazione HDD	40	375*	Decine di migliaia (linea di base)	0,4 memoria	Metadati: sub-ms Dati: ms a una cifra	12	80 (letto) 50 (scrittura)
Cache di lettura SSD	200	1.900	Centinaia di migliaia sono scoppiate	200 cache SSD	Dati: sub-ms	200	-
PERSISTENTE-40							
archiviazione HDD	150	1.300*	Decine di migliaia di valori di base	1.5	Metadati: sub-ms Dati: ms a una cifra	40	250 (letto) 150 (scrittura)
Cache di lettura SSD	750	6500	Centinaia di migliaia sono scoppiate	200 cache SSD	Dati: sub-ms	200	-

Prestazioni del file system per le opzioni di storage SSD della generazione precedente

Tipo di distribuzione	Throughput di rete (MBps per TiB di storage fornito)		IOPS di rete (IOPS per TiB di storage fornito)	Archiviazione cache (GiB per TiB di storage fornito)	Latenze su disco per operazione su file (millisecondi, P50)	Throughput del disco (MBps per TiB di storage o cache SSD fornita)	
	Linea di base	Scoppio				Linea di base	Scoppio
PERSISTENTE-50	250	1.300*	Decine di migliaia di valori di base	2,2 RAM	Metadati: sub-ms	50	240
PERSISTENTE-100	500	1.300*		4,4 RAM	Dati: sub-ms	100	240
PERSISTENTE-200	750	1.300*	Centinaia di migliaia sono scoppiate	8,8 RAM		200	240

> **Note**
>
> * I file system persistenti nei seguenti paesi Regioni AWS forniscono un'espansione della rete fino a 530 per MBps TiB di storage: Africa (Città del Capo), Asia Pacifico (Hong Kong), Asia Pacifico (Osaka), Asia Pacifico (Singapore), Canada (Centrale), Europa (Francoforte), Europa (Londra), Europa (Milano), Europa (Stoccolma), Medio Oriente (Bahrein), Sud America (San Paolo), Cina e Stati Uniti occidentali (Los Angeles).

Esempio: velocità effettiva aggregata di base e burst

L'esempio seguente illustra come la capacità di storage e la velocità effettiva del disco influiscano sulle prestazioni del file system.

Un file system persistente con una capacità di storage di 4,8 TiB e 50 per TiB di throughput MBps per unità di storage fornisce un throughput aggregato del disco di base di 240 e un throughput del disco burst di MBps 1,152. GBps

Indipendentemente dalle dimensioni del file system, Amazon FSx for Lustre offre latenze costanti inferiori al millisecondo per le operazioni sui file.

Caratteristiche prestazionali della classe di storage Intelligent-Tiering

La classe di storage FSx for Lustre Intelligent-Tiering offre uno storage elastico e ottimizzato in termini di costi per carichi di lavoro che tradizionalmente vengono eseguiti su file system di archiviazione di file ad alte prestazioni basati su HDD o misti HDD/SDD basati su HDD/SDD. I file system che utilizzano la classe di storage Intelligent-Tiering utilizzano uno storage regionale completamente elastico e intelligente su più livelli, che cresce e si riduce automaticamente per adattarsi al carico di lavoro man mano che cambia. Per informazioni su come suddivide i dati su più livelli, consulta. In che modo la classe di storage Intelligent-Tiering suddivide i dati su più livelli

Il throughput supportato da un file system FSx for Lustre con classe di storage Intelligent-Tiering è indipendente dallo storage. I file system Intelligent-Tiering sono scalabili fino a raggiungere livelli multipli di throughput e milioni di IOPS. TBps I file system che utilizzano la classe di storage Intelligent-Tiering forniscono anche una cache di lettura SSD opzionale predisposta per l'accesso a bassa latenza ai dati a cui si accede di frequente. Per impostazione predefinita, Amazon FSx

for Lustre fornisce una cache di lettura SSD per i metadati a cui si accede di frequente. Poiché la maggior parte dei carichi di lavoro tende ad essere impegnativa in termini di lettura e funziona attivamente solo con un piccolo sottoinsieme del set di dati complessivo in un dato momento, il modello ibrido di storage Intelligent-Tiering e le cache di lettura SSD consente ai file system che utilizzano la classe di storage Intelligent-Tiering di fornire uno storage con prestazioni paragonabili ai file system SSD per la maggior parte dei carichi di lavoro, garantendo al contempo risparmi sui costi di archiviazione rispetto alle classi di storage SSD e HDD.

Durante la lettura e la scrittura di dati su un file system Intelligent-Tiering, in particolare dati a cui non è stato effettuato l'accesso di recente o non è stato effettuato abbastanza frequentemente da trovarsi nella cache in memoria del file server, le prestazioni dipendono dalla dimensione della cache di lettura SSD. L'accesso ai dati dallo storage Intelligent-Tiering ha time-to-first-byte latenze di circa decine di millisecondi e costi per richiesta, mentre gli accessi dalla cache di lettura SSD restituiscono con una latenza inferiore al millisecondo e senza costi per richiesta.

Quando si configura la dimensione della cache di lettura SSD per il file system, è necessario considerare sia la dimensione del set di dati a cui si accede di frequente all'interno del carico di lavoro sia la sensibilità del carico di lavoro a una latenza più elevata per le letture di dati a cui si accede meno frequentemente. È possibile passare da una modalità di dimensionamento della cache di lettura SSD all'altra dopo la creazione del file system e aumentare o ridurre la cache. Per ulteriori informazioni su come modificare la cache di lettura dell'SSD, consulta. Gestione della cache di lettura SSD fornita

Una richiesta di scrittura si verifica quando FSx for Lustre scrive un blocco di dati sullo storage Intelligent-Tiering. Quando si scrivono dati sul file system, le richieste di scrittura vengono aggregate e scritte sullo storage Intelligent-Tiering, aumentando la velocità effettiva e riducendo i costi delle richieste. Le letture possono essere eseguite dalla cache in memoria del file server, dalla cache di lettura SSD o direttamente dallo storage Intelligent-Tiering. Quando viene fornita una lettura dallo storage Intelligent-Tiering, viene effettuata una richiesta di lettura per ogni blocco di dati recuperati. Quando si leggono i dati in sequenza, FSx for Lustre prerecupererà i dati per migliorare le prestazioni.

I dati della cache in memoria sui file system che utilizzano la classe di storage Intelligent-Tiering vengono forniti direttamente al client richiedente come I/O di rete. Quando un client accede a dati che non si trovano nella cache in memoria, questi vengono letti dalla cache di lettura SSD o dallo storage Intelligent-Tiering come I/O su disco e quindi serviti al client come I/O di rete.

Prestazioni del file system per Intelligent-Tiering

La tabella seguente mostra le prestazioni FSx per cui sono progettati i file system Lustre Intelligent-Tiering.

Capacità di throughput assegnata () MBps	Throughput di rete () MBps		IOPS di rete	Archiviazione cache in memoria (GB)	Throughput massimo su disco di cache SSD () MBps	Numero massimo di IOPS su disco di cache SSD	
	Linea di base	Scoppio				Linea di base	Scoppio
Ogni 4000	12500	-	Centinaia di migliaia	76,8	4000	160000	-

Suggerimenti per le prestazioni

Quando usi Amazon FSx for Lustre, tieni a mente i seguenti suggerimenti sulle prestazioni. Per i limiti del servizio, consultaQuote di servizio per Amazon FSx for Lustre.

- I/O Dimensioni medie: poiché Amazon FSx for Lustre è un file system di rete, ogni operazione sui file passa attraverso un viaggio di andata e ritorno tra il client e Amazon FSx for Lustre, con un piccolo sovraccarico di latenza. A causa di questa latenza per operazione, la velocità effettiva complessiva generalmente aumenta all'aumentare della I/O dimensione media, poiché il sovraccarico viene ammortizzato su una maggiore quantità di dati.
- Modello di richiesta: abilitando le scritture asincrone sul file system, le operazioni di scrittura in sospeso vengono memorizzate nel buffer sull'istanza Amazon prima di essere scritte su EC2 Amazon for Lustre in modo asincrono. FSx Le scritture asincrone presentano generalmente delle latenze inferiori. Quando si eseguono delle scritture asincrone, il kernel utilizza della memoria aggiuntiva per la memorizzazione nella cache. Un file system che ha abilitato le scritture sincrone invia richieste sincrone ad Amazon FSx for Lustre. Ogni operazione passa attraverso un viaggio di andata e ritorno tra il cliente e Amazon FSx for Lustre.

  > **Note**
  >
  > Il modello di richiesta scelto presenta dei compromessi in termini di coerenza (se utilizzi più EC2 istanze Amazon) e velocità.

- Limita la dimensione delle directory: per ottenere prestazioni ottimali dei metadati sui file system Persistent 2 FSx for Lustre, limita ogni directory a meno di 100.000 file. La limitazione del numero di file in una directory riduce il tempo necessario al file system per acquisire un blocco sulla directory principale.
- EC2 Istanze Amazon: le applicazioni che eseguono un gran numero di operazioni di lettura e scrittura richiedono probabilmente più memoria o capacità di elaborazione rispetto alle applicazioni che non lo fanno. Quando avvii le tue EC2 istanze Amazon per un carico di lavoro ad alta intensità di calcolo, scegli i tipi di istanze che hanno la quantità di queste risorse necessaria alla tua applicazione. Le caratteristiche prestazionali dei file system Amazon FSx for Lustre non dipendono dall'uso di istanze ottimizzate per Amazon EBS.
- Ottimizzazione consigliata delle istanze del client per prestazioni ottimali

  1. Per i tipi di istanze client con memoria superiore a 64 GiB, consigliamo di applicare la seguente ottimizzazione:

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

2. Per i tipi di istanze client con più di 64 core vCPU, consigliamo di applicare la seguente ottimizzazione:

```
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
```

Dopo aver montato il client, è necessario applicare la seguente ottimizzazione:

```
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
```

Nota che `lctl set_param` è noto che non persiste dopo il riavvio. Poiché questi parametri non possono essere impostati in modo permanente dal lato client, si consiglia di implementare un boot cron job per impostare la configurazione con le ottimizzazioni consigliate.

- Equilibrio del carico di lavoro OSTs: in alcuni casi, il carico di lavoro non determina il throughput aggregato che il file system è in grado di fornire (200 per MBps TiB di storage). In tal caso, puoi utilizzare le CloudWatch metriche per risolvere i problemi se le prestazioni sono influenzate da uno squilibrio nei modelli del carico di lavoro. I/O Per identificare se questa è la causa, consulta la CloudWatch metrica Maximum per Amazon FSx for Lustre.

  In alcuni casi, questa statistica mostra un carico pari o superiore a 240 MBps di throughput (la capacità di throughput di un singolo disco Amazon for Lustre da 1,2 TiB). FSx In questi casi, il carico di lavoro non è distribuito uniformemente tra i dischi. In tal caso, puoi utilizzare il `lfs setstripe` comando per modificare lo striping dei file a cui il tuo carico di lavoro accede più frequentemente. Per prestazioni ottimali, suddividete i file con requisiti di throughput elevati in tutto il OSTs file system.

  Se i tuoi file vengono importati da un archivio di dati, puoi adottare un altro approccio per suddividere i file ad alta velocità in modo uniforme su tutto il tuo. OSTs A tale scopo, puoi modificare il `ImportedFileChunkSize` parametro durante la creazione del tuo prossimo file system Amazon FSx for Lustre.

Ad esempio, supponiamo che il carico di lavoro utilizzi un file system da 7,0 TiB (composto da 6 x 1,17 TiB) e debba garantire un throughput elevato su file da 2,4 GiB OSTs. In questo caso, potete impostare il valore in modo che i file siano distribuiti in modo uniforme su tutto il file system`ImportedFileChunkSize`. `(2.4 GiB / 6 OSTs) = 400 MiB` OSTs

- Lustreclient per Metadata IOPS: se nel tuo file system è specificata una configurazione di metadati, ti consigliamo di installare un client Lustre 2.15 o un client Lustre 2.12 con una di queste versioni del sistema operativo: Amazon Linux 2023; Amazon Linux 2; Red Hat/Rocky Linux 8.9, 8.10 o 9.x; CentOS 8.9 o 8.10; Ubuntu 22+ con kernel 6.2, 6.5 o 6.8 o Ubuntu 20.

Considerazioni sulle prestazioni di Intelligent-Tiering

Ecco alcune importanti considerazioni sulle prestazioni quando si lavora con i file system che utilizzano la classe di storage Intelligent-Tiering:

- I carichi di lavoro che leggono dati di I/O dimensioni inferiori richiederanno una maggiore concorrenza e comporteranno costi di richiesta maggiori per raggiungere lo stesso throughput dei carichi di lavoro che utilizzano grandi dimensioni a causa della maggiore latenza dei livelli di storage Intelligent-Tiering. I/O Consigliamo di configurare la cache di lettura SSD sufficientemente grande da supportare una concorrenza e un throughput più elevati quando si lavora con I/O di dimensioni inferiori.
- Il numero massimo di IOPS su disco che i client possono gestire con un file system Intelligent-Tiering dipende dai modelli di accesso specifici del carico di lavoro e dal fatto che sia stata predisposta una cache di lettura SSD. Per i carichi di lavoro con accesso casuale, i client possono in genere ottenere IOPS molto più elevati se i dati vengono memorizzati nella cache di lettura SSD rispetto a quando i dati non sono presenti nella cache.
- La classe di storage Intelligent-Tiering supporta il read-ahead per ottimizzare le prestazioni per le richieste di lettura sequenziali. Si consiglia di configurare il modello di accesso ai dati in sequenza, ove possibile, per consentire il recupero anticipato dei dati e prestazioni superiori.

Accesso ai file system

Con Amazon FSx, puoi trasferire i carichi di lavoro ad alta intensità di calcolo dall'ambiente locale ad Amazon Web Services Cloud importando dati tramite VPN. AWS Direct Connect Puoi accedere al tuo FSx file system Amazon da locale, copiare i dati nel file system secondo necessità ed eseguire carichi di lavoro a elaborazione intensiva su istanze in-cloud.

Nella sezione seguente, puoi imparare come accedere al tuo file system Amazon FSx for Lustre su un'istanza Linux. Inoltre, è possibile scoprire come utilizzare il file`fstab` per rimontare automaticamente il file system dopo un riavvio del sistema.

Prima di installare un file system, è necessario creare, configurare e avviare le risorse AWS correlate. Per istruzioni dettagliate, vedi Guida introduttiva ad Amazon FSx for Lustre. Successivamente, puoi installare e configurare il Lustre client sulla tua istanza di calcolo.

Argomenti

Lustrecompatibilità tra file system e kernel client

Consigliamo vivamente di utilizzare una Lustre versione FSx per il file system for Lustre compatibile con le versioni del kernel Linux delle istanze client.

Client Amazon Linux

Sistema operativo	Versione SO	Versione minima del kernel	Versione massima del kernel	Versione del client Lustre	Versione del file system Lustre		
					2.10	2,12	2,15
Amazon Linux 2023	6.1	61,79-99,167	6,179-99,167+	2.15	no	sì	sì
Amazon Linux 2	5,10	5,10,144-127,601	5,10,144-127,601+	2,12	sì	sì	sì
			<5,10,144-127,601	(2.10)	sì	sì	no
	5.4	5,4,214-120,368	5,4,214-120,368+	2,12	sì	sì	sì
			<5,4,214-120,368	(2.10)	sì	sì	no
	4,14	4,14,294-220,533	4,14,294-220,533+	2,12	sì	sì	sì
			<4,14,294-220,533	(2.10)	sì	sì	no

Client Ubuntu

Sistema operativo	Versione SO	Versione minima del kernel	Versione massima del kernel	Versione del client Lustre	Versione del file system Lustre		
					2.10	2,12	2,15
Ubuntu	24	6,8,0-1024	6,8,0*	2.15	no	sì	sì
	22	6,8,0-1017	6,8,0*	2.15	no	sì	sì
		6,5,0-1023	6,5,0*	2.15	no	sì	sì
		6,2,0-1017	6,2,0*	2.15	no	sì	sì
		5.15.0-1015-aws	5.15.0-1051-aws	2,12	sì	sì	sì
	20	5.15.0-1015-aws	5.15,0*	2,12	sì	sì	sì
		5.4.0-1011-aws	5.13.0-1031-aws	(2.10)	sì	sì	no

RHEL/CentOS/RockyClient Linux

Sistema operativo	Versione SO	Architettura	Versione minima del kernel	Versione massima del kernel	Versione del client Lustre	Versione del file system Lustre		
						2.10	2,12	2,15

Sistema operativo	Versione SO	Architettura	Versione minima del kernel	Versione massima del kernel	Versione del client Lustre	Versione del file system Lustre		
RHEL/ Rocky Linux	9.6	Braccio + x86	5.14.0-57 0,12.1	5,14,0-57 0*	2.15	no	sì	sì
	9,5	Braccio + x86	5.14.0-50 319.1	5,14,0-50 3*	2.15	no	sì	sì
	9.4	Braccio + x86	5.14.0-42 7,13.1	5,14,0-42 7*	2.15	no	sì	sì
	9.3	Braccio + x86	5.14.0-36 218.1	5,140-36 ,18,1	2.15	no	sì	sì
	9,0	Braccio + x86	5.14,0-70 .13,1	5,14-70,3 0,1	2.15	no	sì	sì
RHEL/ CentOS/ RockyLinux	8.10	Arm+ x86	4.18.0-55 3	4,18,0-55 3*	2,12	sì	sì	sì
	8.9	Braccio + x86	4.18.0-51 3*	4,180-51 *	2,12	sì	sì	sì
	8.8	Braccio + x86	4.18,0-47 7*	4,180-47 *	2,12	sì	sì	sì
	8.7	Braccio + x86	4.18,0-42 5*	4,180-42 *	2,12	sì	sì	sì
	8.6	Braccio + x86	4.18.0-37 2*	4,18,0-37 2*	2,12	sì	sì	sì

Sistema operativo	Versione SO	Architettura	Versione minima del kernel	Versione massima del kernel	Versione del client Lustre	Versione del file system Lustre		
	8,5	Braccio + x86	4.18.0-34 8*	4,18,0-34 8*	2,12	sì	sì	sì
	8.4	Braccio + x86	4.18.0-30 5*	4,18,0-30 5*	2,12	sì	sì	sì
RHEL/ CentOS	8.3	Braccio + x86	4.18,0-24 0*	4,18,0-24 0*	(2.10)	sì	sì	no
	8.2	Braccio + x86	4,18,0-19 3*	4,180-19 *	(2.10)	sì	sì	no
	7.9	x86	3,10,0-1 60*	3,10,0-1 60*	2,12	sì	sì	sì
	7.8	x86	3,10,0-1 27*	3,10,0-1 27*	(2.10)	sì	sì	no
	7.7	x86	3,10,0-10 62*	3,10,0-10 62*	(2.10)	sì	sì	no
CentOS	7.9	Arm	4,180-19 *	4,180-19 *	2,12	sì	sì	sì
	7.8	Arm	4,180-14 *	4,18,0-14 7*	2,12	sì	sì	sì

Installazione del client Lustre

Per montare il tuo file system Amazon FSx for Lustre da un'istanza Linux, installa prima il client open sourceLustre. Quindi, a seconda della versione del sistema operativo, utilizza una delle seguenti

procedure. Per informazioni sul supporto del kernel, vedereLustrecompatibilità tra file system e kernel client.

Se la tua istanza di calcolo non esegue il kernel Linux specificato nelle istruzioni di installazione e non puoi modificare il kernel, puoi creare il tuo client. Lustre Per ulteriori informazioni, consulta Compilazione Lustre sul Wiki. Lustre

Amazon Linux

Per installare il Lustre client su Amazon Linux 2023

1. Apri un terminale sul tuo client.
2. Determina quale kernel è attualmente in esecuzione sulla tua istanza di calcolo eseguendo il comando seguente.

   ```
   uname -r
   ```
3. Esamina la risposta del sistema e confrontala con i seguenti requisiti minimi del kernel per l'installazione del Lustre client su Amazon Linux 2023:

   - Requisiti minimi del kernel 6.1:6.1.79-99.167.amzn2023

   Se l' EC2 istanza soddisfa i requisiti minimi del kernel, procedi con il passaggio e installa il client. Lustre

   Se il comando restituisce un risultato inferiore al requisito minimo del kernel, aggiorna il kernel e riavvia l' EC2 istanza Amazon eseguendo il comando seguente.

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

   Verifica che il kernel sia stato aggiornato utilizzando il comando. uname -r
4. Scarica e installa il Lustre client con il seguente comando.

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

Per installare il Lustre client su Amazon Linux 2

1. Apri un terminale sul tuo client.

2. Determina quale kernel è attualmente in esecuzione sulla tua istanza di calcolo eseguendo il comando seguente.

```
uname -r
```

3. Esamina la risposta del sistema e confrontala con i seguenti requisiti minimi del kernel per l'installazione del Lustre client su Amazon Linux 2:

   - Requisiti minimi del kernel 5.10:5.10.144-127.601.amzn2
   - Requisiti minimi del kernel 5.4:5.4.214-120.368.amzn2
   - Requisiti minimi del kernel 4.14 - 4.14.294-220.533.amzn2

   Se la tua EC2 istanza soddisfa i requisiti minimi del kernel, procedi con il passaggio e installa il client. Lustre

   Se il comando restituisce un risultato inferiore al requisito minimo del kernel, aggiorna il kernel e riavvia l' EC2 istanza Amazon eseguendo il comando seguente.

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

   Verifica che il kernel sia stato aggiornato utilizzando il comando. uname -r

4. Scarica e installa il Lustre client con il seguente comando.

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

   Se non riesci ad aggiornare il kernel ai requisiti minimi del kernel, puoi installare il client 2.10 legacy con il seguente comando.

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

Per installare il Lustre client su Amazon Linux

1. Apri un terminale sul tuo client.
2. Determina quale kernel è attualmente in esecuzione sulla tua istanza di calcolo eseguendo il comando seguente. Il Lustre client richiede un kernel Amazon Linux `4.14, version 104` o superiore.

```
uname -r
```

3. Esegui una di queste operazioni:

   - Se il comando restituisce `4.14.104-78.84.amzn1.x86_64` o una versione successiva di 4.14, scarica e installa il Lustre client utilizzando il comando seguente.

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

   - Se il comando restituisce un risultato inferiore a`4.14.104-78.84.amzn1.x86_64`, aggiorna il kernel e riavvia l' EC2 istanza Amazon eseguendo il comando seguente.

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

     Verifica che il kernel sia stato aggiornato utilizzando il comando. uname -r Quindi scarica e installa il Lustre client come descritto in precedenza.

CentOS, Rocky Linux e Red Hat

Per installare il Lustre client su Red Hat e Rocky Linux 9.0 o 9.3—9.6

Puoi installare e aggiornare pacchetti Lustre client compatibili con Red Hat Enterprise Linux (RHEL) e Rocky Linux dal repository di pacchetti yum FSx Lustre del client Amazon. Questi pacchetti sono firmati per garantire che non siano stati manomessi prima o durante il download. L'installazione del repository fallisce se non si installa la chiave pubblica corrispondente sul sistema.

Per aggiungere il repository di pacchetti yum del FSx Lustre client Amazon

1. Apri un terminale sul tuo client.
2. Installa la chiave pubblica Amazon FSx rpm utilizzando il seguente comando.

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

3. Importa la chiave utilizzando il seguente comando.

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

4. Aggiungi il repository e aggiorna il gestore di pacchetti usando il seguente comando.

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

Per configurare il repository yum FSx Lustre del client Amazon

L'archivio di pacchetti yum del FSx Lustre client Amazon è configurato di default per installare il Lustre client compatibile con la versione del kernel inizialmente fornita con l'ultima versione supportata di Rocky Linux e RHEL 9. Per installare un Lustre client compatibile con la versione del kernel che stai utilizzando, puoi modificare il file di configurazione del repository.

Questa sezione descrive come determinare quale kernel è in esecuzione, se è necessario modificare la configurazione del repository e come modificare il file di configurazione.

1. Determina quale kernel è attualmente in esecuzione sulla tua istanza di calcolo utilizzando il comando seguente.

   ```
   uname -r
   ```

2. Esegui una di queste operazioni:

   - Se il comando viene restituito`5.14.0-570*`, non è necessario modificare la configurazione del repository. Continuare con la procedura Per installare il Lustre client.
   - Se il comando viene restituito`5.14.0-503*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release Rocky Linux e RHEL 9.5.
   - Se il comando viene restituito`5.14.0-427*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release Rocky Linux e RHEL 9.4.
   - Se il comando viene restituito`5.14.0-362.18.1`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release Rocky Linux e RHEL 9.3.
   - Se il comando viene restituito`5.14.0-70*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le versioni Rocky Linux e RHEL 9.0.

3. Modifica il file di configurazione del repository in modo che punti a una versione specifica di RHEL utilizzando il comando seguente. *`specific_RHEL_version`*Sostituiscilo con la versione RHEL che devi usare.

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

Ad esempio, per puntare alla versione 9.5, sostituitela *specific_RHEL_version* con `9.5` nel comando, come nell'esempio seguente.

```
sudo sed -i 's#9#9.5#' /etc/yum.repos.d/aws-fsx.repo
```

4. Usate il comando seguente per cancellare la cache yum.

```
sudo yum clean all
```

Per installare il client Lustre

- Installa i pacchetti dal repository usando il seguente comando.

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

Informazioni aggiuntive (Rocky Linux e Red Hat 9.0 e versioni successive)

I comandi precedenti installano i due pacchetti necessari per il montaggio e l'interazione con il FSx file system Amazon. Il repository include Lustre pacchetti aggiuntivi, come un pacchetto contenente il codice sorgente e pacchetti contenenti test, e puoi installarli facoltativamente. Per elencare tutti i pacchetti disponibili nel repository, utilizzare il comando seguente.

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

Per scaricare il codice sorgente rpm, contenente un archivio tar del codice sorgente originale e il set di patch che abbiamo applicato, usa il comando seguente.

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

Quando esegui yum update, viene installata una versione più recente del modulo, se disponibile, e la versione esistente viene sostituita. Per evitare che la versione attualmente installata venga rimossa durante l'aggiornamento, aggiungi una riga come la seguente al tuo `/etc/yum.conf` file.

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

Questo elenco include i pacchetti predefiniti di sola installazione, specificati nella pagina `yum.conf` man, e il `kmod-lustre-client` pacchetto.

Per installare il Lustre client su CentOS e Red Hat 8.2—8.10 o su Rocky Linux 8.4—8.10

Puoi installare e aggiornare pacchetti Lustre client compatibili con Red Hat Enterprise Linux (RHEL), Rocky Linux e CentOS dal repository di pacchetti yum del FSx Lustre client Amazon. Questi pacchetti sono firmati per garantire che non siano stati manomessi prima o durante il download. L'installazione del repository fallisce se non si installa la chiave pubblica corrispondente sul sistema.

Per aggiungere il repository di pacchetti yum del FSx Lustre client Amazon

1. Apri un terminale sul tuo client.
2. Installa la chiave pubblica Amazon FSx rpm utilizzando il seguente comando.

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

3. Importa la chiave utilizzando il seguente comando.

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

4. Aggiungi il repository e aggiorna il gestore di pacchetti usando il seguente comando.

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

Per configurare il repository yum FSx Lustre del client Amazon

L'archivio di pacchetti yum del FSx Lustre client Amazon è configurato di default per installare il Lustre client compatibile con la versione del kernel inizialmente fornita con l'ultima versione supportata di CentOS, Rocky Linux e RHEL 8. Per installare un Lustre client compatibile con la versione del kernel che stai utilizzando, puoi modificare il file di configurazione del repository.

Questa sezione descrive come determinare quale kernel è in esecuzione, se è necessario modificare la configurazione del repository e come modificare il file di configurazione.

1. Determina quale kernel è attualmente in esecuzione sulla tua istanza di calcolo utilizzando il comando seguente.

```
uname -r
```

2. Esegui una di queste operazioni:

   - Se il comando viene restituito`4.18.0-553*`, non è necessario modificare la configurazione del repository. Continuare con la procedura Per installare il Lustre client.
   - Se il comando viene restituito`4.18.0-513*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per la versione CentOS, Rocky Linux e RHEL 8.9.
   - Se il comando viene restituito`4.18.0-477*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release CentOS, Rocky Linux e RHEL 8.8.
   - Se il comando viene restituito`4.18.0-425*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release CentOS, Rocky Linux e RHEL 8.7.
   - Se il comando viene restituito`4.18.0-372*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release CentOS, Rocky Linux e RHEL 8.6.
   - Se il comando viene restituito`4.18.0-348*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release CentOS, Rocky Linux e RHEL 8.5.
   - Se il comando viene restituito`4.18.0-305*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per la versione CentOS, Rocky Linux e RHEL 8.4.
   - Se il comando viene restituito`4.18.0-240*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release CentOS e RHEL 8.3.
   - Se il comando viene restituito`4.18.0-193*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release CentOS e RHEL 8.2.

3. Modificate il file di configurazione del repository in modo che punti a una versione specifica di RHEL utilizzando il comando seguente.

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

   Ad esempio, per puntare alla versione 8.9, sostituitela *`specific_RHEL_version`* con `8.9` nel comando.

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

4. Usate il seguente comando per cancellare la cache yum.

   ```
   sudo yum clean all
   ```

Per installare il client Lustre

- Installa i pacchetti dal repository usando il seguente comando.

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

Informazioni aggiuntive (CentOS, Rocky Linux e Red Hat 8.2 e versioni successive)

I comandi precedenti installano i due pacchetti necessari per il montaggio e l'interazione con il FSx file system Amazon. Il repository include Lustre pacchetti aggiuntivi, come un pacchetto contenente il codice sorgente e pacchetti contenenti test, e puoi installarli facoltativamente. Per elencare tutti i pacchetti disponibili nel repository, utilizzare il comando seguente.

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

Per scaricare il codice sorgente rpm, contenente un archivio tar del codice sorgente originale e il set di patch che abbiamo applicato, usa il comando seguente.

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

Quando esegui yum update, viene installata una versione più recente del modulo, se disponibile, e la versione esistente viene sostituita. Per evitare che la versione attualmente installata venga rimossa durante l'aggiornamento, aggiungi una riga come la seguente al tuo `/etc/yum.conf` file.

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

Questo elenco include i pacchetti predefiniti di sola installazione, specificati nella pagina `yum.conf` man, e il `kmod-lustre-client` pacchetto.

Per installare il Lustre client su CentOS e Red Hat 7.7, 7.8 o 7.9 (istanze x86_64)

Puoi installare e aggiornare pacchetti Lustre client compatibili con Red Hat Enterprise Linux (RHEL) e CentOS dal repository di pacchetti yum del client FSx Lustre Amazon. Questi pacchetti sono firmati per garantire che non siano stati manomessi prima o durante il download. L'installazione del repository fallisce se non si installa la chiave pubblica corrispondente sul sistema.

Per aggiungere il repository di pacchetti yum del FSx Lustre client Amazon

1. Apri un terminale sul tuo client.
2. Installa la chiave pubblica Amazon FSx rpm utilizzando il seguente comando.

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

3. Importa la chiave usando il seguente comando.

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

4. Aggiungi il repository e aggiorna il gestore di pacchetti usando il seguente comando.

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

Per configurare il repository yum FSx Lustre del client Amazon

L'archivio di pacchetti yum del FSx Lustre client Amazon è configurato di default per installare il Lustre client compatibile con la versione del kernel inizialmente fornita con l'ultima versione supportata di CentOS e RHEL 7. Per installare un Lustre client compatibile con la versione del kernel che stai utilizzando, puoi modificare il file di configurazione del repository.

Questa sezione descrive come determinare quale kernel è in esecuzione, se è necessario modificare la configurazione del repository e come modificare il file di configurazione.

1. Determina quale kernel è attualmente in esecuzione sulla tua istanza di calcolo utilizzando il comando seguente.

```
uname -r
```

2. Esegui una di queste operazioni:

   - Se il comando viene restituito`3.10.0-1160*`, non è necessario modificare la configurazione del repository. Continuare con la procedura Per installare il Lustre client.
   - Se il comando viene restituito`3.10.0-1127*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release CentOS e RHEL 7.8.

- Se il comando viene restituito`3.10.0-1062*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per le release CentOS e RHEL 7.7.

3. Modificate il file di configurazione del repository in modo che punti a una versione specifica di RHEL utilizzando il comando seguente.

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

   Per puntare alla versione 7.8, sostituitela *`specific_RHEL_version`* con `7.8` nel comando.

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

   Per puntare alla versione 7.7, sostituitela *`specific_RHEL_version`* con `7.7` nel comando.

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

4. Usate il seguente comando per cancellare la cache yum.

   ```
   sudo yum clean all
   ```

Per installare il client Lustre

- Installa i pacchetti Lustre client dal repository utilizzando il seguente comando.

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

Informazioni aggiuntive (CentOS e Red Hat 7.7 e versioni successive)

I comandi precedenti installano i due pacchetti necessari per il montaggio e l'interazione con il FSx file system Amazon. Il repository include Lustre pacchetti aggiuntivi, come un pacchetto contenente il codice sorgente e pacchetti contenenti test, e puoi installarli facoltativamente. Per elencare tutti i pacchetti disponibili nel repository, utilizzare il comando seguente.

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

Per scaricare il codice sorgente rpm contenente un archivio tar del codice sorgente originale e il set di patch che abbiamo applicato, usa il seguente comando.

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

Quando esegui yum update, viene installata una versione più recente del modulo, se disponibile, e la versione esistente viene sostituita. Per evitare che la versione attualmente installata venga rimossa durante l'aggiornamento, aggiungi una riga come la seguente al tuo `/etc/yum.conf` file.

```
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
```

Questo elenco include i pacchetti predefiniti di sola installazione, specificati nella pagina `yum.conf` man, e il `kmod-lustre-client` pacchetto.

Per installare il Lustre client su CentOS 7.8 o 7.9 (istanze basate su ARM basate su Graviton) AWS

Puoi installare e aggiornare i pacchetti Lustre client dal repository di pacchetti yum del FSx Lustre client Amazon compatibili con CentOS 7 per istanze basate su ARM basate su Graviton. AWS EC2 Questi pacchetti sono firmati per garantire che non siano stati manomessi prima o durante il download. L'installazione del repository fallisce se non si installa la chiave pubblica corrispondente sul sistema.

Per aggiungere il repository di pacchetti yum del FSx Lustre client Amazon

1. Apri un terminale sul tuo client.
2. Installa la chiave pubblica Amazon FSx rpm utilizzando il seguente comando.

   ```
   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. Importa la chiave usando il seguente comando.

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

4. Aggiungi il repository e aggiorna il gestore di pacchetti usando il seguente comando.

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

Per configurare il repository yum FSx Lustre del client Amazon

Il repository di pacchetti yum del FSx Lustre client Amazon è configurato di default per installare il Lustre client compatibile con la versione del kernel inizialmente fornita con l'ultima versione supportata di CentOS 7. Per installare un Lustre client compatibile con la versione del kernel che stai utilizzando, puoi modificare il file di configurazione del repository.

Questa sezione descrive come determinare quale kernel è in esecuzione, se è necessario modificare la configurazione del repository e come modificare il file di configurazione.

1. Determina quale kernel è attualmente in esecuzione sulla tua istanza di calcolo utilizzando il comando seguente.

   ```
   uname -r
   ```

2. Esegui una di queste operazioni:

   - Se il comando viene restituito`4.18.0-193*`, non è necessario modificare la configurazione del repository. Continuare con la procedura Per installare il Lustre client.
   - Se il comando ritorna`4.18.0-147*`, è necessario modificare la configurazione del repository in modo che punti al Lustre client per la versione CentOS 7.8.

3. Modifica il file di configurazione del repository in modo che punti alla versione CentOS 7.8 utilizzando il seguente comando.

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

4. Usa il seguente comando per cancellare la cache yum.

   ```
   sudo yum clean all
   ```

Per installare il client Lustre

- Installa i pacchetti dal repository usando il seguente comando.

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

Informazioni aggiuntive (CentOS 7.8 o 7.9 per istanze basate su ARM basate su Graviton) AWS EC2

I comandi precedenti installano i due pacchetti necessari per il montaggio e l'interazione con il FSx file system Amazon. Il repository include Lustre pacchetti aggiuntivi, come un pacchetto contenente il codice sorgente e pacchetti contenenti test, e puoi installarli facoltativamente. Per elencare tutti i pacchetti disponibili nel repository, utilizzare il comando seguente.

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

Per scaricare il codice sorgente rpm, contenente un archivio tar del codice sorgente originale e il set di patch che abbiamo applicato, usa il comando seguente.

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

Quando esegui yum update, viene installata una versione più recente del modulo, se disponibile, e la versione esistente viene sostituita. Per evitare che la versione attualmente installata venga rimossa durante l'aggiornamento, aggiungi una riga come la seguente al tuo `/etc/yum.conf` file.

```
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
```

Questo elenco include i pacchetti predefiniti di sola installazione, specificati nella pagina `yum.conf` man, e il `kmod-lustre-client` pacchetto.

Ubuntu

Per installare il Lustre client su Ubuntu 18.04, 20.04, 22.04 o 24.04

Puoi scaricare Lustre i pacchetti dal repository Amazon FSx Ubuntu. Per verificare che il contenuto del repository non sia stato manomesso prima o durante il download, viene applicata una firma GNU Privacy Guard (GPG) ai metadati del repository. L'installazione del repository fallisce a meno che sul sistema non sia installata la chiave GPG pubblica corretta.

1. Apri un terminale sul tuo client.

2. Segui questi passaggi per aggiungere il repository Amazon FSx Ubuntu:

   a. Se non hai registrato in precedenza un repository Amazon FSx Ubuntu sull'istanza client, scarica e installa la chiave pubblica richiesta. Utilizza il seguente comando.

   ```
   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. Aggiungi l'archivio di FSx pacchetti Amazon al tuo gestore di pacchetti locale utilizzando il seguente comando.

   ```
   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. Determina quale kernel è attualmente in esecuzione sull'istanza client e aggiorna se necessario. Per un elenco dei kernel richiesti per il Lustre client su Ubuntu sia per le istanze basate su x86 che per le EC2 istanze basate su ARM alimentate da processori Graviton, EC2 vedi. AWS Client Ubuntu

   a. Esegui il comando seguente per determinare quale kernel è in esecuzione.

   ```
   uname -r
   ```

   b. Esegui il comando seguente per eseguire l'aggiornamento al kernel e alla Lustre versione di Ubuntu più recenti, quindi riavvia.

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

   Se la versione del kernel è superiore alla versione minima del kernel sia per le istanze basate su x86 che per EC2 le istanze basate su Graviton e non desideri eseguire l'aggiornamento alla versione più recente del kernel, puoi eseguire l' EC2 installazione per il kernel corrente con il seguente comando. Lustre

   ```
   sudo apt install -y lustre-client-modules-$(uname -r)
   ```

   Vengono installati i due Lustre pacchetti necessari per il montaggio e l'interazione con il file system for Lustre. FSx Facoltativamente, è possibile installare pacchetti correlati aggiuntivi,

come un pacchetto contenente il codice sorgente e pacchetti contenenti test inclusi nel repository.

c. Elenca tutti i pacchetti disponibili nel repository utilizzando il comando seguente.

```
sudo apt-cache search ^lustre
```

d. (Facoltativo) Se desiderate che l'aggiornamento del sistema aggiorni sempre anche i moduli Lustre client, assicuratevi che il `lustre-client-modules-aws` pacchetto sia installato utilizzando il comando seguente.

```
sudo apt install -y lustre-client-modules-aws
```

> **Note**
>
> Se si `Module Not Found` verifica un errore, consultaPer risolvere gli errori dei moduli mancanti.

Per risolvere gli errori dei moduli mancanti

Se si `Module Not Found` verifica un errore durante l'installazione su qualsiasi versione di Ubuntu, procedi come segue:

Effettua il downgrade del kernel all'ultima versione supportata. Elenca tutte le versioni disponibili del lustre-client-modules pacchetto e installa il kernel corrispondente. A questo scopo, eseguire il comando seguente.

```
sudo apt-cache search lustre-client-modules
```

Ad esempio, se la versione più recente inclusa nel repository è`lustre-client-modules-5.4.0-1011-aws`, procedi come segue:

1. Installa il kernel per cui è stato creato questo pacchetto usando i seguenti comandi.

```
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. Riavviate l'istanza utilizzando il seguente comando.

```
sudo reboot
```

3. Installa il Lustre client utilizzando il seguente comando.

```
sudo apt-get install -y lustre-client-modules-$(uname -r)
```

SUSE Linux

Per installare il Lustre client su SUSE Linux 12 SP3 SP4, oppure SP5

Per installare il Lustre client su SUSE Linux 12 SP3

1. Apri un terminale sul tuo client.
2. Installa la chiave pubblica Amazon FSx rpm utilizzando il seguente comando.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-
public-key.asc
```

3. Importa la chiave utilizzando il seguente comando.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Aggiungere il repository per il Lustre client utilizzando il comando seguente.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-
lustre-client.repo
```

5. Scarica e installa il Lustre client con i seguenti comandi.

```
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
```

Per installare il Lustre client su SUSE Linux 12 SP4

1. Apri un terminale sul tuo client.
2. Installa la chiave pubblica Amazon FSx rpm utilizzando il seguente comando.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Importa la chiave utilizzando il seguente comando.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Aggiungere il repository per il Lustre client utilizzando il comando seguente.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Esegui una di queste operazioni:

   - Se l'hai installato SP4 direttamente, scarica e installa il Lustre client con i seguenti comandi.

     ```
     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
     ```

   - Se hai eseguito la migrazione da SP3 a SP4 e in precedenza hai aggiunto il FSx repository Amazon per SP3, scarica e installa il Lustre client con i seguenti comandi.

     ```
     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
     ```

Per installare il Lustre client su SUSE Linux 12 SP5

1. Apri un terminale sul tuo client.

2. Installa la chiave pubblica Amazon FSx rpm utilizzando il seguente comando.

```
sudo wget https://fsx-lustre-client-repo-public-keys.s3.amazonaws.com/fsx-sles-public-key.asc
```

3. Importa la chiave utilizzando il seguente comando.

```
sudo rpm --import fsx-sles-public-key.asc
```

4. Aggiungere il repository per il Lustre client utilizzando il comando seguente.

```
sudo wget https://fsx-lustre-client-repo.s3.amazonaws.com/suse/sles-12/SLES-12/fsx-lustre-client.repo
```

5. Esegui una di queste operazioni:

   - Se l'hai installato SP5 direttamente, scarica e installa il Lustre client con i seguenti comandi.

```
sudo zypper ar --gpgcheck-strict fsx-lustre-client.repo
sudo zypper refresh
sudo zypper in lustre-client
```

   - Se hai eseguito la migrazione da SP4 a SP5 e in precedenza hai aggiunto il FSx repository Amazon per SP4, scarica e installa il Lustre client con i seguenti comandi.

```
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**
>
> Potrebbe essere necessario riavviare l'istanza di calcolo per completare l'installazione del client.

Montaggio da un'istanza Amazon Elastic Compute Cloud

Puoi montare il tuo file system da un' EC2 istanza Amazon.

Per montare il tuo file system da Amazon EC2

1. Connect alla tua EC2 istanza Amazon.
2. Crea una directory sul tuo file system FSx for Lustre per il punto di montaggio con il seguente comando.

```
$ sudo mkdir -p /fsx
```

3. Installa il file system Amazon FSx for Lustre nella directory che hai creato. Usa il seguente comando e sostituisci i seguenti elementi:

   - Sostituire *`file_system_dns_name`* con il nome DNS effettivo del file system.
   - Sostituisci *`mountname`* con il nome di mount del file system. Questo nome di montaggio viene restituito nella risposta dell'operazione `CreateFileSystem` API. Viene inoltre restituito nella risposta del describe-file-systems AWS CLI comando e nell'operazione DescribeFileSystemsAPI.

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

   Questo comando monta il file system con due opzioni `-o relatime eflock`:

   - `relatime`— Sebbene l'`atime`opzione mantenga `atime` (tempi di accesso agli inode) i dati per ogni accesso a un file, l'`relatime`opzione mantiene anche `atime` i dati, ma non per ogni volta che si accede a un file. Con l'`relatime`opzione abilitata, `atime` i dati vengono scritti su disco solo se il file è stato modificato dall'ultimo aggiornamento `atime` dei dati (`mtime`) o se l'ultimo accesso al file è avvenuto più di un certo periodo di tempo fa (6 ore per impostazione predefinita). L'utilizzo dell'`atime`opzione `relatime` o ottimizzerà i processi di rilascio dei file.

     > **Note**
     >
     > Se il carico di lavoro richiede una precisione precisa nel tempo di accesso, puoi montarlo con l'opzione di `atime` montaggio. Tuttavia, ciò può influire sulle prestazioni del carico di lavoro aumentando il traffico di rete necessario per mantenere valori precisi del tempo di accesso.
     > Se il carico di lavoro non richiede tempi di accesso ai metadati, l'utilizzo dell'opzione di `noatime` montaggio per disabilitare gli aggiornamenti al tempo di accesso può fornire un miglioramento delle prestazioni. Tieni presente che `atime` processi specifici come

il rilascio dei file o il rilascio della validità dei dati saranno imprecisi al momento del rilascio.

- `flock`— Abilita il blocco dei file per il file system. Se non vuoi abilitare il blocco dei file, usa il `mount` comando without. `flock`

4. Verificate che il comando mount abbia avuto successo elencando il contenuto della directory in cui avete montato il file system, /mnt/fsx, utilizzando il seguente comando.

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

È inoltre possibile utilizzare il comando seguente. `df`

```
$ 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
```

I risultati mostrano il FSx file system Amazon montato su /fsx.

Configurazione dei client EFA

Utilizza le seguenti procedure per configurare il client Lustre per accedere a un file system abilitato FSx per EFA per Lustre.

Argomenti

- Installazione dei moduli EFA e configurazione delle interfacce
- Aggiungere o rimuovere interfacce EFA
- Installazione del driver GDS

Installazione dei moduli EFA e configurazione delle interfacce

Per accedere a un file system FSx for Lustre utilizzando un'interfaccia EFA, è necessario installare i moduli Lustre EFA e configurare le interfacce EFA. EFA è attualmente supportato su client Lustre che eseguono AL2 023, RHEL 9.5 e versioni successive o Ubuntu 22+ con versione del kernel 6.8 e successive. Consulta la Fase 3: Installa il software EFA nella Amazon EC2 User Guide e scopri come installare il driver EFA.

Per configurare l'istanza del client su un file system compatibile con EFA

> **Important**
>
> È necessario eseguire lo `configure-efa-fsx-lustre-client.sh` script (al passaggio 3 di seguito) prima di montare il file system.

1. Connect alla tua EC2 istanza Amazon.
2. Copia lo script seguente e salvalo come file denominato`configure-efa-fsx-lustre-client.sh`.

```
#!/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin

echo "Started ${0} at $(date)"

lfs_version="$(lfs --version | awk '{print $2}')"
if [[ ! $lfs_version =~ (2.15) ]]; then
    echo "Error: Lustre client version 2.15 is required"
    exit 1
fi

eth_intf="$(ip -br -4 a sh | grep $(hostname -i)/ | awk '{print $1}')"
efa_version=$(modinfo efa | awk '/^version:/ {print $2}' | sed 's/[^0-9.]//g')
min_efa_version="2.12.1"

# Check the EFA driver version. Minimum v2.12.1 supported
if [[ -z "$efa_version" ]]; then
    echo "Error: EFA driver not found"
    exit 1
fi
```

```
if [[ "$(printf '%s\n' "$min_efa_version" "$efa_version" | sort -V | head -n1)" !=
 "$min_efa_version" ]]; then
    echo "Error: EFA driver version $efa_version does not meet the minimum
 requirement $min_efa_version"
    exit 1
else
    echo "Using EFA driver version $efa_version"
fi

echo "Loading Lustre/EFA modules..."
sudo /sbin/modprobe lnet
sudo /sbin/modprobe kefalnd ipif_name="$eth_intf"
sudo /sbin/modprobe ksocklnd
sudo lnetctl lnet configure

echo "Configuring TCP interface..."
sudo lnetctl net del --net tcp 2> /dev/null
sudo lnetctl net add --net tcp --if $eth_intf

# For P5 instance type which supports 32 network cards,
# by default add 8 EFA interfaces selecting every 4th device (1 per PCI bus)
echo "Configuring EFA interface(s)..."
instance_type="$(ec2-metadata --instance-type | awk '{ print $2 }')"
num_efa_devices="$(ls -1 /sys/class/infiniband | wc -l)"
echo "Found $num_efa_devices available EFA device(s)"

if [[ "$instance_type" == "p5.48xlarge" || "$instance_type" == "p5e.48xlarge" ]];
 then
    for intf in $(ls -1 /sys/class/infiniband | awk 'NR % 4 == 1'); do
        sudo lnetctl net add --net efa --if $intf --peer-credits 32
    done
else
# Other instances: Configure 2 EFA interfaces by default if the instance supports
 multiple network cards,
# or 1 interface for single network card instances
# Can be modified to add more interfaces if instance type supports it
    sudo lnetctl net add --net efa --if $(ls -1 /sys/class/infiniband | head -n1)
 --peer-credits 32
    if [[ $num_efa_devices -gt 1 ]]; then
        sudo lnetctl net add --net efa --if $(ls -1 /sys/class/infiniband | tail -
n1) --peer-credits 32
    fi
fi
```

```
echo "Setting discovery and UDSP rule"
sudo lnetctl set discovery 1
sudo lnetctl udsp add --src efa --priority 0
sudo /sbin/modprobe lustre

sudo lnetctl net show
echo "Added $(sudo lnetctl net show | grep -c '@efa') EFA interface(s)"
```

3. Esegui lo script di configurazione EFA.

```
sudo apt-get install amazon-ec2-utils cron
sudo chmod +x configure-efa-fsx-lustre-client.sh
./configure-efa-fsx-lustre-client.sh
```

4. Utilizzate i seguenti comandi di esempio per impostare un cron job che riconfigura automaticamente EFA sulle istanze client dopo il riavvio:

```
(sudo crontab -l 2>/dev/null; echo "@reboot /path/to/configure-efa-fsx-lustre-
client.sh > /var/log/configure-efa-fsx-lustre-client-output.log") | sudo crontab -
```

Aggiungere o rimuovere interfacce EFA

Ciascun file system FSx for Lustre ha un limite massimo di 1024 connessioni EFA su tutte le istanze client.

Lo `configure-efa-fsx-lustre-client.sh` script configura automaticamente il numero di interfacce Elastic Fabric Adapter (EFA) su un' EC2 istanza in base al tipo di istanza. Per le istanze P5 (`p5.48xlargeop5e.48xlarge`), configura 8 interfacce EFA per impostazione predefinita. Per altre istanze con più schede di rete, configura 2 interfacce EFA. Per le istanze con una singola scheda di rete, configura 1 interfaccia EFA. Quando un'istanza client si connette a un file system FSx for Lustre, ogni interfaccia EFA configurata sull'istanza del client conta ai fini del limite di 1024 connessioni EFA.

Le istanze client con più interfacce EFA in genere supportano livelli di throughput più elevati per istanza client rispetto alle istanze client con un minor numero di interfacce EFA. Purché non superi il limite di connessione EFA, puoi modificare lo script per aumentare o diminuire il numero di interfacce EFA per istanza per ottimizzare le prestazioni di throughput per client per i tuoi carichi di lavoro.

Per aggiungere un'interfaccia EFA:

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

Dove *device_name* è elencato un dispositivo. `ls -1 /sys/class/infiniband`

Per eliminare un'interfaccia EFA:

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

Installazione del driver GDS

Per utilizzare GPUDirect Storage (GDS) su FSx for Lustre, devi usare un'istanza client Amazon EC2 P5 o P5e e il driver NVIDIA GDS con una versione di release 2.24.2 o successiva.

> **Note**
>
> Se utilizzi un'istanza AMI Deep Learning, il driver NVIDIA GPUDirect Storage (GDS) è preinstallato e puoi saltare questa procedura di installazione del driver.

Per installare il driver NVIDIA GPUDirect Storage sull'istanza client

1. Clona il repository NVIDIA/ disponibile su gds-nvidia-fs . GitHub

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

2. Dopo aver clonato il repository, usa i seguenti comandi per creare il driver:

   ```
   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
   ```

Montaggio da Amazon Elastic Container Service

Puoi accedere al tuo file system FSx for Lustre da un contenitore Docker Amazon Elastic Container Service (Amazon ECS) su un'istanza Amazon. EC2 Puoi farlo utilizzando una delle seguenti opzioni:

1. Montando il file system FSx for Lustre dall' EC2 istanza Amazon che ospita le attività di Amazon ECS ed esportando questo punto di montaggio nei contenitori.
2. Montando il file system direttamente all'interno del contenitore delle attività.

Per ulteriori informazioni su Amazon ECS, consulta Cos'è Amazon Elastic Container Service? nella Amazon Elastic Container Service Developer Guide.

Ti consigliamo di utilizzare l'opzione 1 (Montaggio da un' EC2 istanza Amazon che ospita attività Amazon ECS) perché consente un migliore utilizzo delle risorse, soprattutto se avvii molti container (più di cinque) sulla stessa EC2 istanza o se le tue attività sono di breve durata (meno di 5 minuti).

Usa l'opzione 2 (Montaggio da un contenitore Docker), se non riesci a configurare l' EC2 istanza o se l'applicazione richiede la flessibilità del contenitore.

> **Note**
>
> Il montaggio FSx di Lustre su un tipo di lancio AWS Fargate non è supportato.

Le sezioni seguenti descrivono le procedure per ciascuna delle opzioni per il montaggio del file system FSx for Lustre da un contenitore Amazon ECS.

Argomenti

- Montaggio da un' EC2 istanza Amazon che ospita attività Amazon ECS
- Montaggio da un contenitore Docker

Montaggio da un' EC2 istanza Amazon che ospita attività Amazon ECS

Questa procedura mostra come configurare un Amazon ECS su EC2 istanza per montare localmente il file system FSx for Lustre. La procedura utilizza `volumes` le proprietà del `mountPoints` contenitore per condividere la risorsa e rendere questo file system accessibile alle attività eseguite localmente. Per ulteriori informazioni, consulta Launching an Amazon ECS Container Instance nella Amazon Elastic Container Service Developer Guide.

Questa procedura è per un'AMI Amazon Linux 2 ottimizzata per Amazon ECS. Se stai usando un'altra distribuzione Linux, vedi. Installazione del client Lustre

Per montare il file system da Amazon ECS su un'istanza EC2

1. Quando avvii istanze Amazon ECS, manualmente o utilizzando un gruppo Auto Scaling, aggiungi le righe nel seguente esempio di codice alla fine del campo Dati utente. Sostituisci i seguenti elementi nell'esempio:

- Sostituire *file_system_dns_name* con il nome DNS effettivo del file system.
- Sostituisci *mountname* con il nome di mount del file system.
- Sostituisci *mountpoint* con il punto di montaggio del file system, che devi creare.

```
#!/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. Quando crei le tue attività Amazon ECS, aggiungi quanto segue `volumes` e le proprietà del `mountPoints` contenitore nella definizione JSON. Sostituisci *mountpoint* con il punto di montaggio del file system (ad esempio`/mnt/fsx`).

```
{
    "volumes": [
           {
                 "host": {
                      "sourcePath": "mountpoint"
                 },
                 "name": "Lustre"
           }
    ],
    "mountPoints": [
           {
                 "containerPath": "mountpoint",
                 "sourceVolume": "Lustre"
           }
    ],
}
```

Montaggio da un contenitore Docker

La procedura seguente mostra come configurare un contenitore di attività Amazon ECS per installare il `lustre-client` pacchetto e montare al suo interno il file system FSx for Lustre. La procedura utilizza un'immagine Docker di Amazon Linux (`amazonlinux`), ma un approccio simile può funzionare per altre distribuzioni.

Per montare il file system da un contenitore Docker

1. Sul tuo contenitore Docker, installa il `lustre-client` pacchetto e monta il file system FSx for Lustre con la proprietà. `command` Sostituisci i seguenti elementi nell'esempio:

   - Sostituire *`file_system_dns_name`* con il nome DNS effettivo del file system.
   - Sostituisci *`mountname`* con il nome di mount del file system.
   - Sostituisci *`mountpoint`* con il punto di montaggio del file system.

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

2. Aggiungi `SYS_ADMIN` la funzionalità al contenitore per autorizzarlo a montare il file system FSx for Lustre, utilizzando la `linuxParameters` proprietà.

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

Montaggio di FSx file system Amazon da un ambiente locale o da un Amazon VPC peer-to-peer

Puoi accedere al tuo FSx file system Amazon in due modi. Una proviene da EC2 istanze Amazon situate in un Amazon VPC collegato al VPC del file system. L'altro proviene da client locali collegati al VPC del file system AWS Direct Connect tramite una VPN.

Collega il VPC del client e il VPC del tuo FSx file system Amazon utilizzando una connessione peering VPC o un gateway di transito VPC. Quando utilizzi una connessione peering VPC o un gateway di transito per connetterti, EC2 le istanze VPCs Amazon che si trovano in un VPC possono accedere ai file FSx system Amazon in un altro VPC, anche se appartengono a account diversi. VPCs

Prima di utilizzare la procedura seguente, è necessario configurare una connessione peering VPC o un gateway di transito VPC.

Un gateway di transito è un hub di transito di rete che puoi utilizzare per interconnettere le tue VPCs reti e quelle locali. Per ulteriori informazioni sull'utilizzo di VPC Transit Gateway, consulta l'argomento relativo alle nozioni di base su Transit Gateway nella Guida di Amazon VPC Transit Gateway.

Una connessione peering VPC è una connessione di rete tra due. VPCs Questo tipo di connessione consente di instradare il traffico tra di essi utilizzando indirizzi privati del protocollo Internet versione 4 (IPv4) o del protocollo Internet versione 6 (IPv6). Puoi utilizzare il peering VPC per connetterti VPCs all'interno della stessa AWS regione o tra regioni. AWS Per ulteriori informazioni, consulta Che cos'è il peering di VPC? nella Guida al peering di Amazon VPC.

È possibile montare il file system dall'esterno del VPC utilizzando l'indirizzo IP dell'interfaccia di rete principale. L'interfaccia di rete principale è la prima interfaccia di rete restituita quando si esegue il `aws fsx describe-file-systems` AWS CLI comando. Puoi ottenere questo indirizzo IP anche dalla console di gestione di Amazon Web Services.

La tabella seguente illustra i requisiti degli indirizzi IP per accedere ai FSx file system Amazon utilizzando un client esterno al VPC del file system.

Per i clienti che si trovano in...	Accesso ai file system creati prima del 17 dicembre 2020	Accesso ai file system creati a partire dal 17 dicembre 2020
Peering VPCs tramite peering VPC o AWS Transit Gateway	Client con indirizzi IP in un intervallo di indirizzi IP privati RFC 1918: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	✓
Reti peer che utilizzano o AWS Direct Connect AWS VPN		✓

Se devi accedere al tuo FSx file system Amazon creato prima del 17 dicembre 2020 utilizzando un intervallo di indirizzi IP non privato, puoi creare un nuovo file system ripristinando un backup del file system. Per ulteriori informazioni, consulta Protezione dei dati con backup.

Per recuperare l'indirizzo IP dell'interfaccia di rete principale per un file system

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione, scegli File system.
3. Scegli il tuo file system dalla dashboard.
4. Dalla pagina dei dettagli del file system, scegli Rete e sicurezza.
5. Per Interfaccia di rete, scegli l'ID per la tua interfaccia elastica di rete principale. In questo modo si accede alla EC2 console Amazon.
6. Nella scheda Dettagli, trova l' IPv4 IP privato primario. Questo è l'indirizzo IP dell'interfaccia di rete principale.

> **Note**
>
> Non puoi utilizzare la risoluzione dei nomi DNS (Domain Name System) quando monti un FSx file system Amazon dall'esterno del VPC a cui è associato.

Montaggio automatico FSx del file system Amazon

Puoi aggiornare il `/etc/fstab` file nella tua EC2 istanza Amazon dopo esserti connesso all'istanza per la prima volta in modo che monti il tuo FSx file system Amazon ogni volta che si riavvia.

Utilizzo di /etc/fstab per il montaggio automatico di Lustre FSx

Per montare automaticamente la directory FSx del file system Amazon al riavvio dell' EC2 istanza Amazon, puoi utilizzare il `fstab` file. Il file `fstab` contiene informazioni sui file system. Il comando`mount -a`, che viene eseguito durante l'avvio dell'istanza, monta i file system elencati nel `fstab` file.

> **Note**
>
> Prima di poter aggiornare il `/etc/fstab` file della tua EC2 istanza, assicurati di aver già creato il tuo FSx file system Amazon. Per ulteriori informazioni, consulta Passaggio 1: crea il tuo FSx file system for Lustre l'esercizio Getting Started.

Per aggiornare il file /etc/fstab nell'istanza EC2

1. Connect all' EC2 istanza e apri il `/etc/fstab` file in un editor.
2. Aggiungere la seguente riga al file `/etc/fstab`.

   Installa il file system Amazon FSx for Lustre nella directory che hai creato. Usa il seguente comando e sostituisci quanto segue:

   - Sostituisci *`/fsx`* con la directory in cui desideri montare il tuo FSx file system Amazon.
   - Sostituisci *`file_system_dns_name`* con il nome DNS effettivo del file system.
   - Sostituisci *`mountname`* con il nome di mount del file system. Questo nome di montaggio viene restituito nella risposta dell'operazione `CreateFileSystem` API. Viene inoltre restituito nella risposta del describe-file-systems AWS CLI comando e nell'operazione `DescribeFileSystems` API.

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

> **Warning**
>
> In caso di montaggio automatico del file system, utilizzare l'opzione `_netdev`, usata per identificare i file system di rete. Se `_netdev` manca, l' EC2istanza potrebbe smettere di rispondere. Questo risultato è dovuto al fatto che i file system di rete devono essere inizializzati dopo che l'istanza di calcolo ha avviato la sua interfaccia di rete. Per ulteriori informazioni, consulta Il montaggio automatico non funziona e l'istanza non risponde.

3. Salvare le modifiche apportate al file.

L' EC2 istanza è ora configurata per montare il FSx file system Amazon ogni volta che viene riavviato.

> **Note**
>
> In alcuni casi, potrebbe essere necessario avviare l' EC2 istanza Amazon indipendentemente dallo stato del FSx file system Amazon montato. In questi casi, aggiungi l'`nofail`opzione alla voce del file system nel `/etc/fstab` file.

I campi della riga di codice che avete aggiunto al `/etc/fstab` file eseguono le seguenti operazioni.

Campo	Descrizione
`file_system_dns_name` `@tcp:/`	Il nome DNS del tuo FSx file system Amazon, che identifica il file system. Puoi ottenere questo nome dalla console o a livello di codice da o da un SDK. AWS CLI AWS
`mountname`	Il nome di montaggio per il file system. È possibile ottenere questo nome dalla console o a livello di codice AWS CLI utilizzando il describe-file-systems comando oppure l' AWS API o l'SDK utilizzando l'operazione. `DescribeFileSystems`
/fsx	Il punto di montaggio per il FSx file system Amazon sulla tua EC2 istanza.
`lustre`	Il tipo di file system, Amazon FSx.

Campo	Descrizione
`mount options`	Opzioni di montaggio per il file system, presentate come elenco separato da virgole delle seguenti opzioni: • `defaults`— Questo valore indica al sistema operativo di utilizzare le opzioni di montaggio predefinite. È possibile elencare le opzioni di montaggio predefinite dopo il montaggio del file system visualizz ando l'output del `mount` comando. • `relatime`— Questa opzione mantiene i dati `atime` (tempi di accesso agli inode), ma non per ogni accesso a un file. Con questa opzione abilitata, `atime` i dati vengono scritti su disco solo se il file è stato modificato dall'ultimo aggiornamento `atime` dei dati (`mtime`) o se l'ultimo accesso al file è avvenuto più di un certo periodo di tempo fa (un giorno per impostazione predefinita). Se vuoi disattivare gli aggiornamenti del tempo di accesso agli inode, usa invece l'opzione `noatime` mount. • `flock`— installa il file system con il blocco dei file abilitato. Se non vuoi abilitare il blocco dei file, usa invece l'opzione di `noflock` montaggio. • `_netdev`— Il valore indica al sistema operativo che il file system risiede su un dispositivo che richiede l'accesso alla rete. Questa opzione impedisce all'istanza da montare il file system fino a quando la rete non è stata abilitata sul client.
`x-systemd .automount,x- systemd.requir es=networ k.service`	Queste opzioni assicurano che il montaggio automatico non funzioni finché la connettività di rete non è online. **Note** Per Amazon Linux 2023 e Ubuntu 22.04, usa l'`x-systemd .requires=systemd-networkd-wait-onli ne.service` opzione anziché l'`x-systemd.requires =network.service` opzione.

Campo	Descrizione
`0`	Un valore che indica se il file system deve essere sottoposto a backup dadump. Per Amazon FSx, questo valore dovrebbe essere`0`.
`0`	Un valore che indica l'ordine in cui `fsck` controlla i file system all'avvio . Per i FSx file system Amazon, questo valore dovrebbe `0` indicare che non `fsck` deve essere eseguito all'avvio.

Montaggio di set di file specifici

Utilizzando la funzionalità Lustre fileset, è possibile montare solo un sottoinsieme dello spazio dei nomi del file system, chiamato fileset. Per montare un set di file del file system, sul client si specifica il percorso della sottodirectory dopo il nome del file system. Un montaggio su un set di file (chiamato anche montaggio di sottodirectory) limita la visibilità dello spazio dei nomi del file system su un client specifico.

Esempio: monta un set di file Lustre

1. Supponiamo di avere un file system FSx for Lustre con le seguenti directory:

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

2. Si monta solo il `team1/dataset1` fileset, rendendo visibile localmente sul client solo questa parte del file system. Utilizzate il seguente comando e sostituite i seguenti elementi:

   - Sostituire *`file_system_dns_name`* con il nome DNS effettivo del file system.
   - Sostituisci *`mountname`* con il nome di mount del file system. Questo nome di montaggio viene restituito nella risposta dell'operazione `CreateFileSystem` API. Viene inoltre restituito nella risposta del describe-file-systems AWS CLI comando e nell'operazione DescribeFileSystemsAPI.

   ```
   mount -t lustre file_system_dns_name@tcp:/mountname/team1/dataset1 /fsx
   ```

Quando utilizzate la funzione Lustre fileset, tenete presente quanto segue:

- Non ci sono vincoli che impediscano a un client di rimontare il file system utilizzando un set di file diverso o nessun set di file.
- Quando si utilizza un fileset, alcuni comandi Lustre amministrativi che richiedono l'accesso alla `.lustre/` directory potrebbero non funzionare, come il comando. `lfs fid2path`
- Se prevedi di montare diverse sottodirectory dello stesso file system sullo stesso host, tieni presente che ciò consuma più risorse di un singolo punto di montaggio e potrebbe essere più efficiente montare invece la directory principale del file system una sola volta.

Per ulteriori informazioni sulla funzionalità del Lustre set di file, consultate il Lustre Operations Manual sul sito Web della documentazione. Lustre

Smontaggio dei file system

Prima di eliminare un file system FSx for Lustre, assicurati che sia smontato da tutte le EC2 istanze Amazon che lo hanno montato e, prima di chiudere o terminare qualsiasi EC2 istanza Amazon, assicurati che tutti i file system montati FSx per Lustre siano smontati da quell'istanza.

FSx i server for Lustre garantiscono blocchi temporanei di file e directory ai client durante I/O le operazioni e i client devono rispondere prontamente quando i server chiedono ai client di sbloccare i blocchi per sbloccare le operazioni. 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 Per evitare questi periodi di attesa, è sempre consigliabile smontare il file system dalle istanze client prima di chiuderle o terminarle e prima di eliminarle per i file system Lustre. FSx

Puoi smontare un file system sulla tua EC2 istanza Amazon eseguendo il `umount` comando sull'istanza stessa. Non puoi smontare un FSx file system Amazon tramite AWS CLI AWS Management Console, il o tramite uno qualsiasi dei AWS SDKs. Per smontare un FSx file system Amazon connesso a un' EC2 istanza Amazon che esegue Linux, usa il `umount` comando seguente:

```
umount /mnt/fsx
```

È consigliabile non specificare nessun'altra opzione di `umount`. Evitare di impostare qualsiasi altra opzione di `umount` differente da quelle di default.

Puoi verificare che il tuo FSx file system Amazon sia stato smontato eseguendo il `df` comando. Questo comando visualizza le statistiche sull'utilizzo del disco per i file system attualmente montati sulla tua istanza Amazon EC2 basata su Linux. Se il FSx file system Amazon che desideri smontare non è elencato nell'output del `df` comando, significa che il file system è smontato.

Example — Identifica lo stato di montaggio di un FSx file system Amazon e smontalo

```
$ 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% /
```

Utilizzo delle istanze Amazon EC2 Spot

FSx for Lustre può essere utilizzato con le istanze EC2 Spot per ridurre significativamente i costi di Amazon EC2 . Un'istanza Spot è un' EC2 istanza inutilizzata disponibile a un prezzo inferiore a quello di On-Demand. Amazon EC2 può interrompere un'istanza Spot quando il prezzo Spot supera il prezzo massimo, quando la domanda di istanze Spot aumenta o quando l'offerta di istanze Spot diminuisce.

Quando Amazon EC2 interrompe un'istanza Spot, invia un avviso di interruzione dell'istanza Spot, che invia all'istanza un avviso di due minuti prima che Amazon EC2 la interrompa. Per ulteriori informazioni, consulta le istanze Spot nella Amazon EC2 User Guide.

Per garantire che i FSx file system Amazon non siano influenzati dalle interruzioni delle istanze EC2 Spot, consigliamo di smontare i FSx file system Amazon prima di terminare o ibernare le istanze Spot. EC2 Per ulteriori informazioni, consulta Smontaggio dei file system.

Gestione delle interruzioni delle istanze Amazon EC2 Spot

FSx for Lustre è un file system distribuito in cui istanze server e client collaborano per fornire un file system affidabile e performante. Mantengono uno stato distribuito e coerente tra le istanze client e server. FSx i server for Lustre delegano le autorizzazioni di accesso temporanee ai client mentre gestiscono I/O e memorizzano attivamente nella cache i dati del file system. I client dovrebbero

rispondere in un breve periodo di tempo quando i server richiedono loro di revocare le autorizzazioni di accesso temporanee. Per proteggere il file system dai client che si comportano male, i server possono eliminare i Lustre client che non rispondono dopo pochi minuti. Per evitare di dover attendere diversi minuti prima che un client che non risponde risponda alla richiesta del server, è importante smontare i Lustre client in modo corretto, soprattutto prima di chiudere le istanze Spot. EC2

EC2 Spot invia avvisi di cessazione con 2 minuti di anticipo prima di chiudere un'istanza. Ti consigliamo di automatizzare il processo di smontaggio accurato dei client prima di chiudere le istanze SpotLustre. EC2

Example — Script per smontare in modo pulito e terminare le istanze Spot EC2

Questo script di esempio smonta in modo pulito le istanze Spot che EC2 terminano effettuando le seguenti operazioni:

- Controlla gli avvisi di cessazione di Spot.
- Quando riceve un avviso di risoluzione:
  - Arresta le applicazioni che accedono al file system.
  - Smonta il file system prima che l'istanza venga terminata.

È possibile adattare lo script in base alle esigenze, soprattutto per chiudere correttamente l'applicazione. Per ulteriori informazioni sulle migliori pratiche per la gestione delle interruzioni delle istanze Spot, consulta Best practice per la gestione EC2 delle interruzioni delle istanze Spot.

```
#!/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
```

Amministrazione dei file system

FSx for Lustre offre una serie di funzionalità che semplificano l'esecuzione delle attività amministrative. Queste includono la possibilità di eseguire point-in-time backup, gestire le quote di storage del file system, gestire la capacità di storage e di throughput, gestire la compressione dei dati e impostare finestre di manutenzione per l'esecuzione di patch software di routine del sistema.

Puoi amministrare i tuoi file system FSx for Lustre utilizzando Amazon FSx Management Console, AWS Command Line Interface (AWS CLI), Amazon FSx API o. AWS SDKs

Argomenti

Utilizzo di file system compatibili con EFA

Se stai creando un file system con oltre il 10% GBps della capacità di throughput, ti consigliamo di abilitare Elastic Fabric Adapter (EFA) per ottimizzare il throughput per istanza client. EFA è un'interfaccia di rete ad alte prestazioni che utilizza una tecnica di bypass del sistema operativo personalizzata e il protocollo di rete AWS Scalable Reliable Datagram (SRD) per aumentare le prestazioni. Per informazioni su EFA, consulta Elastic Fabric Adapter per carichi di lavoro AI/ML e HPC su Amazon nella EC2 Amazon User Guide. EC2

I file system compatibili con EFA supportano due funzionalità prestazionali aggiuntive: GPUDirect Storage (GDS) ed ENA Express. Il supporto GDS si basa su EFA per migliorare ulteriormente le prestazioni abilitando il trasferimento diretto dei dati tra il file system e la memoria della GPU, bypassando la CPU. Questo percorso diretto elimina la necessità di copie di memoria ridondanti e il coinvolgimento della CPU nelle operazioni di trasferimento dei dati. Con il supporto di EFA e GDS, è possibile ottenere un throughput più elevato per le singole istanze client abilitate per EFA. ENA Express fornisce comunicazioni di rete ottimizzate per EC2 le istanze Amazon utilizzando un algoritmo avanzato di selezione del percorso e un meccanismo di controllo della congestione migliorato. Con il supporto ENA Express, puoi ottenere un throughput più elevato per le singole istanze client abilitate per ENA Express. Per informazioni su ENA Express, consulta Migliorare le prestazioni di rete tra EC2 le istanze con ENA Express nella Amazon EC2 User Guide.

Argomenti

Considerazioni sull'utilizzo di file system compatibili con EFA

Ecco alcuni elementi importanti da considerare quando si creano file system compatibili con EFA:

- Molteplici opzioni di connettività: i file system compatibili con EFA possono comunicare con le istanze client utilizzando ENA, ENA Express ed EFA.
- Tipo di implementazione: EFA è supportato sui file system Persistent 2 con una configurazione di metadati specificata, inclusi i file system che utilizzano la classe di storage Intelligent-Tiering.
- Aggiornamento delle impostazioni EFA: puoi scegliere di abilitare EFA quando crei un nuovo file system, ma non puoi abilitare o disabilitare EFA su un file system esistente.
- Scalabilità del throughput in base alla capacità di archiviazione: è possibile scalare la capacità di storage su un file system basato su SSD abilitato EFA per aumentare la capacità di throughput, ma non è possibile modificare il livello di throughput di un file system compatibile con EFA.
- Regioni AWS: Per un elenco dei file system Persistent 2 compatibili con EFA, vedere Regioni AWS . Disponibilità del tipo di implementazione

Prerequisiti per l'utilizzo di file system compatibili con EFA

Di seguito sono riportati i prerequisiti per l'utilizzo di file system compatibili con EFA:

Per creare un file system compatibile con EFA:

- Utilizza un gruppo di sicurezza abilitato all'EFA. Per ulteriori informazioni, consulta gruppi di sicurezza abilitati all'EFA.
- Utilizza la stessa zona di disponibilità e /16 CIDR delle istanze client abilitate per EFA all'interno del tuo Amazon VPC.
- Sui file system Intelligent-Tiering, EFA è supportato solo con una capacità di throughput di 4.000 o incrementi di 4.000. MBps MBps

Per accedere al file system utilizzando Elastic Fabric Adapter (EFA):

- Utilizza istanze Nitro v4 (o superiore) che supportano EFA, escluse le famiglie di EC2 istanze p5en e trn2. Consulta i tipi di istanze supportati nella Amazon EC2 User Guide.
- Esegui AL2 023, RHEL 9.5 e versioni successive oppure Ubuntu 22+ con la versione del kernel 6.8 e successive. Per ulteriori informazioni, consulta Installazione del client Lustre.
- Installa i moduli EFA e configura le interfacce EFA sulle istanze client. Per ulteriori informazioni, consulta Configurazione dei client EFA.

Per accedere al file system utilizzando GPUDirect Storage (GDS):

- Usa un'istanza client Amazon EC2 P5 o P5e.
- Installa il pacchetto NVIDIA Compute Unified Device Architecture (CUDA), il driver NVIDIA open source e il driver di storage NVIDIA sull'istanza client. GPUDirect Per ulteriori informazioni, consulta Installazione del driver GDS.

Per accedere al file system utilizzando ENA Express:

- Usa EC2 istanze Amazon che supportano ENA Express. Consulta i tipi di istanze supportati per ENA Express nella Amazon EC2 User Guide.
- Aggiorna le impostazioni per la tua istanza Linux. Consulta i prerequisiti per le istanze Linux nella Amazon EC2 User Guide.
- Abilita ENA Express sulle interfacce di rete per le istanze dei tuoi client. Per i dettagli, consulta Rivedi le impostazioni ENA Express per la tua EC2 istanza nella Amazon EC2 User Guide.

Utilizzo Lustre quote di archiviazione

È possibile creare quote di archiviazione per utenti, gruppi e progetti sui file system FSx Lustre. Con le quote di archiviazione, è possibile limitare la quantità di spazio su disco e il numero di file che un utente, un gruppo o un progetto può consumare. Le quote di archiviazione tengono automaticamente traccia dell'utilizzo a livello di utente, a livello di gruppo e a livello di progetto in modo da poter monitorare il consumo indipendentemente dalla scelta o meno di impostare limiti di archiviazione.

Amazon FSx impone le quote e impedisce agli utenti che le hanno superate di scrivere nello spazio di archiviazione. Quando gli utenti superano le quote, devono eliminare un numero sufficiente di file per rientrare nei limiti di quota, in modo da poter scrivere nuovamente sul file system.

Argomenti

Applicazione delle quote

L'applicazione delle quote per utenti, gruppi e progetti viene abilitata automaticamente su tutti i file system FSx di For Lustre. Non è possibile disabilitare l'applicazione delle quote.

Tipi di quote

Gli amministratori di sistema con credenziali utente root dell' AWS account possono creare i seguenti tipi di quote:

- Una quota utente si applica a un singolo utente. Una quota di utenti per un utente specifico può essere diversa dalle quote di altri utenti.
- Una quota di gruppo si applica a tutti gli utenti che sono membri di un gruppo specifico.
- Una quota di progetto si applica a tutti i file o le directory associati a un progetto. Un progetto può includere più directory o singoli file situati in diverse directory all'interno di un file system.

> **Note**
>
> Le quote di progetto sono supportate solo su Lustre versione 2.15 in poi FSx per i file system Lustre.

- Una quota di blocco limita la quantità di spazio su disco che un utente, un gruppo o un progetto può consumare. È possibile configurare la dimensione di archiviazione in kilobyte.
- Una quota di inode limita il numero di file o directory che un utente, un gruppo o un progetto può creare. Il numero massimo di inode viene configurato come numero intero.

> **Note**
>
> Le quote predefinite non sono supportate.

Se imposti quote per un particolare utente e un gruppo e l'utente è membro di quel gruppo, l'utilizzo dei dati da parte dell'utente si applica a entrambe le quote. È inoltre limitato da entrambe le quote. Se viene raggiunto uno dei limiti di quota, all'utente viene impedito di scrivere sul file system.

> **Note**
>
> Le quote impostate per l'utente root non vengono applicate. Analogamente, la scrittura di dati come utente root utilizzando il `sudo` comando ignora l'imposizione della quota.

Limiti di quota e periodi di tolleranza

Amazon FSx impone le quote di utenti, gruppi e progetti come limite rigido o limite minimo con un periodo di tolleranza configurabile.

Il limite rigido è il limite assoluto. Se gli utenti superano il limite rigido, l'allocazione di blocchi o inode ha esito negativo e viene visualizzato il messaggio «Quota disco superata». Gli utenti che hanno raggiunto il limite di quota devono eliminare un numero sufficiente di file o directory per rientrare al di sotto del limite di quota prima di poter scrivere nuovamente sul file system. Quando viene impostato un periodo di prova, gli utenti possono superare il limite minimo entro il periodo di prova, se al di sotto del limite rigido.

Per i limiti non vincolanti, si configura un periodo di tolleranza in secondi. Il limite flessibile deve essere inferiore al limite rigido.

È possibile impostare periodi di grazia diversi per inode e quote di blocco. È inoltre possibile impostare periodi di grazia diversi per una quota utente, una quota di gruppo e una quota di progetto. Quando le quote utente, di gruppo e di progetto hanno periodi di grazia diversi, il limite minimo si trasforma in un limite rigido dopo lo scadere del periodo di grazia di una di queste quote.

Quando gli utenti superano un limite consentito, Amazon FSx consente loro di continuare a superare la quota fino allo scadere del periodo di prova o fino al raggiungimento del limite rigido. Al termine del periodo di prova, il limite flessibile si converte in un limite rigido e agli utenti viene impedito di eseguire ulteriori operazioni di scrittura fino a quando l'utilizzo dello storage non torna al di sotto della quota di blocchi o dei limiti di inode definiti. Gli utenti non ricevono notifiche o avvisi all'inizio del periodo di prova.

Impostazione e visualizzazione delle quote

Le quote di archiviazione vengono impostate utilizzando Lustre `lfs`comandi del file system nel terminale Linux. Il `lfs setquota` comando imposta i limiti di quota e visualizza le informazioni sulle quote. `lfs quota`

Per ulteriori informazioni sull' Lustre comandi di quota, vedere il Manuale operativo di Lustre sul Lustre sito web di documentazione.

Impostazione delle quote per utenti, gruppi e progetti

La sintassi del `setquota` comando per impostare le quote di utenti, gruppi o progetti è la seguente.

```
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
```

Dove:

- `-u` o `--user` specifica un utente per cui impostare una quota.
- `-g` o `--group` specifica un gruppo per cui impostare una quota.
- `-p` o `--project` specifica un progetto per cui impostare una quota.

- `-b`imposta una quota di blocco con un limite flessibile. `-B`Imposta una quota di blocco con un limite rigido. Entrambi *`block_softlimit`* *`block_hardlimit`* sono espressi in kilobyte e il valore minimo è 1024 KB.
- `-i`imposta una quota di inode con un limite flessibile. `-I`imposta una quota di inode con un limite rigido. Entrambi *`inode_softlimit`* gli inodi *`inode_hardlimit`* sono espressi in numero di inodi e il valore minimo è 1024 inode.
- *`mount_point`*è la directory su cui è stato montato il file system.

Esempio di quota utente: il comando seguente imposta un limite di soft block di 5.000 KB, un limite di 8.000 KB di hard block, un limite di 2.000 soft inode e una quota limite di 3.000 hard inode per il file system `user1` su cui è montato. `/mnt/fsx`

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

Esempio di quota di gruppo: il comando seguente imposta un limite di 100.000 KB per i blocchi fissi per il gruppo indicato nel file system `group1` su cui è montato. `/mnt/fsx`

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

Esempio di quota di progetto: assicurati innanzitutto di aver utilizzato il `project` comando per associare i file e le directory desiderati al progetto. Ad esempio, il comando seguente associa tutti i file e le sottodirectory della `/mnt/fsxfs/dir1` directory al progetto il cui ID del progetto è. `100`

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

Quindi utilizzate il `setquota` comando per impostare la quota del progetto. Il comando seguente imposta un limite di 307.200 KB per i soft block, un limite di 309.200 KB per i blocchi rigidi, un limite di 10.000 soft inode e una quota limite di 11.000 hard inode per il progetto `250` sul file system su cui è montato. `/mnt/fsx`

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

Impostazione dei periodi di grazia

Il periodo di tolleranza predefinito è di una settimana. È possibile modificare il periodo di tolleranza predefinito per utenti, gruppi o progetti utilizzando la seguente sintassi.

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

Dove:

- `-t`indica che verrà impostato un periodo di tolleranza.
- `-u`imposta un periodo di grazia per tutti gli utenti.
- `-g`imposta un periodo di grazia per tutti i gruppi.
- `-p`imposta un periodo di grazia per tutti i progetti.
- `-b`imposta un periodo di grazia per le quote in blocco. `-i`imposta un periodo di grazia per le quote di inode. Entrambi *`block_grace`* e *`inode_grace`* sono espressi in secondi interi o nel formato. `XXwXXdXXhXXmXXs`
- *`mount_point`*è la directory su cui è stato montato il file system.

Il comando seguente imposta periodi di grazia di 1.000 secondi per le quote di blocco utente e di 1 settimana e 4 giorni per le quote di inode utente.

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

Visualizzazione delle quote

Il `quota` comando visualizza informazioni sulle quote degli utenti, sulle quote di gruppo, sulle quote di progetto e sui periodi di tolleranza.

Comando View quota	Informazioni sulla quota visualizzate
`lfs quota /mount_point`	Informazioni generali sulla quota (utilizzo e limiti del disco) per l'utente che esegue il comando e il gruppo primario dell'utente.
`lfs quota -u username /mount_point`	Informazioni generali sulle quote per un utente specifico

Comando View quota	Informazioni sulla quota visualizzate
	. Gli utenti con credenzia li utente root dell' AWS account possono eseguire questo comando per qualsiasi utente, ma gli utenti non root non possono eseguire questo comando per ottenere informazioni sulle quote relative ad altri utenti.
`lfs quota -u username -v /mount_point`	Informazioni generali sulle quote per un utente specifico e statistiche dettagliate sulle quote per ogni object storage target (OST) e metadata target (MDT). Gli utenti con credenziali utente root dell' AWS account possono eseguire questo comando per qualsiasi utente, ma gli utenti non root non possono eseguire questo comando per ottenere informazioni sulle quote relative ad altri utenti.
`lfs quota -g groupname  /mount_point`	Informazioni generali sulle quote per un gruppo specifico.
`lfs quota -p projectid  /mount_point`	Informazioni generali sulle quote per un progetto specifico.
`lfs quota -t -u /mount_point`	Tempi di tolleranza relativi ai blocchi e agli inode per le quote degli utenti.

Comando View quota	Informazioni sulla quota visualizzate
`lfs quota -t -g /mount_point`	Tempi di tolleranza di blocco e inode per le quote di gruppo.
`lfs quota -t -p /mount_point`	Tempi di tolleranza dei blocchi e degli inode per le quote di progetto.

Quotas e bucket collegati ad Amazon S3

Puoi collegare il file system FSx for Lustre a un repository di dati Amazon S3. Per ulteriori informazioni, consulta Collegamento del file system a un bucket Amazon S3.

Facoltativamente, puoi scegliere una cartella o un prefisso specifico all'interno di un bucket S3 collegato come percorso di importazione verso il tuo file system. Quando una cartella in Amazon S3 viene specificata e importata nel tuo file system da S3, solo i dati di quella cartella vengono applicati alla quota. I dati dell'intero bucket non vengono conteggiati nei limiti di quota.

I metadati dei file in un bucket S3 collegato vengono importati in una cartella con una struttura corrispondente alla cartella importata da Amazon S3. Questi file vengono conteggiati ai fini delle quote di inode degli utenti e dei gruppi proprietari dei file.

Quando un utente esegue `hsm_restore` o carica in modo lento un file, la dimensione completa del file viene conteggiata ai fini della quota di blocco associata al proprietario del file. Ad esempio, se l'utente A lazy carica un file di proprietà dell'utente B, la quantità di spazio di archiviazione e di utilizzo degli inode viene conteggiata ai fini della quota dell'utente B. Allo stesso modo, quando un utente utilizza l' FSx API Amazon per rilasciare un file, i dati vengono liberati dalle quote di blocco dell'utente o del gruppo proprietario del file.

Poiché i ripristini HSM e il lazy loading vengono eseguiti con accesso root, aggirano l'applicazione delle quote. Una volta importati, i dati vengono conteggiati ai fini dell'utente o del gruppo in base alla proprietà impostata in S3, il che può far sì che utenti o gruppi superino i limiti di blocco. In tal caso, dovranno liberare i file per poter scrivere nuovamente sul file system.

Allo stesso modo, i file system con importazione automatica abilitata creeranno automaticamente nuovi inode per gli oggetti aggiunti a S3. Questi nuovi inode vengono creati con accesso root e

bypassano l'applicazione delle quote durante la creazione. Questi nuovi inode verranno conteggiati per gli utenti e i gruppi, in base a chi possiede l'oggetto in S3. Se tali utenti e gruppi superano le rispettive quote di inode in base all'attività di importazione automatica, dovranno eliminare i file per liberare ulteriore capacità e scendere al di sotto dei limiti di quota.

Quote e ripristino dei backup

Quando si ripristina un backup, le impostazioni delle quote del file system originale vengono implementate nel file system ripristinato. Ad esempio, se le quote sono impostate nel file system A e il file system B viene creato da un backup del file system A, le quote del file system A vengono applicate nel file system B.

Gestione della capacità di archiviazione

È possibile aumentare la capacità di archiviazione SSD o HDD configurata sul file system FSx for Lustre in base alle esigenze di storage e throughput aggiuntivi. Poiché il throughput di un file system FSx for Lustre è scalabile in modo lineare con la capacità di archiviazione, si ottiene anche un aumento comparabile della capacità di throughput. Per aumentare la capacità di archiviazione, puoi utilizzare la FSx console Amazon, AWS Command Line Interface (AWS CLI) o l' FSx API Amazon.

Quando richiedi un aggiornamento della capacità di storage del tuo file system, Amazon aggiunge FSx automaticamente nuovi file server di rete e ridimensiona il tuo server di metadati. Durante la scalabilità della capacità di archiviazione, il file system potrebbe non essere disponibile per alcuni minuti. Le operazioni sui file eseguite dai client mentre il file system non è disponibile verranno riprovate in modo trasparente e alla fine avranno esito positivo una volta completata la scalabilità dello storage. Durante il periodo in cui il file system non è disponibile, lo stato del file system è impostato su. `UPDATING` Una volta completata la scalabilità dello storage, lo stato del file system viene impostato `AVAILABLE` su.

Amazon esegue FSx quindi un processo di ottimizzazione dello storage che riequilibra in modo trasparente i dati tra i file server esistenti e quelli appena aggiunti. Il ribilanciamento viene eseguito in background senza alcun impatto sulla disponibilità del file system. Durante il ribilanciamento, è possibile che si verifichi una riduzione delle prestazioni del file system a causa del consumo di risorse per lo spostamento dei dati. Per la maggior parte dei file system, l'ottimizzazione dello storage richiede da alcune ore a qualche giorno. È possibile accedere e utilizzare il file system durante la fase di ottimizzazione.

Puoi monitorare i progressi dell'ottimizzazione dello storage in qualsiasi momento utilizzando la FSx console Amazon, la CLI e l'API. Per ulteriori informazioni, consulta Monitoraggio dell'aumento della capacità di archiviazione.

Argomenti

Considerazioni sull'aumento della capacità di storage

Ecco alcuni elementi importanti da considerare quando si aumenta la capacità di archiviazione:

- Solo aumento: è possibile solo aumentare la quantità di capacità di archiviazione di un file system, ma non diminuire la capacità di archiviazione.
- Aumenta gli incrementi: quando si aumenta la capacità di archiviazione, utilizzare gli incrementi elencati nella finestra di dialogo Aumenta la capacità di archiviazione.
- Tempo tra un aumento e l'altro: non è possibile aumentare ulteriormente la capacità di archiviazione su un file system fino a 6 ore dopo l'ultima richiesta di aumento.
- Capacità di throughput: si aumenta automaticamente la capacità di throughput quando si aumenta la capacità di storage. Per i file system HDD persistenti con cache SSD, anche la capacità di archiviazione della cache di lettura viene aumentata in modo analogo per mantenere una cache SSD con dimensioni pari al 20 percento della capacità di archiviazione dell'HDD. Amazon FSx calcola i nuovi valori per le unità di capacità di storage e throughput e li elenca nella finestra di dialogo Incrementa la capacità di storage.

  > **Note**
  >
  > Puoi modificare in modo indipendente la capacità di throughput di un file system persistente basato su SSD senza dover aggiornare la capacità di archiviazione del file system. Per ulteriori informazioni, consulta Gestione della capacità di throughput assegnata.

- Tipo di implementazione: è possibile aumentare la capacità di archiviazione di tutti i tipi di distribuzione ad eccezione dei file system Scratch 1.

Quando aumentare la capacità di archiviazione

Aumenta la capacità di storage del file system quando la capacità di storage disponibile sta per esaurirsi. Utilizza la `FreeStorageCapacity` CloudWatch metrica per monitorare la quantità di spazio di archiviazione gratuito disponibile sul file system. Puoi creare un CloudWatch allarme Amazon in base a questa metrica e ricevere una notifica quando scende al di sotto di una soglia specifica. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.

Puoi utilizzare i CloudWatch parametri per monitorare i livelli di utilizzo del throughput continuo del tuo file system. Se si determina che il file system necessita di una maggiore capacità di throughput, è possibile utilizzare le informazioni relative alle metriche per decidere di quanto aumentare la capacità di storage. Per informazioni su come determinare la velocità effettiva attuale del file system, consulta. Come usare i parametri di Amazon FSx for Lustre CloudWatch Per informazioni su come la capacità di storage influisce sulla capacità di throughput, vedere. Prestazioni FSx di Amazon for Lustre

È inoltre possibile visualizzare la capacità di archiviazione e la velocità effettiva totale del file system nel pannello Riepilogo della pagina dei dettagli del file system.

Come vengono gestite le richieste simultanee di scalabilità dello storage e di backup

È possibile richiedere un backup appena prima dell'inizio di un flusso di lavoro di scalabilità dello storage o mentre è in corso. La sequenza di FSx gestione delle due richieste da parte di Amazon è la seguente:

- Se è in corso un flusso di lavoro di scalabilità dello storage (lo stato di ridimensionamento dello storage è `IN_PROGRESS` uguale allo stato del file system`UPDATING`) e richiedi un backup, la richiesta di backup viene messa in coda. L'attività di backup viene avviata quando il ridimensionamento dello storage è in fase di ottimizzazione dello storage (lo stato di scalabilità dello storage è `UPDATED_OPTIMIZING` e lo stato del file system è). `AVAILABLE`
- Se il backup è in corso (lo stato del backup è`CREATING`) e si richiede il ridimensionamento dello storage, la richiesta di scalabilità dello storage viene messa in coda. Il flusso di lavoro di scalabilità dello storage viene avviato quando Amazon trasferisce il backup su Amazon S3 (lo stato del backup FSx è). `TRANSFERRING`

Se una richiesta di scalabilità dello storage è in sospeso e anche una richiesta di backup del file system è in sospeso, l'attività di backup ha la precedenza maggiore. L'attività di scalabilità dello storage non viene avviata fino al termine dell'attività di backup.

Aumento della capacità di archiviazione

Puoi aumentare la capacità di storage di un file system utilizzando la FSx console Amazon AWS CLI, o l' FSx API Amazon.

Per aumentare la capacità di archiviazione di un file system (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il Lustre file system per cui desideri aumentare la capacità di archiviazione.
3. Per Azioni, scegli Aggiorna capacità di archiviazione. Oppure, nel pannello Riepilogo, scegliete Aggiorna accanto alla capacità di archiviazione del file system per visualizzare la finestra di dialogo Aumenta la capacità di archiviazione.
4. Per la capacità di archiviazione desiderata, fornire una nuova capacità di archiviazione in GiB superiore alla capacità di archiviazione corrente del file system:

   - Per un SSD persistente o un file system scratch 2, questo valore deve essere espresso in multipli di 2400 GiB.
   - Per un file system HDD persistente, questo valore deve essere espresso in multipli di 6000 GiB per file system da 12 MBps /TiB e multipli di 1800 GiB per file system da 40 GiB. MBps
   - Per un file system compatibile con EFA, questo valore deve essere espresso in multipli di 38400 GiB per file system 125 MBps /TiB, multipli di 19200 GiB per file system 250 /TiB, multipli di 9600 GiB per file system 500 MBps /TiB e multipli di 4800 GiB per file system 1000 / TiB. MBps MBps

   > **Note**
   >
   > Non è possibile aumentare la capacità di archiviazione dei file system scratch 1.

5. Scegli Aggiorna per avviare l'aggiornamento della capacità di archiviazione.
6. È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system nella scheda Aggiornamenti.

Per aumentare la capacità di archiviazione per un file system (CLI)

1. Per aumentare la capacità di archiviazione di un file system FSx for Lustre, usa il AWS CLI comando. update-file-system Imposta i seguenti parametri:

   Imposta `--file-system-id` l'ID del file system che stai aggiornando.

   Impostato su `--storage-capacity` un valore intero che rappresenta la quantità, in GiB, dell'aumento della capacità di storage. Per un SSD persistente o un file system scratch 2, questo valore deve essere espresso in multipli di 2400. Per un file system HDD persistente, questo valore deve essere espresso in multipli di 6000 per i file system da 12 MBps /TiB e multipli di 1800 per i file system da 40 /TiB. MBps Il nuovo valore di destinazione deve essere maggiore della capacità di archiviazione corrente del file system.

   Questo comando specifica un valore di destinazione della capacità di archiviazione di 9600 GiB per un SSD persistente o un file system scratch 2.

   ```
   $ aws fsx update-file-system \
       --file-system-id fs-0123456789abcdef0 \
       --storage-capacity 9600
   ```

2. È possibile monitorare l'avanzamento dell'aggiornamento utilizzando il comando. AWS CLI describe-file-systems Cerca il `administrative-actions` nell'output.

   Per ulteriori informazioni, consulta AdministrativeAction.

Monitoraggio dell'aumento della capacità di archiviazione

Puoi monitorare l'avanzamento di un aumento della capacità di storage utilizzando la FSx console Amazon, l'API o il AWS CLI.

Monitoraggio degli aumenti della console

Nella scheda Aggiornamenti della pagina dei dettagli del file system, puoi visualizzare i 10 aggiornamenti più recenti per ogni tipo di aggiornamento.

È possibile visualizzare le seguenti informazioni:

Tipo di aggiornamento

I tipi supportati sono la capacità di archiviazione e l'ottimizzazione dello spazio di archiviazione.

Target value (Valore target)

Il valore desiderato a cui aggiornare la capacità di archiviazione del file system.

Stato

Lo stato attuale della capacità di archiviazione si aggiorna. I valori possibili sono i seguenti:

- In sospeso: Amazon FSx ha ricevuto la richiesta di aggiornamento, ma non ha avviato l'elaborazione.
- In corso: Amazon FSx sta elaborando la richiesta di aggiornamento.
- Aggiornato; ottimizzazione: Amazon FSx ha aumentato la capacità di archiviazione del file system. Il processo di ottimizzazione dello storage sta ora riequilibrando i dati tra i file server.
- Completato: l'aumento della capacità di archiviazione è stato completato con successo.
- Fallito: l'aumento della capacità di archiviazione non è riuscito. Scegli il punto interrogativo (?) per visualizzare i dettagli sul motivo per cui l'aggiornamento dello storage non è riuscito.

Progresso%

Visualizza l'avanzamento del processo di ottimizzazione dello storage come percentuale di completamento.

Orario della richiesta

L'ora in cui Amazon FSx ha ricevuto la richiesta di azione di aggiornamento.

Il monitoraggio aumenta con l'API AWS CLI and

È possibile visualizzare e monitorare le richieste di aumento della capacità di archiviazione del file system utilizzando il describe-file-systems AWS CLI comando e l'azione DescribeFileSystemsAPI. L'`AdministrativeActions`array elenca le 10 azioni di aggiornamento più recenti per ogni tipo di azione amministrativa. Quando si aumenta la capacità di archiviazione di un file system, `AdministrativeActions` ne vengono generate due: una `FILE_SYSTEM_UPDATE` e un'`STORAGE_OPTIMIZATIO`Nazione.

L'esempio seguente mostra un estratto della risposta di un comando CLIdescribe-file-systems. Il file system ha una capacità di archiviazione di 4800 GB ed è in corso un'azione amministrativa per aumentare la capacità di archiviazione a 9600 GB.

```
{
    "FileSystems": [
        {
```

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

Amazon FSx elabora prima l'`FILE_SYSTEM_UPDATE`azione, aggiungendo nuovi file server al file system. Quando il nuovo storage è disponibile per il file system, lo `FILE_SYSTEM_UPDATE` stato cambia in`UPDATED_OPTIMIZING`. La capacità di storage mostra il nuovo valore più elevato e Amazon FSx inizia a elaborare l'azione `STORAGE_OPTIMIZATION` amministrativa. Questo è mostrato nel seguente estratto della risposta di un comando CLIdescribe-file-systems.

La `ProgressPercent` proprietà mostra lo stato di avanzamento del processo di ottimizzazione dello storage. Una volta completato correttamente il processo di ottimizzazione dello storage, lo stato dell'`FILE_SYSTEM_UPDATE`azione cambia in `COMPLETED` e l'`STORAGE_OPTIMIZATIO`Nazione non viene più visualizzata.

```
{
    "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,
                }
            ]
```

Se l'aumento della capacità di archiviazione fallisce, lo stato dell'`FILE_SYSTEM_UPDATE`azione cambia in`FAILED`. La `FailureDetails` proprietà fornisce informazioni sull'errore, illustrate nell'esempio seguente.

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

Gestione della cache di lettura SSD fornita

Quando crei un file system con la classe di storage Intelligent-Tiering, hai la possibilità di fornire anche una cache di lettura basata su SSD che fornisce latenze SSD per la lettura dei dati a cui accedi di frequente, fino a 3 IOPS per GiB.

È possibile configurare la cache di lettura SSD per i dati a cui si accede di frequente con una di queste opzioni di modalità di dimensionamento:

- Automatico (proporzionale alla capacità di throughput). Con Automatic, Amazon FSx for Lustre seleziona automaticamente la dimensione della cache di lettura dei dati SSD in base alla capacità di throughput assegnata.
- Personalizzato (fornito dall'utente). Con Custom, puoi personalizzare le dimensioni della cache di lettura dell'SSD e aumentarla o ridurla in qualsiasi momento in base alle esigenze del tuo carico di lavoro.
- Scegli No Cache se non desideri utilizzare una cache di lettura dei dati SSD con il tuo file system.

In modalità Automatica (proporzionale alla capacità di throughput), Amazon fornisce FSx automaticamente le seguenti dimensioni predefinite della cache di lettura in base alla capacità di throughput del file system.

Capacità di throughput fornita () MBps	Cache di lettura SSD in modalità automatica (proporzionale alla capacità di trasmissione) (GiB)	Dimensioni della cache di lettura SSD supportate	
		minimo (GiB)	massimo (GiB)
Ogni 4000	20000	32	131072

Dopo aver creato il file system, puoi modificare la modalità di dimensionamento e la capacità di archiviazione della cache di lettura in qualsiasi momento.

Argomenti

Considerazioni sull'aggiornamento della cache di lettura SSD

Ecco alcune considerazioni importanti da fare quando si modifica la cache di lettura dei dati SSD:

- Ogni volta che modifichi la cache di lettura dell'SSD, tutti i suoi contenuti verranno cancellati. Ciò significa che potresti notare una diminuzione dei livelli di prestazioni fino a quando la cache di lettura dell'SSD non verrà nuovamente popolata.
- È possibile aumentare o diminuire le dimensioni della capacità di una cache di lettura SSD. Tuttavia, è possibile eseguire questa operazione solo una volta ogni sei ore. Non ci sono limiti di tempo per aggiungere o rimuovere una cache di lettura SSD dal file system.
- È necessario aumentare o diminuire le dimensioni della cache di lettura SSD di almeno il 10% ogni volta che la si modifica.

Aggiornamento di una cache di lettura SSD fornita

Puoi aggiornare la cache di lettura dei dati SSD utilizzando la FSx console Amazon AWS CLI, o l' FSx API Amazon.

Per aggiornare la cache di lettura SSD per un file system Intelligent-Tiering (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione a sinistra, scegli File system. Nell'elenco File system, scegli il file system FSx for Lustre per cui desideri aggiornare la cache di lettura SSD.
3. SSD Nel pannello Riepilogo, scegli Aggiorna accanto al valore della cache di lettura SSD del file system.

   Viene visualizzata la finestra di dialogo Aggiorna cache di lettura SSD.

4. Seleziona la nuova modalità di dimensionamento che desideri per la cache di lettura dei dati, come segue:

   - Scegli Automatico (proporzionale alla capacità di trasmissione) per far sì che la cache di lettura dei dati venga ridimensionata automaticamente in base alla capacità di throughput.
   - Scegli Personalizzato (fornito dall'utente) se conosci la dimensione approssimativa del tuo set di dati e desideri personalizzare la cache di lettura dei dati. Se si seleziona Personalizzato, sarà inoltre necessario specificare la capacità della cache di lettura desiderata in GiB.
   - Scegli Nessuno se non desideri utilizzare una cache di lettura dei dati SSD con il tuo file system Intelligent-Tiering.

5. Scegli Aggiorna.

Per aggiornare la cache di lettura SSD per un file system (CLI) Intelligent-Tiering

Per aggiornare la cache di lettura dei dati SSD per un file system Intelligent-Tiering, utilizza il comando o l'azione API equivalente. AWS CLI update-file-system UpdateFileSystem Imposta i seguenti parametri:

- Imposta `--file-system-id` l'ID del file system che stai aggiornando.
- Per modificare la cache di lettura dell'SSD, utilizza la `--lustre-configuration DataReadCacheConfiguration` proprietà. Questa proprietà ha due parametri `SizeGiB eSizingMode`:
  - SizeGiB - Imposta la dimensione della cache di lettura SSD in GiB quando si `USER_PROVISIONED` utilizza la modalità.
  - SizingMode- Imposta la modalità di dimensionamento della cache di lettura SSD.
    - Impostare su `NO_CACHE` se non si desidera utilizzare una cache di lettura SSD con il file system Intelligent-Tiering.
    - Imposta su `USER_PROVISIONED` per specificare la dimensione esatta della cache di lettura dell'SSD.
    - Imposta per `PROPORTIONAL_TO_THROUGHPUT_CAPACITY` far sì che la cache di lettura dei dati SSD venga ridimensionata automaticamente in base alla capacità di throughput.

L'esempio seguente aggiorna la cache di lettura SSD alla `USER_PROVISIONED` modalità e imposta la dimensione su 524288 GiB.

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

Per monitorare lo stato di avanzamento dell'aggiornamento, utilizzare il comando. describe-file-systems AWS CLI Cerca la `AdministrativeActions` sezione nell'output.

Per ulteriori informazioni, AdministrativeActionconsulta Amazon FSx API Reference.

Monitoraggio degli aggiornamenti della cache di lettura degli SSD

Puoi monitorare l'avanzamento di un aggiornamento della cache di lettura SSD utilizzando la FSx console Amazon, l'API o il AWS CLI.

Monitoraggio degli aggiornamenti nella console

È possibile monitorare gli aggiornamenti del file system nella scheda Aggiornamenti della pagina dei dettagli del file system.

Per gli aggiornamenti della cache di lettura SSD, puoi visualizzare le seguenti informazioni:

Tipo di aggiornamento

I tipi supportati sono la modalità di dimensionamento della cache di lettura SSD e la dimensione della cache di lettura SSD.

Target value (Valore target)

Il valore aggiornato per la modalità di dimensionamento della cache di lettura SSD o la dimensione della cache di lettura SSD del file system.

Stato

Lo stato attuale dell'aggiornamento. I valori possibili sono i seguenti:

- In sospeso: Amazon FSx ha ricevuto la richiesta di aggiornamento, ma non ha avviato l'elaborazione.
- In corso: Amazon FSx sta elaborando la richiesta di aggiornamento.
- Completato: l'aggiornamento è stato completato con successo.

- Fallita: la richiesta di aggiornamento non è riuscita. Scegli il punto interrogativo (?) per visualizzare i dettagli sul motivo per cui la richiesta non è riuscita.

Orario della richiesta

L'ora in cui Amazon FSx ha ricevuto la richiesta di azione di aggiornamento.

Monitoraggio degli aggiornamenti della cache di lettura dell'SSD con l'API AWS CLI and

È possibile visualizzare e monitorare le richieste di aggiornamento della cache di lettura SSD del file system utilizzando il describe-file-systems AWS CLI comando e l'operazione DescribeFileSystemsAPI. L'`AdministrativeActions`array elenca le 10 azioni di aggiornamento più recenti per ogni tipo di azione amministrativa. Quando si aggiorna la cache di lettura SSD di un file system, `FILE_SYSTEM_UPDATE` `AdministrativeActions` viene generato un.

L'esempio seguente mostra un estratto della risposta di un comando CLI`describe-file-systems`. Il file system ha un'azione amministrativa in sospeso per modificare la modalità di dimensionamento della cache di lettura SSD `USER_PROVISIONED` e la dimensione della cache di lettura SSD su 524288.

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

Quando la nuova configurazione della cache di lettura SSD è disponibile per il file system, lo stato cambia in. `FILE_SYSTEM_UPDATE` `COMPLETED` Se la richiesta di aggiornamento della cache di lettura SSD non riesce, lo stato dell'`FILE_SYSTEM_UPDATE`azione cambia in. `FAILED`

Gestione delle prestazioni dei metadati

Puoi aggiornare la configurazione dei metadati del tuo file system FSx for Lustre senza interruzioni per gli utenti finali o le applicazioni utilizzando la console Amazon FSx , l' FSx API Amazon o AWS Command Line Interface ().AWS CLI La procedura di aggiornamento aumenta il numero di IOPS di metadati assegnati per il file system.

> **Note**
>
> I metadati avanzati sono disponibili solo per i file system 2.15. È possibile aumentare le prestazioni dei metadati solo sui FSx file system Lustre creati con il tipo di distribuzione Persistent 2 e una configurazione di metadati specificata. Non è possibile aggiungere o aggiornare la configurazione dei metadati per un file system FSx for Lustre se la configurazione dei metadati non è specificata al momento della creazione del file system. Ciò vale anche per i file system ripristinati dai backup dei file system 2.12 che non supportavano prestazioni migliorate dei metadati o dai file system 2.15 per i quali non era specificata alcuna configurazione dei metadati.

Le migliori prestazioni dei metadati del file system sono disponibili per l'uso in pochi minuti. È possibile aggiornare le prestazioni dei metadati in qualsiasi momento, a condizione che le richieste di aumento delle prestazioni dei metadati avvengano a distanza di almeno 6 ore. Durante la scalabilità delle prestazioni dei metadati, il file system potrebbe non essere disponibile per alcuni minuti. Le operazioni sui file eseguite dai client mentre il file system non è disponibile riproveranno in modo trasparente e alla fine avranno esito positivo una volta completata la scalabilità delle prestazioni dei metadati. Ti verrà addebitato il costo del nuovo aumento delle prestazioni dei metadati non appena questi saranno disponibili.

Puoi monitorare l'avanzamento di un aumento delle prestazioni dei metadati in qualsiasi momento utilizzando la FSx console Amazon, la CLI e l'API. Per ulteriori informazioni, consulta Monitoraggio degli aggiornamenti della configurazione dei metadati.

Argomenti

- Lustreconfigurazione delle prestazioni dei metadati
- Considerazioni sull'aumento delle prestazioni dei metadati
- Quando aumentare le prestazioni dei metadati
- Aumento delle prestazioni dei metadati

- Modifica della modalità di configurazione dei metadati
- Monitoraggio degli aggiornamenti della configurazione dei metadati

Lustreconfigurazione delle prestazioni dei metadati

Il numero di IOPS di metadati assegnati determina la velocità massima di operazioni sui metadati che può essere supportata dal file system.

Quando create il file system, scegliete una modalità di configurazione dei metadati:

- Per i file system SSD, puoi scegliere la modalità Automatica se desideri che Amazon FSx fornisca e ridimensioni automaticamente gli IOPS dei metadati sul tuo file system in base alla capacità di storage del file system. Tieni presente che i file system Intelligent-Tiering non supportano la modalità automatica.
- Per i file system SSD, puoi scegliere User-provisioned se desideri specificare il numero di IOPS di metadati da fornire per il tuo file system.
- Per i file system Intelligent-Tiering, è necessario scegliere la modalità User-provisioned. Con la modalità User-provisioned, è possibile specificare il numero di IOPS di metadati da fornire per il file system.

Sui file system SSD, puoi passare dalla modalità Automatica alla modalità User-provisioned in qualsiasi momento. È inoltre possibile passare dalla modalità User-Provisioned alla modalità Automatica se il numero di IOPS di metadati forniti sul file system corrisponde al numero predefinito di IOPS di metadati forniti in modalità Automatica. I file system Intelligent-Tiering supportano solo la modalità User-provisioned, quindi non è possibile cambiare modalità di configurazione dei metadati.

I valori IOPS dei metadati validi sono i seguenti:

- Per i file system SSD, i valori IOPS dei metadati validi sono 1500, 3000, 6000 e multipli di 12000 fino a un massimo di 192000.
- Per i file system Intelligent-Tiering, i valori IOPS dei metadati validi sono 6000 e 12000.

Se le prestazioni dei metadati del carico di lavoro superano il numero di IOPS di metadati forniti in modalità automatica, puoi utilizzare la modalità User-provisioned per aumentare il valore IOPS dei metadati per il tuo file system.

È possibile visualizzare il valore corrente della configurazione del server di metadati del file system nel modo seguente:

- Utilizzo della console: nel pannello Riepilogo della pagina dei dettagli del file system, il campo Metadata IOPS mostra il valore corrente dell'IOPS dei metadati fornito e la modalità di configurazione dei metadati corrente del file system.
- Utilizzo della CLI o dell'API: utilizza il comando describe-file-systemsCLI o l'operazione DescribeFileSystemsAPI e cerca la proprietà. `MetadataConfiguration`

Considerazioni sull'aumento delle prestazioni dei metadati

Ecco alcune considerazioni importanti su come aumentare le prestazioni dei metadati:

- Solo aumento delle prestazioni dei metadati: è possibile solo aumentare il numero di IOPS dei metadati per un file system; non è possibile diminuire il numero di IOPS dei metadati.
- La specificazione degli IOPS dei metadati in modalità automatica non è supportata: non è possibile specificare il numero di IOPS dei metadati su un file system in modalità automatica. Dovrai passare alla modalità User-provisioned e quindi effettuare la richiesta. Per ulteriori informazioni, consulta Modifica della modalità di configurazione dei metadati.
- Metadata IOPS per i dati scritti prima del ridimensionamento: quando si scalano Metadata IOPS oltre 12000, FSx for Lustre aggiunge nuovi server di metadati al file system. I nuovi metadati vengono distribuiti automaticamente su tutti i server per migliorare le prestazioni. Tuttavia, i metadati e le sottodirectory esistenti creati prima del ridimensionamento rimangono sui server originali, senza alcun aumento degli IOPS dei metadati.
- Tempo tra un aumento e l'altro: non è possibile aumentare ulteriormente le prestazioni dei metadati su un file system fino a 6 ore dopo l'ultima richiesta di aumento.
- Aumento simultaneo delle prestazioni dei metadati e dello storage SSD: non è possibile scalare contemporaneamente le prestazioni dei metadati e la capacità di storage del file system.

Quando aumentare le prestazioni dei metadati

Aumenta il numero di IOPS di metadati quando devi eseguire carichi di lavoro che richiedono livelli di prestazioni dei metadati più elevati di quelli forniti di default sul tuo file system. È possibile monitorare le prestazioni dei metadati AWS Management Console utilizzando il `Metadata IOPS Utilization` grafico che fornisce la percentuale delle prestazioni del server di metadati predisposto che si sta consumando sul file system.

È inoltre possibile monitorare le prestazioni dei metadati utilizzando metriche più granulari. CloudWatch CloudWatch le metriche includono `DiskReadOperations` `eDiskWriteOperations`, che forniscono il volume delle operazioni del server di metadati che richiedono l'I/O del disco, nonché metriche granulari per le operazioni sui metadati, tra cui creazione, statistiche, letture ed eliminazioni di file e directory. Per ulteriori informazioni, consulta FSx per le metriche dei metadati Lustre.

Aumento delle prestazioni dei metadati

Puoi aumentare le prestazioni dei metadati di un file system utilizzando la FSx console Amazon AWS CLI, o l' FSx API Amazon.

Per aumentare le prestazioni dei metadati per un file system (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione a sinistra, scegli File system. Nell'elenco File system, scegli il file system FSx for Lustre per cui desideri aumentare le prestazioni dei metadati.
3. Per Azioni, scegliete Aggiorna metadati IOPS. Oppure, nel pannello Riepilogo, scegliete Aggiorna accanto al campo IOPS dei metadati del file system.

   Viene visualizzata la finestra di dialogo Aggiorna metadati IOPS.
4. Scegliete User-provisioned.
5. Per Desired Metadata IOPS, scegliete il nuovo valore Metadata IOPS. Il valore immesso deve essere maggiore o uguale al valore IOPS di Metadata corrente.

   - Per i file system SSD, i valori validi sono`1500`,`3000`, `600012000`, e multipli `12000` fino a un massimo di. `192000`
   - Per i file system Intelligent-Tiering, i valori validi sono e. `6000` `12000`
6. Scegli Aggiorna.

Per aumentare le prestazioni dei metadati per un file system (CLI)

Per aumentare le prestazioni dei metadati per un file system FSx for Lustre, utilizzate il AWS CLI comando update-file-system(UpdateFileSystem è l'azione API equivalente). Imposta i seguenti parametri:

- Imposta `--file-system-id` l'ID del file system che stai aggiornando.
- Per aumentare le prestazioni dei metadati, utilizzate la `--lustre-configuration` `MetadataConfiguration` proprietà. Questa proprietà ha due parametri, `Mode` `eIops`.

1. Se il file system è in modalità USER_PROVISIONED, l'utilizzo `Mode` è facoltativo (se utilizzato, impostato su`Mode`). `USER_PROVISIONED`

   Se il file system SSD è in modalità AUTOMATICA, imposta su `Mode` `USER_PROVISIONED` (che commuta la modalità del file system su USER_PROVISIONED oltre ad aumentare il valore IOPS dei metadati).
2. Per i file system SSD, imposta un valore di, `1500` `30006000`, `12000` o multipli `Iops` fino a un massimo di. `12000` `192000` Per i file system Intelligent-Tiering, impostate su o. `Iops` `6000` `12000` Il valore immesso deve essere maggiore o uguale al valore IOPS dei metadati corrente.

L'esempio seguente aggiorna gli IOPS dei metadati assegnati a 12000.

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

Modifica della modalità di configurazione dei metadati

Per i file system basati su SSD, è possibile modificare la modalità di configurazione dei metadati di un file system esistente utilizzando la console AWS e la CLI, come spiegato nelle procedure seguenti.

Quando si passa dalla modalità Automatica alla modalità User-provisioned, è necessario fornire un valore IOPS dei metadati maggiore o uguale al valore IOPS dei metadati del file system corrente.

Se richiedi di passare dalla modalità User-provisioned alla modalità Automatica e il valore corrente di Metadata IOPS è superiore a quello predefinito automatizzato, Amazon FSx rifiuta la richiesta, perché il downscaling degli IOPS dei metadati non è supportato. Per sbloccare il cambio di modalità, devi aumentare la capacità di archiviazione in modo che corrisponda agli attuali IOPS dei metadati in modalità automatica per abilitare nuovamente il cambio di modalità.

Puoi modificare la modalità di configurazione dei metadati di un file system utilizzando la FSx console Amazon AWS CLI, o l' FSx API Amazon.

Per modificare la modalità di configurazione dei metadati per un file system (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione a sinistra, scegli File system. Nell'elenco File system, scegli il file system FSx for Lustre per cui desideri modificare la modalità di configurazione dei metadati.

3. Per Azioni, scegliete Aggiorna metadati IOPS. Oppure, nel pannello Riepilogo, scegliete Aggiorna accanto al campo IOPS dei metadati del file system.

   Viene visualizzata la finestra di dialogo Aggiorna metadati IOPS.

4. Scegli una delle seguenti operazioni.

   - Per passare dalla modalità User-provisioned alla modalità Automatica, scegliete Automatico.
   - Per passare dalla modalità Automatica alla modalità User-Provisioned, scegliete User-Provisioned. Quindi, per Desired Metadata IOPS, fornite un valore IOPS dei metadati maggiore o uguale al valore IOPS dei metadati del file system corrente.

5. Scegli Aggiorna.

Per modificare la modalità di configurazione dei metadati per un file system SSD (CLI)

Per modificare la modalità di configurazione dei metadati per un SSD FSx for Lustre file system, usa il AWS CLI comando update-file-system(UpdateFileSystem è l'azione API equivalente). Imposta i seguenti parametri:

- Imposta `--file-system-id` l'ID del file system che stai aggiornando.
- Per modificare la modalità di configurazione dei metadati sui file system basati su SSD, utilizzate la proprietà. `--lustre-configuration MetadataConfiguration` Questa proprietà ha due parametri, e. `Mode Iops`
  - Per passare dal file system SSD alla modalità AUTOMATIC alla modalità `USER_PROVISIONED` USER_PROVISIONED, `Mode` impostate un valore IOPS dei metadati maggiore o uguale `Iops` al valore IOPS dei metadati del file system corrente. Per esempio:

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

  - Per passare dalla modalità USER_PROVISIONED alla modalità AUTOMATIC, impostate e non utilizzate il parametro. `Mode AUTOMATIC Iops` Per esempio:

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

Monitoraggio degli aggiornamenti della configurazione dei metadati

Puoi monitorare lo stato di avanzamento degli aggiornamenti della configurazione dei metadati utilizzando la FSx console Amazon, l'API o il AWS CLI.

Monitoraggio degli aggiornamenti della configurazione dei metadati (console)

È possibile monitorare gli aggiornamenti della configurazione dei metadati nella scheda Aggiornamenti della pagina dei dettagli del file system.

Per gli aggiornamenti della configurazione dei metadati, è possibile visualizzare le seguenti informazioni:

Tipo di aggiornamento

I tipi supportati sono Metadata IOPS e Metadata configuration mode.

Target value (Valore target)

Il valore aggiornato per la modalità di configurazione Metadata IOPS o Metadata del file system.

Stato

Lo stato attuale dell'aggiornamento. I valori possibili sono i seguenti:

- In sospeso: Amazon FSx ha ricevuto la richiesta di aggiornamento, ma non ha avviato l'elaborazione.
- In corso: Amazon FSx sta elaborando la richiesta di aggiornamento.
- Completato: l'aggiornamento è stato completato con successo.
- Fallita: la richiesta di aggiornamento non è riuscita. Scegli il punto interrogativo (?) per visualizzare i dettagli sul motivo per cui la richiesta non è riuscita.

Orario della richiesta

L'ora in cui Amazon FSx ha ricevuto la richiesta di azione di aggiornamento.

Monitoraggio degli aggiornamenti della configurazione dei metadati (CLI)

È possibile visualizzare e monitorare le richieste di aggiornamento della configurazione dei metadati utilizzando il describe-file-systems AWS CLI comando e l'DescribeFileSystemsoperazione API. L'`AdministrativeActions`array elenca le 10 azioni di aggiornamento più recenti per ogni tipo di

azione amministrativa. Quando si aggiorna la modalità di configurazione o le prestazioni dei metadati di un file system, `FILE_SYSTEM_UPDATE` `AdministrativeActions` viene generato un.

L'esempio seguente mostra un estratto della risposta di un comando CLI`describe-file-systems`. Il file system ha un'azione amministrativa in sospeso per aumentare l'IOPS dei metadati a 96000 e la modalità di configurazione dei metadati a USER_PROVISIONED.

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

Amazon FSx elabora l'`FILE_SYSTEM_UPDATE`azione, modificando gli IOPS dei metadati del file system e la modalità di configurazione dei metadati. Quando le nuove risorse di metadati sono disponibili per il file system, lo stato cambia in. `FILE_SYSTEM_UPDATE` `COMPLETED`

Se la richiesta di aggiornamento della configurazione dei metadati fallisce, lo stato dell'`FILE_SYSTEM_UPDATE`azione cambia in`FAILED`, come illustrato nell'esempio seguente. La `FailureDetails` proprietà fornisce informazioni sull'errore.

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

```
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

Gestione della capacità di throughput assegnata

Ogni file system FSx for Lustre ha una capacità di throughput che viene configurata al momento della creazione del file system. Per i file system che utilizzano l'archiviazione SSD o HDD, la capacità di trasmissione viene misurata in megabyte al secondo per 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/Ooperazioni al secondo (IOPS) e maggiore memoria per la memorizzazione nella cache dei dati sul file server. Per ulteriori informazioni, consulta Prestazioni FSx di Amazon for Lustre.

È possibile modificare il livello di throughput di un file system persistente basato su SSD aumentando o diminuendo il valore della velocità effettiva del file system per unità di storage. I valori validi dipendono dal tipo di distribuzione del file system, come segue:

- Per i tipi di distribuzione basati su SSD Persistent 1, i valori validi sono 50, 100 e 200 /TiB. MBps
- Per i tipi di distribuzione basati su SSD Persistent 2, i valori validi sono 125, 250, 500 e 1000 /TiB. MBps

È possibile modificare la capacità di throughput di un file system Intelligent-Tiering aumentando il valore della capacità di throughput totale per il file system. I valori validi sono 4.000 MBps o incrementi di 4.000, fino a un massimo di 2.000.000. MBps MBps

È possibile visualizzare il valore corrente della capacità di trasmissione del file system nel modo seguente:

- Utilizzo della console: nel pannello Riepilogo della pagina dei dettagli del file system, il campo Throughput per unità di storage mostra il valore corrente per i file system basati su SSD, mentre il campo Throughput capacity mostra il valore corrente per i file system Intelligent-Tiering.

- Utilizzo della CLI o dell'API: utilizza il comando describe-file-systemsCLI o l'operazione DescribeFileSystemsAPI e cerca la proprietà. `PerUnitStorageThroughput`

Quando modifichi la capacità di throughput del tuo file system, dietro le quinte, Amazon FSx disattiva i file server del file system sui file system SSD o aggiunge nuovi file server sui file system Intelligent-Tiering. Il file system non sarà disponibile per alcuni minuti durante la scalabilità della capacità di throughput. Ti verrà addebitata la nuova quantità di capacità di throughput non appena sarà disponibile per il tuo file system.

Argomenti

Considerazioni relative all'aggiornamento della capacità di throughput

Di seguito sono riportati alcuni elementi importanti da considerare quando si aggiorna la capacità di throughput:

- Aumentare o diminuire: è possibile aumentare o diminuire la quantità di capacità di trasmissione per un file system basato su SSD. È possibile solo aumentare la quantità di capacità di throughput per un file system Intelligent-Tiering.
- Aggiorna incrementi: quando modificate la capacità di throughput, utilizzate gli incrementi elencati nella finestra di dialogo Update throughput tier per i file system basati su SSD o nella finestra di dialogo Update throughput capacity per i file system Intelligent-Tiering.
- Tempo tra un aumento e l'altro: non è possibile apportare ulteriori modifiche alla capacità di throughput su un file system fino a 6 ore dopo l'ultima richiesta o fino al completamento del processo di ottimizzazione del throughput, a seconda di quale periodo sia più lungo.
- Ridimensionamento automatico della cache di lettura SSD: per la modalità predefinita della cache di lettura SSD (proporzionale alla capacità di throughput), Amazon fornisce automaticamente FSx 5 GiB di storage di dati per ogni capacità di throughput fornita. MBps Man mano che aumenti la capacità di throughput del tuo file system, Amazon ridimensiona FSx automaticamente la cache di dati SSD collegando ulteriore spazio di archiviazione cache a tutti i file server appena aggiunti.

- Tipo di distribuzione: puoi aggiornare la capacità di throughput solo dei tipi di distribuzione persistenti basati su SSD o Intelligent-Tiering. Non è possibile modificare la capacità di throughput dei file system basati su SSD abilitati per EFA.

Quando modificare la capacità di throughput

Amazon FSx si integra con Amazon CloudWatch, consentendoti di monitorare i livelli di utilizzo del throughput continuo del tuo file system. Le prestazioni (throughput e IOPS) che puoi ottenere attraverso il tuo file system dipendono dalle caratteristiche specifiche del carico di lavoro, oltre che dalla capacità di throughput, dalla capacità di storage e dalla classe di storage del file system. Per informazioni su come determinare la velocità effettiva attuale del file system, consulta. Come usare i parametri di Amazon FSx for Lustre CloudWatch Per informazioni sulle CloudWatch metriche, consulta. Monitoraggio con Amazon CloudWatch

Modifica della capacità di throughput

Puoi modificare la capacità di throughput di un file system FSx for Lustre utilizzando la FSx console Amazon, AWS Command Line Interface (AWS CLI) o l'API Amazon FSx .

Per modificare la capacità di trasmissione di un file system SSD (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il file system FSx for Lustre per cui desideri modificare la capacità di throughput.
3. Per Azioni, scegliete Update throughput tier. Oppure, nel pannello Riepilogo, scegliete Aggiorna accanto al Throughput per unità di storage del file system.

   Viene visualizzata la finestra Update throughput tier.
4. Scegli il nuovo valore per Throughput desiderato per unità di storage dall'elenco.
5. Scegliete Aggiorna per avviare l'aggiornamento della capacità di throughput.

> **Note**
>
> Il file system potrebbe subire un periodo di indisponibilità molto breve durante l'aggiornamento.

Per modificare la capacità di throughput (CLI) di un file system SSD

- Per modificare la capacità di throughput di un file system, utilizzate il comando update-file-systemCLI (o l'operazione API UpdateFileSystemequivalente). Imposta i seguenti parametri:
  - Imposta `--file-system-id` l'ID del file system che stai aggiornando.
  - Imposta su `--lustre-configuration PerUnitStorageThroughput` un valore di `50100`, o `200` MBps/TiB per i file system SSD Persistent 1, o su un valore di`125`, `250500`, o `1000` MBps/TiB per i file system SSD Persistent 2.

  Questo comando specifica che la capacità di throughput deve essere impostata su 1000 MBps / TiB per il file system.

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

Per modificare la capacità di throughput di un file system Intelligent-Tiering (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il file system FSx for Lustre per cui desideri modificare la capacità di throughput.
3. Per Azioni, scegliete Aggiorna la capacità di trasmissione. Oppure, nel pannello Riepilogo, scegliete Aggiorna accanto alla capacità di throughput del file system.

   Viene visualizzata la finestra di dialogo Aggiorna capacità di trasmissione.
4. Scegliete il nuovo valore per Capacità di trasmissione desiderata dall'elenco.

   Amazon FSx ridimensionerà automaticamente la cache di lettura dei dati per evitare di svuotarne il contenuto.
5. Scegli Aggiorna per avviare l'aggiornamento della capacità di throughput.

> **Note**
>
> Il file system potrebbe subire un periodo di indisponibilità molto breve durante l'aggiornamento.

Per modificare la capacità di throughput (CLI) di un file system Intelligent-Tiering

- Per modificare la capacità di throughput di un file system, utilizzate il comando update-file-systemCLI (o l'operazione API UpdateFileSystemequivalente). Imposta i seguenti parametri:
  - Imposta `--file-system-id` l'ID del file system che stai aggiornando.
  - Se la cache di lettura dei dati è configurata in modo proporzionale alla modalità di capacità di trasmissione, impostala su `--lustre-configuration ThroughputCapacity` un livello di throughput con incrementi di `4000` MBps, fino a un massimo di. `2000000` MBps

    Se la cache di lettura dei dati è configurata in modalità fornita dall'utente, è inoltre necessario utilizzare la `--lustre-configuration DataReadCacheConfiguration` proprietà per specificare la cache di lettura dei dati. È necessario mantenere lo stesso rapporto di archiviazione della cache per server e specificare il nuovo SizeGi B, altrimenti la richiesta verrà rifiutata.

Questo comando specifica che la capacità di throughput deve essere impostata su 8000 MBps per un file system che utilizza una cache di lettura configurata in modo proporzionale alla modalità di capacità di throughput.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration '{
      "ThroughputCapacity": 8000
      }'
```

Questo comando specifica che la capacità di throughput deve essere impostata su 8000 MBps per un file system che utilizza una cache di lettura configurata in modalità fornita dall'utente.

```
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
         }
```

```
}'
```

Monitoraggio delle variazioni della capacità di throughput

Puoi monitorare lo stato di avanzamento di una modifica della capacità di throughput utilizzando la FSx console Amazon, l'API e il AWS CLI.

Monitoraggio delle variazioni della capacità di throughput (console)

- Nella scheda Aggiornamenti della pagina dei dettagli del file system, è possibile visualizzare le 10 azioni di aggiornamento più recenti per ogni tipo di azione di aggiornamento.

  Per le azioni di aggiornamento della capacità di throughput, è possibile visualizzare le seguenti informazioni.

  Tipo di aggiornamento

  Il tipo supportato è Throughput di storage per unità.

  Target value (Valore target)

  Il valore desiderato su cui modificare la velocità effettiva del file system per unità di storage.

  Stato

  Lo stato attuale dell'aggiornamento. Per gli aggiornamenti della capacità di throughput, i valori possibili sono i seguenti:

  - In sospeso: Amazon FSx ha ricevuto la richiesta di aggiornamento, ma non ha avviato l'elaborazione.
  - In corso: Amazon FSx sta elaborando la richiesta di aggiornamento.
  - Aggiornato; ottimizzazione: Amazon FSx ha aggiornato le 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 prestazioni di rete del file system tra il livello precedente e il nuovo livello fino a quando il file system non si trova più in questo stato.
  - Completato: l'aggiornamento della capacità di throughput è stato completato con successo.
  - Non riuscito: l'aggiornamento della capacità di throughput non è riuscito. Scegli il punto interrogativo (?) per visualizzare i dettagli sul motivo per cui l'aggiornamento del throughput non è riuscito.

Orario della richiesta

L'ora in cui Amazon FSx ha ricevuto la richiesta di aggiornamento.

Monitoraggio degli aggiornamenti del file system (CLI)

- È possibile visualizzare e monitorare le richieste di modifica della capacità di throughput del file system utilizzando il comando describe-file-systemsCLI e DescribeFileSystemsl'azione API. L'`AdministrativeActions`array elenca le 10 azioni di aggiornamento più recenti per ogni tipo di azione amministrativa. Quando si modifica la capacità di throughput di un file system, viene generata un'azione `FILE_SYSTEM_UPDATE` amministrativa.

  L'esempio seguente mostra l'estratto della risposta di un comando CLI`describe-file-systems`. Il file system ha un throughput di destinazione per unità di storage di 500 MBps /TiB.

```
.
.
.
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "LustreConfiguration": {
            "PerUnitStorageThroughput": 500
          }
        }
    }
]
```

  Quando Amazon FSx elabora correttamente l'azione, lo stato cambia in`COMPLETED`. La nuova capacità di throughput è quindi disponibile per il file system e viene visualizzata nella `PerUnitStorageThroughput` proprietà.

  Se la modifica della capacità di throughput non riesce, lo stato cambia e la `FailureDetails` proprietà fornisce informazioni sull'errore. `FAILED`

Lustrecompressione dei dati

Puoi utilizzare la funzionalità di compressione Lustre dei dati per ottenere risparmi sui costi dei file system e dello storage di backup Amazon FSx for Lustre ad alte prestazioni. Quando la compressione dei dati è abilitata, Amazon FSx for Lustre comprime automaticamente i file appena scritti prima che vengano scritti su disco e li decomprime automaticamente quando vengono letti.

La compressione dei dati utilizza l' LZ4 algoritmo, ottimizzato per fornire alti livelli di compressione senza influire negativamente sulle prestazioni del file system. LZ4 è un algoritmo Lustre affidabile e orientato alle prestazioni che fornisce un equilibrio tra velocità di compressione e dimensioni dei file compressi. L'abilitazione della compressione dei dati in genere non ha un impatto misurabile sulla latenza.

La compressione dei dati riduce la quantità di dati trasferiti tra i file server e lo storage Amazon FSx for Lustre. Se non utilizzi già formati di file compressi, noterai un aumento della capacità di trasmissione complessiva del file system quando utilizzi la compressione dei dati. Gli aumenti della capacità di trasmissione correlati alla compressione dei dati verranno limitati dopo la saturazione delle schede di interfaccia di rete front-end.

Ad esempio, se il file system è un tipo di implementazione SSD PERSISTENT-50, il throughput di rete ha una linea di base di 250 MBps per TiB di storage. La velocità effettiva del disco ha una linea di base di 50 per MBps TiB. Con la compressione dei dati, la velocità effettiva del disco potrebbe aumentare da 50 MBps per TiB a un massimo di 250 MBps per TiB, che è il limite di throughput di rete di base. Per ulteriori informazioni sui limiti di velocità effettiva della rete e del disco, consulta le tabelle delle prestazioni del file system in. Caratteristiche prestazionali delle classi di storage SSD e HDD Per ulteriori informazioni sulle prestazioni di compressione dei dati, consulta il post Spendi meno aumentando le prestazioni con la compressione Amazon FSx for Lustre dei dati sullo AWS Storage Blog.

Argomenti

Gestione della compressione dei dati

Puoi attivare o disattivare la compressione dei dati quando crei un nuovo file system Amazon FSx for Lustre. La compressione dei dati è disattivata per impostazione predefinita quando crei un file system Amazon FSx for Lustre dalla console o dall'API. AWS CLI

Per attivare la compressione dei dati durante la creazione di un file system (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo file system descritta Passaggio 1: crea il tuo FSx file system for Lustre nella sezione Guida introduttiva.
3. Nella sezione Dettagli del file system, per Tipo di compressione dei dati, scegli LZ4.
4. Completa la procedura guidata come quando crei un nuovo file system.
5. Scegliere Review and create (Rivedi e crea).
6. Controlla le impostazioni che hai scelto per il tuo file system Amazon FSx for Lustre, quindi scegli Crea file system.

Quando il file system è disponibile, la compressione dei dati è attivata.

Per attivare la compressione dei dati durante la creazione di un file system (CLI)

- Per creare un file system FSx for Lustre con la compressione dei dati attivata, usa il `create-file-system`comando Amazon FSx CLI con `DataCompressionType` il parametro, come illustrato di seguito. L'operazione API corrispondente è. 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
```

Dopo aver creato correttamente il file system, Amazon FSx restituisce la descrizione del file system come JSON, come mostrato nell'esempio seguente.

```
{

    "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
            }
        }
    ]
}
```

Puoi anche modificare la configurazione di compressione dei dati dei tuoi file system esistenti. Quando si attiva la compressione dei dati per un file system esistente, vengono compressi solo i file appena scritti, mentre i file esistenti non vengono compressi. Per ulteriori informazioni, consulta Compressione di file scritti in precedenza.

Per aggiornare la compressione dei dati su un file system esistente (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il Lustre file system per cui desideri gestire la compressione dei dati.
3. Per Azioni, scegli Aggiorna il tipo di compressione dei dati.
4. Nella finestra di dialogo Aggiorna il tipo di compressione dei dati, scegli di LZ4attivare la compressione dei dati oppure scegli NESSUNO per disattivarla.
5. Scegli Aggiorna.
6. È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system nella scheda Aggiornamenti.

Per aggiornare la compressione dei dati su un file system (CLI) esistente

Per aggiornare la configurazione di compressione dei dati per un file system FSx for Lustre esistente, usa il AWS CLI comando. update-file-system Imposta i seguenti parametri:

- `--file-system-id`Imposta l'ID del file system che stai aggiornando.
- `--lustre-configuration DataCompressionTypeNONE`Impostare per disattivare la compressione dei dati o `LZ4` per attivare la compressione dei dati con l' LZ4 algoritmo.

Questo comando specifica che la compressione dei dati è attivata con l' LZ4 algoritmo.

```
$ aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --lustre-configuration DataCompressionType=LZ4
```

Configurazione della compressione dei dati durante la creazione di un file system dal backup

Puoi utilizzare un backup disponibile per creare un nuovo file system Amazon FSx for Lustre. Quando crei un nuovo file system dal backup, non è necessario specificare il`DataCompressionType`; l'impostazione verrà applicata utilizzando l'`DataCompressionType`impostazione del backup.
Se si sceglie di specificare `DataCompressionType` quando si crea da backup, il valore deve corrispondere all'`DataCompressionType`impostazione del backup.

Per visualizzare le impostazioni di un backup, selezionalo dalla scheda Backup della FSx console Amazon. I dettagli del backup verranno elencati nella pagina di riepilogo relativa al backup. Puoi anche eseguire il `describe-backups` AWS CLI comando (l'azione API equivalente è `DescribeBackups`).

Compressione di file scritti in precedenza

I file non sono compressi se sono stati creati quando la compressione dei dati è stata disattivata sul file system Amazon FSx for Lustre. L'attivazione della compressione dei dati non comprimerà automaticamente i dati non compressi esistenti.

È possibile utilizzare il `lfs_migrate` comando installato come parte dell'installazione del Lustre client per comprimere i file esistenti. Per un esempio, vedi FSxL-Compression, disponibile su. GitHub

Visualizzazione delle dimensioni dei file

È possibile utilizzare i seguenti comandi per visualizzare le dimensioni non compresse e compresse dei file e delle directory.

- `du`visualizza dimensioni compresse.
- `du --apparent-size`visualizza dimensioni non compresse.
- `ls -l`visualizza dimensioni non compresse.

Gli esempi seguenti mostrano l'output di ogni comando con lo stesso file.

```
$ 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
```

L'`-h`opzione è utile per questi comandi perché stampa le dimensioni in un formato leggibile dall'uomo.

Utilizzo delle metriche CloudWatch

Puoi utilizzare CloudWatch i parametri di Amazon Logs per visualizzare l'utilizzo del tuo file system. La `LogicalDiskUsage` metrica mostra l'utilizzo totale del disco logico (senza compressione) e la

`PhysicalDiskUsage` metrica mostra l'utilizzo totale del disco fisico (con compressione). Queste due metriche sono disponibili solo se il file system ha abilitato la compressione dei dati o l'ha abilitata in precedenza.

È possibile determinare il rapporto di compressione del file system dividendo la `Sum` `LogicalDiskUsage` statistica per la `Sum` statistica. `PhysicalDiskUsage`

Per ulteriori informazioni sul monitoraggio delle prestazioni del file system, consulta. Monitoraggio dei file system Amazon FSx for Lustre

Lustre zucca

Root squash è una funzionalità amministrativa che aggiunge un ulteriore livello di controllo dell'accesso ai file oltre all'attuale controllo degli accessi basato sulla rete e alle autorizzazioni per i file POSIX. Utilizzando la funzionalità root squash, è possibile limitare l'accesso a livello root da parte dei client che tentano di accedere al file system FSx for Lustre come root.

Le autorizzazioni degli utenti root sono necessarie per eseguire azioni amministrative, come la gestione delle autorizzazioni sui FSx file system Lustre. Tuttavia, l'accesso root fornisce un accesso illimitato agli utenti, consentendo loro di aggirare i controlli di autorizzazione per accedere, modificare o eliminare gli oggetti del file system. Utilizzando la funzionalità root squash, è possibile impedire l'accesso o l'eliminazione non autorizzati dei dati specificando un ID utente (UID) non root (UID) e un ID di gruppo (GID) per il file system. Gli utenti root che accedono al file system verranno automaticamente convertiti nell'utente/gruppo con privilegi inferiori specificato con autorizzazioni limitate impostate dall'amministratore dello storage.

La funzione root squash consente inoltre, facoltativamente, di fornire un elenco di client che non sono interessati dall'impostazione root squash. Questi client possono accedere al file system come root, con privilegi illimitati.

Argomenti

- Come funziona il root squash
- Gestire la zucca

Come funziona il root squash

La funzione root squash funziona mappando nuovamente l'ID utente (UID) e l'ID di gruppo (GID) dell'utente root su un UID e un GID specificati dal Lustre amministratore di sistema. La funzione root

squash consente inoltre di specificare facoltativamente un set di client per i quali non si applica la nuova mappatura UID/GID.

Quando si crea un nuovo file system FSx for Lustre, root squash è disabilitato per impostazione predefinita. È possibile abilitare root squash configurando un'impostazione root squash UID e GID per il file system for Lustre. FSx I valori UID e GID sono numeri interi che possono variare da a: `0` `4294967294`

- Un valore diverso da zero per UID e GID abilita il root squash. I valori UID e GID possono essere diversi, ma ognuno deve essere un valore diverso da zero.
- Il valore `0` (zero) per UID e GID indica root e quindi disabilita root squash.

Durante la creazione del file system, puoi utilizzare la FSx console Amazon per fornire i valori UID e GID di root squash nella proprietà Root Squash, come mostrato in. Per abilitare root squash durante la creazione di un file system (console) Puoi anche utilizzare il `RootSquash` parametro con l'API AWS CLI o per fornire i valori UID e GID, come mostrato in. Per abilitare root squash durante la creazione di un file system (CLI)

Facoltativamente, puoi anche specificare un elenco NIDs di client per i quali root squash non è applicabile. Un NID del client è un Lustre Identificatore di rete utilizzato per identificare in modo univoco un client. È possibile specificare il NID come indirizzo singolo o come intervallo di indirizzi:

- Un indirizzo singolo è descritto in standard Lustre Formato NID specificando l'indirizzo IP del client seguito da Lustre ID di rete (ad esempio,`10.0.1.6@tcp`).
- Un intervallo di indirizzi viene descritto utilizzando un trattino per separare l'intervallo (ad esempio,`10.0.[2-10].[1-255]@tcp`).
- Se non specifichi alcun client NIDs, non ci saranno eccezioni a root squash.

Quando crei o aggiorni il tuo file system, puoi utilizzare la proprietà Exceptions to Root Squash nella FSx console Amazon per fornire l'elenco dei client. NIDs Nell'API AWS CLI o, usa il `NoSquashNids` parametro. Per ulteriori informazioni, consulta le procedure inGestire la zucca.

Gestire la zucca

Durante la creazione del file system, root squash è disabilitato per impostazione predefinita. Puoi abilitare root squash quando crei un nuovo file system Amazon FSx for Lustre dalla FSx console Amazon o dall' AWS CLI API.

Per abilitare root squash durante la creazione di un file system (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo file system descritta Passaggio 1: crea il tuo FSx file system for Lustre nella sezione Guida introduttiva.
3. Apri la sezione Root Squash - opzionale.
4. Per Root Squash, fornisci l'utente e il gruppo IDs con cui l'utente root può accedere al file system. È possibile specificare qualsiasi numero intero compreso nell'intervallo di `1` —: `4294967294`

   1. Per ID utente, specificare l'ID utente da utilizzare per l'utente root.
   2. Per ID di gruppo, specifica l'ID di gruppo che l'utente root deve utilizzare.
5. (Facoltativo) Per le eccezioni a Root Squash, effettuate le seguenti operazioni:

   1. Scegli Aggiungi indirizzo cliente.
   2. Nel campo Indirizzi client, specifica l'indirizzo IP di un client a cui non si applica root squash. Per informazioni sul formato dell'indirizzo IP, consultaCome funziona il root squash.
   3. Ripetere l'operazione se necessario per aggiungere altri indirizzi IP del client.
6. Completa la procedura guidata come fai quando crei un nuovo file system.
7. Scegliere Review and create (Rivedi e crea).
8. Controlla le impostazioni che hai scelto per il tuo file system Amazon FSx for Lustre, quindi scegli Crea file system.

Quando il file system è disponibile, root squash è abilitato.

Per abilitare root squash durante la creazione di un file system (CLI)

- Per creare un file system FSx for Lustre con root squash abilitato, usa il comando `create-file-system`Amazon FSx CLI con il parametro. `RootSquashConfiguration` L'operazione API corrispondente è. CreateFileSystem

  Per il `RootSquashConfiguration` parametro, impostate le seguenti opzioni:

  - `RootSquash`— I valori UID:GID separati da due punti che specificano l'ID utente e l'ID di gruppo da utilizzare per l'utente root. È possibile specificare qualsiasi numero intero nell'intervallo di `0` — `4294967294` (0 è root) per ogni ID (ad esempio,). `65534:65534`

- `NoSquashNids`— Specificare Lustre Identificatori di rete (NIDs) dei client a cui non si applica root squash. Per informazioni sul formato NID del client, vedere. Come funziona il root squash

L'esempio seguente crea un file system FSx for Lustre con root squash abilitato:

```
$ 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
```

Dopo aver creato correttamente il file system, Amazon FSx restituisce la descrizione del file system come JSON, come mostrato nell'esempio seguente.

```
{

    "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"
            }
        }
    ]
}
```

Puoi anche aggiornare le impostazioni root squash del tuo file system esistente utilizzando la FSx console Amazon o AWS CLI l'API. Ad esempio, puoi modificare i valori UID e GID di root squash, aggiungere o rimuovere client NIDs o disabilitare root squash.

Per aggiornare le impostazioni di root squash su un file system esistente (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli Lustre file system per cui vuoi gestire root squash.
3. Per Azioni, scegli Aggiorna root squash. Oppure, nel pannello Riepilogo, scegliete Aggiorna accanto al campo Root Squash del file system per visualizzare la finestra di dialogo Aggiorna le impostazioni di Root Squash.
4. Per Root Squash, aggiorna l'utente e il gruppo IDs con cui l'utente root può accedere al file system. È possibile specificare qualsiasi numero intero compreso nell'intervallo di `0` —`4294967294`. Per disabilitare root squash, specifica `0` (zero) per entrambi IDs.

    1. Per ID utente, specifica l'ID utente da utilizzare per l'utente root.
    2. Per ID di gruppo, specifica l'ID di gruppo che l'utente root deve utilizzare.
5. Per le eccezioni a Root Squash, procedi come segue:

    1. Scegli Aggiungi indirizzo cliente.

2. Nel campo Indirizzi client, specifica l'indirizzo IP di un client a cui non si applica root squash,
3. Ripetere l'operazione se necessario per aggiungere altri indirizzi IP del client.

6. Scegli Aggiorna.

> **Note**
>
> Se root squash è abilitato e vuoi disabilitarlo, scegli Disabilita invece di eseguire i passaggi 4-6.

È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli del file system nella scheda Aggiornamenti.

Per aggiornare le impostazioni di root squash su un file system (CLI) esistente

Per aggiornare le impostazioni root squash per un file system FSx for Lustre esistente, usa il comando. AWS CLI update-file-system L'operazione API corrispondente è. UpdateFileSystem

Imposta i seguenti parametri:

- `--file-system-id`Imposta l'ID del file system che stai aggiornando.
- Impostate le `--lustre-configuration RootSquashConfiguration` opzioni come segue:
  - `RootSquash`— Imposta i valori UID:GID separati da due punti che specificano l'ID utente e l'ID di gruppo da utilizzare per l'utente root. È possibile specificare qualsiasi numero intero nell'intervallo di `0` — `4294967294` (0 è root) per ogni ID. Per disabilitare root squash, specificate `0:0` i valori UID:GID.
  - `NoSquashNids`— Specificare Lustre Identificatori di rete (NIDs) dei client a cui non si applica root squash. `[]`Utilizzatelo per rimuovere tutti i client NIDs, il che significa che non ci saranno eccezioni a root squash.

Questo comando specifica che root squash è abilitato utilizzando `65534` come valore l'ID utente e l'ID di gruppo dell'utente root.

```
$ 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"]}
```

Se il comando ha esito positivo, Amazon FSx for Lustre restituisce la risposta in formato JSON.

Puoi visualizzare le impostazioni root squash del tuo file system nel pannello Riepilogo della pagina dei dettagli del file system sulla FSx console Amazon o nella risposta di un comando `describe-file-systems`CLI (l'azione `DescribeFileSystems`API equivalente è).

FSx per lo stato del file system Lustre

Puoi visualizzare lo stato di un FSx file system Amazon utilizzando la FSx console Amazon, il AWS CLI comando describe-file-systemso l'operazione API DescribeFileSystems.

Stato del file system	Descrizione
DISPONIBILE	Il file system è integro, raggiungibile e disponibile per l'uso.
CREAZIONE IN CORSO	Amazon FSx sta creando un nuovo file system.
ELIMINAZIONE IN CORSO	Amazon FSx sta eliminando un file system esistente.
AGGIORNAMENTO IN CORSO	Il file system è in fase di aggiornamento avviato dal cliente.
CONFIGURATO MALE	Il file system è in uno stato guasto ma ripristinabile.
Non riuscito	Questo stato può indicare una delle seguenti condizioni: • Il file system è guasto e Amazon non è in FSx grado di ripristinarlo. • Durante la creazione di un nuovo file system, Amazon non è FSx riuscito a creare il file system.

Etichetta le tue risorse Amazon FSx for Lustre

Per aiutarti a gestire i tuoi file system e altre risorse Amazon FSx for Lustre, puoi assegnare i tuoi metadati a ciascuna risorsa sotto forma di tag. I tag consentono di classificare le AWS risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Questa caratteristicaè molto utile quando hai tante risorse dello stesso tipo in quanto puoi rapidamente individuare una risorsa specifica in base ai tag assegnati. Questo argomento descrive i tag e mostra come crearli.

Argomenti

Nozioni di base sui tag

Un tag è un'etichetta che si assegna a una AWS risorsa. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili.

I tag consentono di classificare le AWS risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ad esempio, puoi definire un set di tag per i file system Amazon FSx for Lustre del tuo account che ti aiutino a tenere traccia del proprietario e del livello di stack di ogni istanza.

Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Con un set di chiavi di tag coerente, la gestione delle risorse risulta semplificata. Puoi cercare e filtrare le risorse in base ai tag aggiunti.

I tag non hanno alcun significato semantico per Amazon FSx e vengono interpretati rigorosamente come una stringa di caratteri. Inoltre, i tag non vengono assegnati automaticamente alle risorse. Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

Se utilizzi l'API Amazon FSx for Lustre, la AWS CLI o AWS un SDK, puoi utilizzare `TagResource` l'azione API per applicare tag alle risorse esistenti. Inoltre, alcune operazioni per la creazione di risorse ti consentono di specificare tag per una risorsa durante la sua creazione. Se i tag non

possono essere applicati durante la creazione della risorsa, eseguiamo il rollback del processo di creazione della risorsa. Ciò fa sì che le risorse vengano create con i tag oppure che non vengano create affatto, nonché che nessuna risorsa sia mai sprovvista di tag. Il tagging delle risorse in fase di creazione ti permette di evitare di eseguire script di tagging personalizzati dopo la creazione delle risorse. Per ulteriori informazioni sull'abilitazione agli utenti affinché possano aggiungere tag alle risorse durante la creazione, vedere Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

Tagging delle risorse

Puoi taggare le risorse Amazon FSx for Lustre presenti nel tuo account. Se utilizzi la FSx console Amazon, puoi applicare tag alle risorse utilizzando la scheda Tag nella schermata delle risorse pertinente. Quando crei risorse, puoi applicare la chiave Name con un valore e puoi applicare tag a tua scelta quando crei un nuovo file system. La console può organizzare le risorse in base al tag Name, ma questo tag non ha alcun significato semantico per il servizio Amazon FSx for Lustre.

Puoi applicare autorizzazioni a livello di risorsa basate su tag nelle tue policy IAM alle azioni dell'API Amazon FSx for Lustre che supportano l'etichettatura alla creazione per implementare il controllo granulare su utenti e gruppi che possono taggare le risorse al momento della creazione. Le risorse vengono adeguatamente protette a partire dal momento della creazione, ovvero i tag vengono applicati subito alle risorse. Pertanto qualsiasi autorizzazione basata su tag a livello di risorsa che controlla l'uso delle risorse risulta immediatamente valida. Le risorse possono essere monitorate e segnalate con maggiore precisione. Puoi applicare l'uso del tagging alle nuove risorse e controllare quali chiavi e valori di tag sono impostati per le risorse.

Puoi anche applicare autorizzazioni a livello di risorsa alle azioni dell'API `TagResource` `UntagResource` Amazon FSx for Lustre nelle tue policy IAM per controllare quali chiavi e valori dei tag sono impostati sulle tue risorse esistenti.

Per ulteriori informazioni sul tagging delle risorse per la fatturazione, consulta Utilizzo di tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing .

Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per risorsa: 50
- Per ciascuna risorsa, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.

- Lunghezza massima della chiave: 128 caratteri Unicode in formato UTF-8
- Lunghezza massima del valore: 256 caratteri Unicode in formato UTF-8
- I caratteri consentiti per i tag Amazon FSx for Lustre sono: lettere, numeri e spazi rappresentabili in UTF-8 e i seguenti caratteri: + - =. _:/@.
- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole.
- Il `aws:` prefisso è riservato all'uso. AWS Se il tag ha una chiave di tag con questo prefisso, non puoi modificare o eliminare la chiave o il valore de tag. I tag con il prefisso `aws:` non vengono conteggiati per il limite del numero di tag per risorsa.

Non è possibile eliminare una risorsa in base esclusivamente ai relativi tag; è necessario specificare l'identificatore della risorsa. Ad esempio, per eliminare un file system etichettato con una chiave di tag chiamata`DeleteMe`, è necessario utilizzare l'`DeleteFileSystem`azione con l'identificatore di risorsa del file system, ad esempio fs-1234567890abcdef0.

Quando taggate risorse pubbliche o condivise, i tag assegnati sono disponibili solo per le vostre risorse; nessun altro avrà accesso a tali tag. Account AWS Account AWS Per il controllo dell'accesso basato su tag alle risorse condivise, ognuno Account AWS deve assegnare il proprio set di tag per controllare l'accesso alla risorsa.

Autorizzazioni e tag

Per ulteriori informazioni sulle autorizzazioni necessarie per etichettare le FSx risorse Amazon al momento della creazione, consulta Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione .Per ulteriori informazioni sull'utilizzo dei tag per limitare l'accesso alle FSx risorse Amazon nelle politiche IAM, consulta. Utilizzo dei tag per controllare l'accesso alle FSx risorse Amazon

Finestre di manutenzione Amazon FSx for Lustre

Amazon FSx for Lustre esegue patch software di routine per il Lustre software che gestisce. L'applicazione delle patch avviene raramente, in genere una volta ogni diverse settimane. La finestra di manutenzione offre l'opportunità di controllare in quale giorno e ora della settimana vengono applicate le patch software. È possibile scegliere la finestra di manutenzione durante la creazione del file system. Se non avete preferenze temporali, viene assegnata una finestra predefinita di 30 minuti.

L'applicazione delle patch dovrebbe richiedere solo una frazione della finestra di manutenzione di 30 minuti. Durante questi pochi minuti, il file system sarà temporaneamente non disponibile. Le

operazioni sui file eseguite dai client mentre il file system non è disponibile verranno riprovate in modo trasparente e alla fine avranno esito positivo al termine della manutenzione. Si noti che la cache in memoria verrà cancellata durante la manutenzione, con conseguenti latenze più elevate fino al completamento della manutenzione.

FSx for Lustre consente di regolare la finestra di manutenzione in base alle esigenze, per adattarla al carico di lavoro e ai requisiti operativi. È possibile spostare la finestra di manutenzione con la frequenza necessaria, a condizione che una finestra di manutenzione sia pianificata almeno una volta ogni 14 giorni. Se viene rilasciata una patch e non avete pianificato una finestra di manutenzione entro 14 giorni, FSx for Lustre procederà alla manutenzione del file system per garantirne la sicurezza e l'affidabilità.

Puoi utilizzare la Console di FSx gestione Amazon AWS CLI, AWS l'API o una delle altre AWS SDKs per modificare la finestra di manutenzione dei tuoi file system.

Per modificare la finestra di manutenzione utilizzando la console

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli File system nel pannello di navigazione.
3. Scegli il file system per cui desideri modificare la finestra di manutenzione. Viene visualizzata la pagina dei dettagli del file system.
4. Scegli la scheda Manutenzione. Viene visualizzato il pannello Impostazioni della finestra di manutenzione.
5. Scegli Modifica e inserisci il nuovo giorno e l'ora in cui desideri che inizi la finestra di manutenzione.
6. Scegliere Salva per salvare le modifiche. La nuova ora di inizio della manutenzione viene visualizzata nel pannello Impostazioni.

È possibile modificare la finestra di manutenzione del file system utilizzando il comando update-file-systemCLI. Esegui il comando seguente, sostituendo l'ID del file system con l'ID del file system e la data e l'ora in cui desideri iniziare la finestra.

```
aws fsx update-file-system --file-system-id fs-01234567890123456 --lustre-configuration
 WeeklyMaintenanceStartTime=1:01:30
```

Gestione delle versioni di Lustre

FSx for Lustre attualmente supporta diverse versioni di Lustre con supporto a lungo termine (LTS) rilasciate dalla comunità Lustre. Le versioni LTS più recenti offrono vantaggi come miglioramenti delle prestazioni, nuove funzionalità e supporto per le ultime versioni del kernel Linux per le istanze client. È possibile aggiornare i file system alle versioni più recenti di Lustre in pochi minuti utilizzando, o. AWS Management Console AWS CLI AWS SDKs

FSx for Lustre attualmente supporta le versioni 2.10, 2.12 e 2.15 di Lustre LTS. È possibile determinare la versione LTS dei file system FSx for Lustre utilizzando o utilizzando il comando. AWS Management Console describe-file-systems AWS CLI

Prima di eseguire un aggiornamento della versione di Lustre, si consiglia di seguire i passaggi descritti in. Procedure consigliate per gli aggiornamenti delle versioni di Lustre

Argomenti

Procedure consigliate per gli aggiornamenti delle versioni di Lustre

Ti consigliamo di seguire queste best practice prima di aggiornare la versione Lustre del file system for Lustre: FSx

- Esegui un test in un ambiente non di produzione: prova un aggiornamento della versione di Lustre su un duplicato del file system di produzione prima di aggiornare il file system di produzione. Ciò garantisce un processo di aggiornamento senza intoppi per il carico di lavoro di produzione.
- Garantite la compatibilità dei client: verificate che le versioni del kernel Linux in esecuzione sulle istanze client siano compatibili con la versione Lustre a cui intendete effettuare l'aggiornamento. Per informazioni dettagliate, vedi Lustrecompatibilità tra file system e kernel client.
- Esegui il backup dei tuoi dati:
  - Per i file system non collegati a S3: ti consigliamo di creare un FSx backup prima di aggiornare la versione Lustre in modo da avere un punto di ripristino noto per il tuo file system. Se i backup giornalieri automatici sono abilitati sul tuo file system, Amazon FSx creerà automaticamente un backup del tuo file system prima dell'aggiornamento.
  - Per i file system collegati a S3 Ti consigliamo di assicurarti che tutte le modifiche siano state esportate in S3 prima dell'aggiornamento. Se hai abilitato l'esportazione automatica, verifica

che la AgeOfOldestQueuedMessage AutoExportmetrica sia zero per confermare che tutte le modifiche siano state esportate correttamente in S3. Se non hai abilitato l'esportazione automatica, puoi eseguire un'esportazione DRT (Manual Data Repository Task) per sincronizzare il file system con il bucket S3 prima dell'aggiornamento.

Esecuzione dell'aggiornamento

Per aggiornare il file system FSx for Lustre a una versione più recente, segui i passaggi elencati:

1. Smonta tutti i client: prima di iniziare l'aggiornamento, è necessario smontare il file system da tutte le istanze del client che accedono al file system. Puoi verificare che tutti i client siano stati smontati correttamente utilizzando la `ClientConnections` metrica su Amazon CloudWatch : questa metrica dovrebbe mostrare zero connessioni. Il processo di aggiornamento non procederà se alcuni client rimangono connessi al file system.

   È possibile visualizzare l'elenco degli identificatori di rete dei client (NIDs) collegati al file system nel `.fsx/clientConnections` file memorizzato nella radice del file system. Questo file viene aggiornato ogni 5 minuti. È possibile utilizzare il `cat` comando per visualizzare il contenuto del file, come in questo esempio:

   ```
   cat /test/.fsx/clientConnections
   ```

2. Aggiorna la versione Lustre: puoi aggiornare la versione Lustre del tuo file system FSx for Lustre utilizzando la FSx console Amazon, o l' AWS CLI API Amazon. FSx Ti consigliamo di aggiornare i tuoi file system all'ultima versione di Lustre supportata da for Lustre. FSx

   Per aggiornare la versione Lustre di un file system (console)

   a. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.

   b. Nel pannello di navigazione a sinistra, scegli File system. Nell'elenco File system, scegli il file system FSx for Lustre per cui desideri aggiornare la versione Lustre.

   c. Per Azioni, scegliete Aggiorna la versione Lustre del file system. Oppure, nel pannello Riepilogo, scegliete Aggiorna accanto al campo della versione Lustre del file system. Viene visualizzata la finestra di dialogo Update file system Lustre version. Viene visualizzata la finestra di dialogo Update file system Lustre version.

   d. Nel campo Seleziona una nuova versione Lustre, scegli una versione Lustre. Il valore scelto deve essere più recente della versione corrente di Lustre.

e. Scegli Aggiorna.

Per aggiornare la versione Lustre di un file system (CLI)

Per aggiornare la versione Lustre di un file system FSx for Lustre, usa il comando. AWS CLI update-file-system (L'azione API equivalente è UpdateFileSystem.) Imposta i seguenti parametri:

- `--file-system-id`Imposta l'ID del file system che stai aggiornando.
- `--file-system-type-version`Impostate su una versione più recente di Lustre per il file system che state aggiornando.

L'esempio seguente aggiorna la versione Lustre del file system dalla 2.12 alla 2.15:

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --file-system-type-version "2.15"
```

3. Monta tutti i client: puoi monitorare lo stato di avanzamento degli aggiornamenti della versione Lustre utilizzando la scheda Updates nella FSx console Amazon o `describe-file-systems` in. AWS CLI Una volta che lo stato di aggiornamento della versione Lustre risulta pari a quello indicato`Completed`, puoi rimontare in sicurezza il file system sulle istanze client e riprendere il carico di lavoro.

Cancellazione di un file system

Puoi eliminare un file system Amazon FSx for Lustre utilizzando la FSx console Amazon AWS CLI, e l' FSx API Amazon. Prima di eliminare un file system FSx for Lustre, devi smontarlo da ogni istanza Amazon connessa. EC2 Sui file system collegati a S3, per garantire che tutti i dati vengano riscritti su S3 prima di eliminare il file system, puoi monitorare che la AgeOfOldestQueuedMessagemetrica sia pari a zero (se utilizzi l'esportazione automatica) oppure puoi eseguire un'attività di esportazione del repository di dati. Se hai abilitato l'esportazione automatica e desideri utilizzare un'attività di esportazione dell'archivio dei dati, devi disabilitare l'esportazione automatica prima di eseguire l'attività di esportazione dell'archivio dei dati.

Per eliminare un file system dopo lo smontaggio da ogni EC2 istanza Amazon:

- Utilizzo della console: segui la procedura descritta inFase 5: eliminazione delle risorse .

- Utilizzo dell'API o della CLI: utilizza l'operazione DeleteFileSystemAPI o il comando CLI delete-file-system.

Protezione dei dati con backup

Con Amazon FSx for Lustre, puoi eseguire backup giornalieri automatici e backup avviati dall'utente di file system persistenti che non sono collegati a un repository di dati durevole di Amazon S3. I FSx backup di Amazon sono file-system-consistent altamente durevoli e incrementali. Per garantire un'elevata durabilità, Amazon FSx for Lustre archivia i backup in Amazon Simple Storage Service (Amazon S3) con una durabilità del 99,99999% (11 9).

FSx per Lustre i backup del file system sono backup incrementali basati su blocchi, indipendentemente dal fatto che vengano generati utilizzando il backup giornaliero automatico o la funzionalità di backup avviato dall'utente. Ciò significa che quando esegui un backup, Amazon FSx confronta i dati sul tuo file system con il backup precedente a livello di blocco. Quindi Amazon FSx archivia una copia di tutte le modifiche a livello di blocco nel nuovo backup. I dati a livello di blocco che rimangono invariati rispetto al backup precedente non vengono archiviati nel nuovo backup. La durata del processo di backup dipende dalla quantità di dati modificati dall'ultimo backup ed è indipendente dalla capacità di archiviazione del file system. L'elenco seguente illustra i tempi di backup in diverse circostanze:

- Il completamento del backup iniziale di un file system nuovo di zecca con pochissimi dati richiede pochi minuti.
- Il completamento del backup iniziale di un file system nuovo di zecca eseguito dopo il caricamento TBs dei dati richiede ore.
- Il completamento di un secondo backup del file system con TBs modifiche minime ai dati a livello di blocco (relativamente poche creazioni/modifiche) richiede pochi secondi.
- Il completamento di un terzo backup dello stesso file system dopo l'aggiunta e la modifica di una grande quantità di dati richiede ore.

Quando si elimina un backup, vengono rimossi solo i dati univoci di quel backup. Ogni FSx backup di For Lustre contiene tutte le informazioni necessarie per creare un nuovo file system a partire dal backup, ripristinando efficacemente un' point-in-timeistantanea del file system.

La creazione di backup regolari per il tuo file system è una best practice che integra la replica che Amazon FSx for Lustre esegue per il tuo file system. FSx I backup di Amazon aiutano a supportare le tue esigenze di conservazione e conformità dei backup. Lavorare con i backup di Amazon FSx for Lustre è semplice, che si tratti di creare backup, copiare un backup, ripristinare un file system da un backup o eliminare un backup.

I backup non sono supportati sui file system scratch perché questi file system sono progettati per l'archiviazione temporanea e l'elaborazione a breve termine dei dati. I backup non sono supportati sui file system collegati a un bucket Amazon S3 perché il bucket S3 funge da repository di dati principale e il file system non contiene necessariamente Lustre il set di dati completo in un dato momento.

Argomenti

Supporto FSx per il backup in Lustre

I backup sono supportati solo sui FSx file system persistenti Lustre che non sono collegati a un repository di dati Amazon S3.

Amazon FSx non supporta i backup su file system scratch perché i file system scratch sono progettati per l'archiviazione temporanea e l'elaborazione a breve termine dei dati. Amazon FSx non supporta i backup su file system collegati a un bucket Amazon S3 perché il bucket S3 funge da repository di dati principale e il file system non contiene necessariamente il set di dati completo in un dato momento. Per ulteriori informazioni, consultare Opzioni di implementazione e classe di archiviazione e Utilizzo di archivi di dati.

Lavorare con backup giornalieri automatici

Amazon FSx for Lustre può eseguire un backup giornaliero automatico del file system. Questi backup giornalieri automatici vengono eseguiti durante la finestra di backup giornaliera stabilita al momento della creazione del file system. Ad un certo punto durante la finestra di backup giornaliera, l'I/O di storage potrebbe essere sospeso brevemente durante l'inizializzazione del processo di backup (in genere per meno di qualche secondo). Quando scegli la finestra di backup giornaliera, ti consigliamo

di scegliere un momento della giornata conveniente. Questo orario è idealmente al di fuori del normale orario di funzionamento delle applicazioni che utilizzano il file system.

I backup giornalieri automatici vengono conservati per un determinato periodo di tempo, noto come periodo di conservazione. È possibile impostare il periodo di conservazione in modo che sia compreso tra 0 e 90 giorni. L'impostazione del periodo di conservazione su 0 (zero) giorni disattiva i backup giornalieri automatici. Il periodo di conservazione predefinito per i backup giornalieri automatici è 0 giorni. I backup giornalieri automatici vengono eliminati quando il file system viene eliminato.

> **Note**
>
> L'impostazione del periodo di conservazione su 0 giorni significa che il backup del file system non viene mai eseguito automaticamente. Si consiglia vivamente di utilizzare backup giornalieri automatici per file system a cui sono associati qualsiasi livello di funzionalità critiche.

È possibile utilizzare AWS CLI o uno di questi AWS SDKs per modificare la finestra di backup e il periodo di conservazione dei backup per i file system. Utilizza l'operazione `UpdateFileSystem`API o il comando `update-file-system`CLI.

Utilizzo dei backup avviati dall'utente

Amazon FSx for Lustre ti consente di eseguire manualmente il backup dei tuoi file system in qualsiasi momento. Puoi farlo utilizzando la console Amazon FSx for Lustre, l'API o la AWS Command Line Interface (CLI). I backup dei FSx file system Amazon avviati dall'utente non scadono mai e sono disponibili per tutto il tempo che desideri conservarli. I backup avviati dall'utente vengono conservati anche dopo l'eliminazione del file system di cui era stato eseguito il backup. Puoi eliminare i backup avviati dall'utente solo utilizzando la console, l'API o la CLI di Amazon FSx for Lustre e non vengono mai eliminati automaticamente da Amazon. FSx Per ulteriori informazioni, consulta Eliminazione di backup.

Creazione di backup avviati dall'utente

La procedura seguente illustra come creare un backup avviato dall'utente nella FSx console Amazon per un file system esistente.

Per creare un backup del file system avviato dall'utente

1. Apri la console Amazon FSx for Lustre all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard della console, scegli il nome del file system di cui desideri eseguire il backup.
3. Da Azioni, scegli Crea backup.
4. Nella finestra di dialogo Crea backup che si apre, fornisci un nome per il backup. I nomi di Backup possono contenere un massimo di 256 caratteri Unicode, inclusi lettere, spazi bianchi, numeri e caratteri speciali. + - = _:/
5. Scegliere Create backup (Crea backup).

A questo punto è stato creato il backup del file system. Puoi trovare una tabella di tutti i tuoi backup nella console Amazon FSx for Lustre selezionando Backup nella barra di navigazione a sinistra. Puoi cercare il nome che hai assegnato al backup e la tabella filtra per mostrare solo i risultati corrispondenti.

Quando crei un backup avviato dall'utente come descritto in questa procedura, ha il tipo `USER_INITIATED` e ha lo stato Creazione mentre Amazon FSx crea il backup. Lo stato cambia in Trasferimento mentre il backup viene trasferito su Amazon S3, fino a quando non è completamente disponibile.

Utilizzo AWS Backup con Amazon FSx

AWS Backup è un modo semplice ed economico per proteggere i dati eseguendo il backup dei file system Amazon FSx . AWS Backup è un servizio di backup unificato progettato per semplificare la creazione, la copia, il ripristino e l'eliminazione dei backup, fornendo al contempo report e controlli migliorati. AWS Backup semplifica lo sviluppo di una strategia di backup centralizzata per la conformità legale, normativa e professionale. AWS Backup semplifica inoltre la protezione dei volumi di AWS storage, dei database e dei file system fornendo una posizione centrale in cui è possibile eseguire le seguenti operazioni:

- Configura e controlla le AWS risorse di cui desideri eseguire il backup.
- Automatizzare la pianificazione dei backup.
- Impostare le policy di conservazione.
- Copia i backup tra AWS regioni e tra AWS account.
- Monitorare tutte le attività recenti di backup e ripristino.

AWS Backup utilizza la funzionalità di backup integrata di Amazon FSx. I backup eseguiti dalla AWS Backup console hanno lo stesso livello di coerenza e prestazioni del file system e le stesse opzioni di ripristino dei backup eseguiti tramite la console Amazon FSx . Se gestisci questi backup, ottieni funzionalità aggiuntive, come opzioni di conservazione illimitate e la possibilità di creare backup pianificati con una frequenza ogni ora. AWS Backup Inoltre, AWS Backup conserva i backup immutabili anche dopo l'eliminazione del file system di origine. Questo aiuta a proteggere da eliminazioni accidentali o dolose.

I backup creati da AWS Backup hanno un tipo di backup `AWS_BACKUP` e sono incrementali rispetto a qualsiasi altro FSx backup Amazon che esegui del tuo file system. I backup eseguiti da AWS Backup sono considerati backup avviati dall'utente e vengono conteggiati ai fini della quota di backup avviata dall'utente per Amazon. FSx Puoi visualizzare e ripristinare i backup eseguiti nella FSx console Amazon, AWS Backup nella CLI e nell'API. Tuttavia, non puoi eliminare i backup eseguiti nella FSx console Amazon, AWS Backup nella CLI o nell'API. Per ulteriori informazioni su come eseguire il backup dei FSx file system Amazon, consulta Working with Amazon FSx File Systems nella AWS Backup Developer Guide. AWS Backup

Copia di backup

Puoi utilizzare Amazon FSx per copiare manualmente i backup all'interno dello stesso AWS account su un altro Regione AWS (copie in più regioni) o all'interno dello stesso Regione AWS (copie all'interno della stessa regione). Puoi creare copie interregionali solo all'interno della stessa partizione. AWS Puoi creare copie di backup avviate dall'utente utilizzando la FSx console Amazon o AWS CLI l'API. Quando crei una copia di backup avviata dall'utente, ha il seguente tipo. `USER_INITIATED`

È inoltre possibile utilizzare AWS Backup per copiare i backup tra Regioni AWS e tra account. AWS AWS Backup è un servizio di gestione dei backup completamente gestito che fornisce un'interfaccia centrale per piani di backup basati su policy. Grazie alla sua gestione tra account, è possibile utilizzare automaticamente le policy di backup per applicare piani di backup a tutti gli account dell'organizzazione.

Le copie di backup in più regioni sono particolarmente utili per il disaster recovery in più regioni. I backup vengono eseguiti e copiati in un'altra AWS regione in modo che, in caso di emergenza nella regione principale Regione AWS, sia possibile eseguire il ripristino dal backup e ripristinare rapidamente la disponibilità nell'altra regione. AWS È inoltre possibile utilizzare copie di backup per clonare il set di dati dei file su un'altra Regione AWS o all'interno della stessa. Regione AWS Puoi creare copie di backup all'interno dello stesso AWS account (interregionale o regionale) utilizzando

la FSx console Amazon o l'API AWS CLI Amazon FSx for Lustre. Puoi anche utilizzarlo AWS Backupper eseguire copie di backup, su richiesta o basate su policy.

Le copie di backup su più account sono utili per soddisfare i requisiti di conformità normativa relativi alla copia dei backup su un account isolato. Forniscono inoltre un ulteriore livello di protezione dei dati per aiutare a prevenire l'eliminazione accidentale o dolosa dei backup, la perdita di credenziali o la compromissione delle chiavi. AWS KMS I backup su più account supportano il fan-in (copia dei backup da più account primari su un account di copia di backup isolato) e il fan-out (copia i backup da un account principale a più account di copia di backup isolati).

È possibile creare copie di backup su più account utilizzando with support. AWS Backup AWS Organizations I limiti degli account per le copie su più account sono definiti dalle AWS Organizations politiche. Per ulteriori informazioni sull'utilizzo per AWS Backup creare copie di backup su più account, consulta Creazione di copie di backup Account AWS nella Guida per gli AWS Backup sviluppatori.

Limitazioni relative alla copia di backup

Di seguito sono riportate alcune limitazioni relative alla copia dei backup:

- I backup dei file system che utilizzano la classe di storage Intelligent-Tiering non supportano le copie di backup.
- Le copie di backup interregionali sono supportate solo tra due regioni commerciali qualsiasi Regioni AWS, tra le regioni Cina (Pechino) e Cina (Ningxia) e tra le regioni AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali), ma non tra questi set di regioni.
- Le copie di backup interregionali non sono supportate nelle regioni che hanno scelto di aderire.
- È possibile creare copie di backup all'interno di qualsiasi regione. Regione AWS
- Il backup di origine deve avere lo stato di `AVAILABLE` prima di poterlo copiare.
- Non è possibile eliminare un backup di origine se viene copiato. Potrebbe verificarsi un breve ritardo tra il momento in cui il backup di destinazione diventa disponibile e il momento in cui è consentito eliminare il backup di origine. È necessario tenere presente questo ritardo se si tenta di eliminare nuovamente un backup di origine.
- Puoi avere fino a cinque richieste di copie di backup in corso verso un'unica destinazione Regione AWS per account.

Autorizzazioni per le copie di backup in più regioni

Si utilizza una dichiarazione di policy IAM per concedere le autorizzazioni per eseguire un'operazione di copia di backup. Per comunicare con la AWS regione di origine e richiedere una copia di backup su più regioni, il richiedente (ruolo IAM o utente IAM) deve avere accesso al backup di origine e alla regione di origine. AWS

La policy viene utilizzata per concedere le autorizzazioni all'`CopyBackup`azione per l'operazione di copia di backup. Si specifica l'azione nel `Action` campo della politica e si specifica il valore della risorsa nel `Resource` campo della politica, come nell'esempio seguente.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111122223333:backup/*"
        }
    ]
}
```

Per ulteriori informazioni sulle policy IAM, consulta Policies and permissions in IAM nella IAM User Guide.

Copie complete e incrementali

Quando copi un backup su un backup diverso Regione AWS da quello di origine, la prima copia è una copia di backup completa. Dopo la prima copia di backup, tutte le copie di backup successive nella stessa regione di destinazione all'interno dello stesso AWS account sono incrementali, a condizione che non siano stati eliminati tutti i backup precedentemente copiati in quella regione e che sia stata utilizzata la stessa chiave. AWS KMS Se entrambe le condizioni non sono soddisfatte, l'operazione di copia genera una copia di backup completa (non incrementale).

Copiare i backup all'interno dello stesso Account AWS

È possibile copiare i backup dei FSx file system Lustre utilizzando la AWS Management Console CLI e l'API, come descritto nelle seguenti procedure.

Per copiare un backup all'interno dello stesso account (interregionale o interregionale) utilizzando la console

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione, scegliere Backup.
3. Nella tabella Backup, scegli il backup che desideri copiare, quindi scegli Copia backup.
4. Nella sezione Rule settings (Impostazioni regole), procedi nel seguente modo:
   - Nell'elenco Regione di destinazione, scegli una AWS regione di destinazione in cui copiare il backup. La destinazione può trovarsi in un'altra AWS regione (copia interregionale) o all'interno della stessa AWS regione (copia interna all'area).
   - (Facoltativo) Seleziona Copia tag per copiare i tag dal backup di origine al backup di destinazione. Se si seleziona Copia tag e si aggiungono anche tag al passaggio 6, tutti i tag vengono uniti.
5. Per Crittografia, scegli la chiave di AWS KMS crittografia per crittografare il backup copiato.
6. Per Tag: facoltativo, inserisci una chiave e un valore per aggiungere tag per il backup copiato. Se aggiungi tag qui e hai selezionato anche Copia tag al passaggio 4, tutti i tag vengono uniti.
7. Scegli Copia backup.

   Il backup viene copiato all'interno dello stesso nel file Account AWS selezionato. Regione AWS

Per copiare un backup all'interno dello stesso account (interregionale o interregionale) utilizzando la CLI

- Utilizza il comando `copy-backup` CLI o l'operazione CopyBackupAPI per copiare un backup all'interno dello stesso AWS account, in una AWS regione o all'interno di una AWS regione.

  Il comando seguente copia un backup con un ID `backup-0abc123456789cba7` proveniente dalla `us-east-1` regione.

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  La risposta mostra la descrizione del backup copiato.

Puoi visualizzare i tuoi backup sulla FSx console Amazon o in modo programmatico utilizzando il comando `describe-backups` CLI o l'operazione API. DescribeBackups

Ripristino dei backup

È possibile utilizzare un backup disponibile per creare un nuovo file system, ripristinando in modo efficace un' point-in-timeistantanea di un altro file system. È possibile ripristinare un backup utilizzando la console o uno dei. AWS CLI AWS SDKs Il ripristino di un backup su un nuovo file system richiede lo stesso tempo della creazione di un nuovo file system. I dati ripristinati dal backup vengono caricati lentamente sul file system, durante il quale si verificherà una latenza leggermente superiore.

> **Note**
>
> È possibile ripristinare il backup solo su un file system dello stesso tipo di implementazione, classe di storage, capacità di throughput, capacità di archiviazione, tipo di compressione dei dati e dell'originale. Regione AWS È possibile aumentare la capacità di archiviazione del file system ripristinato non appena sarà disponibile.

Per ripristinare un file system da un backup utilizzando la console

1. Apri la console Amazon FSx for Lustre all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard della console, scegli Backups dalla barra di navigazione a sinistra.
3. Scegli il backup che desideri ripristinare dalla tabella Backup, quindi scegli Ripristina backup.

   La procedura guidata per la creazione del file system si apre con la maggior parte delle impostazioni precompilate in base alla configurazione del file system da cui è stato creato il backup. Facoltativamente, puoi modificare la configurazione Virtual Private Cloud (VPC) o scegliere una versione più recente di Lustre. Tieni presente che altre impostazioni di configurazione, come il tipo di distribuzione e il throughput per unità di storage, non possono essere modificate durante il ripristino.
4. Completa la procedura guidata come quando crei un nuovo file system.
5. Scegliere Review and create (Rivedi e crea).
6. Controlla le impostazioni che hai scelto per il tuo file system Amazon FSx for Lustre, quindi scegli Crea file system.

Hai eseguito il ripristino da un backup e ora viene creato un nuovo file system. Quando il suo stato cambia a`AVAILABLE`, è possibile utilizzare il file system normalmente.

Eliminazione di backup

L'eliminazione di un backup è un'azione permanente e irrecuperabile. Vengono eliminati anche tutti i dati contenuti in un backup eliminato. Non eliminate un backup a meno che non siate sicuri di non averne più bisogno in futuro. Non puoi eliminare i backup eseguiti dalla AWS Backup FSx console Amazon, dalla CLI o dall'API.

Per eliminare un backup

1. Apri la console Amazon FSx for Lustre all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard della console, scegli Backups dalla barra di navigazione a sinistra.
3. Scegli il backup che desideri eliminare dalla tabella Backup, quindi scegli Elimina backup.
4. Nella finestra di dialogo Elimina backup che si apre, verifica che l'ID del backup identifichi il backup che desideri eliminare.
5. Conferma che la casella di controllo sia selezionata per il backup che desideri eliminare.
6. Scegli Elimina backup.

Il backup e tutti i dati inclusi vengono ora eliminati in modo permanente e irrecuperabile.

Monitoraggio dei file system Amazon FSx for Lustre

Il monitoraggio è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni del file system FSx for Lustre e delle altre AWS soluzioni. La raccolta dei dati di monitoraggio da tutte le parti della AWS soluzione consente di eseguire più facilmente il debug di un errore multipunto, se si verifica uno. È possibile monitorare il file system FSx for Lustre, segnalare quando qualcosa non va e intervenire automaticamente all'occorrenza utilizzando i seguenti strumenti:

- Amazon CloudWatch: monitora AWS le tue risorse e le applicazioni su cui esegui AWS in tempo reale. Puoi raccogliere e tenere traccia delle metriche, creare dashboard personalizzate e impostare allarmi che ti avvisano quando una determinata metrica raggiunge una soglia da te specificata. Ad esempio, puoi CloudWatch tenere traccia della capacità di storage o di altri parametri per le tue istanze Amazon FSx for Lustre e avviare automaticamente nuove istanze quando necessario.
- Lustre logging: monitora gli eventi di registrazione abilitati per il tuo file system. Lustre logging scrive questi eventi su Amazon CloudWatch Logs.
- AWS CloudTrail— Acquisisce le chiamate API e gli eventi correlati effettuati da o per conto dell'utente Account AWS e invia i file di log a un bucket Amazon S3 da te specificato. Puoi identificare quali utenti e account hanno richiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute.

Le sezioni seguenti forniscono informazioni su come utilizzare gli strumenti con i file system FSx for Lustre.

Argomenti

Monitoraggio con Amazon CloudWatch

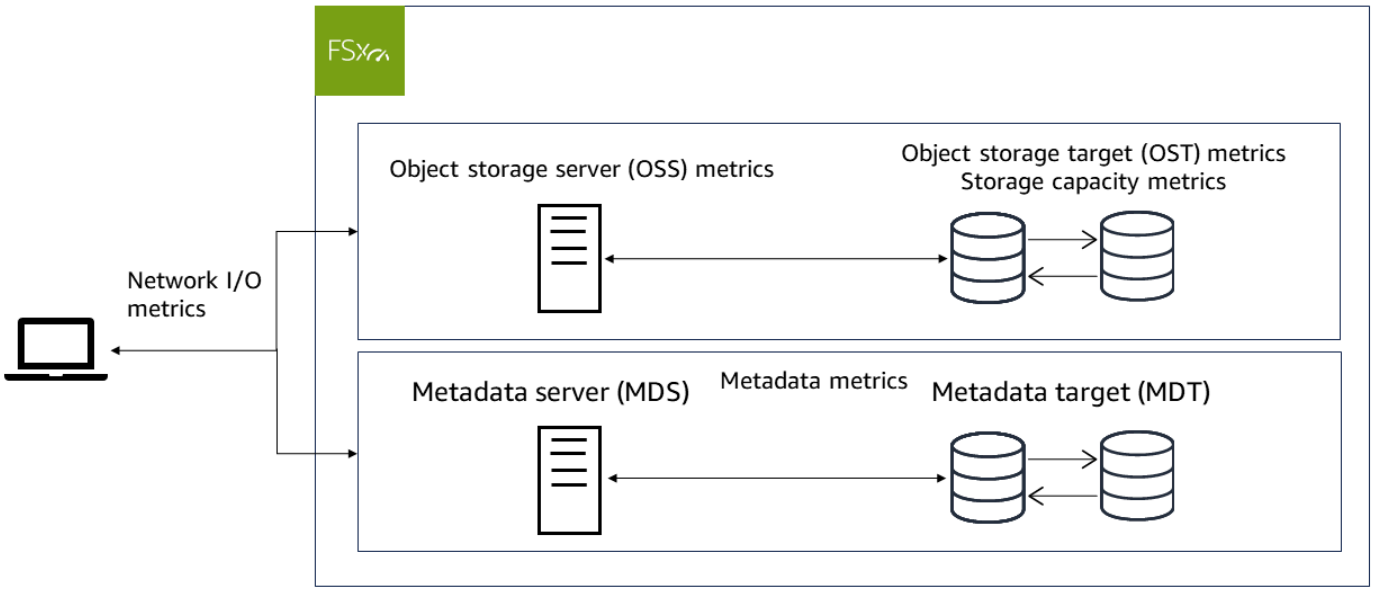
Puoi monitorare Amazon FSx for Lustre utilizzando CloudWatch, che raccoglie ed elabora i dati grezzi di Amazon FSx for Lustre in metriche leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, in modo da poter accedere alle informazioni storiche e avere

una prospettiva migliore sulle prestazioni dell'applicazione o del servizio. Per ulteriori informazioni su CloudWatch, consulta What is Amazon CloudWatch? nella Amazon CloudWatch User Guide.

CloudWatch le metriche di FSx for Lustre sono organizzate in sei categorie:

- I/O Metriche di rete: misura l'attività tra i client e il file system.
- Metriche del server di storage a oggetti: misura il throughput della rete OSS (Object Storage Server) e l'utilizzo del throughput del disco.
- Metriche relative agli obiettivi di storage degli oggetti: misurano la velocità effettiva del disco OST (Object Storage Target) e l'utilizzo degli IOPS del disco.
- Metriche dei metadati: misurano l'utilizzo della CPU del metadata server (MDS), l'utilizzo degli IOPS del metadata target (MDT) e le operazioni sui metadati dei client.
- Metriche della capacità di archiviazione: misura l'utilizzo della capacità di archiviazione.
- Metriche del data repository S3: misura l'età dei messaggi più vecchi in attesa di essere importati o esportati e rinomina i messaggi elaborati dal file system.

Il diagramma seguente illustra un file system FSx for Lustre, i relativi componenti e le relative categorie metriche.



FSx for Lustre invia dati metrici a intervalli di 1 minuto. CloudWatch

> **Note**
>
> Le metriche potrebbero non essere pubblicate durante le finestre di manutenzione del file system Amazon FSx for Lustre.

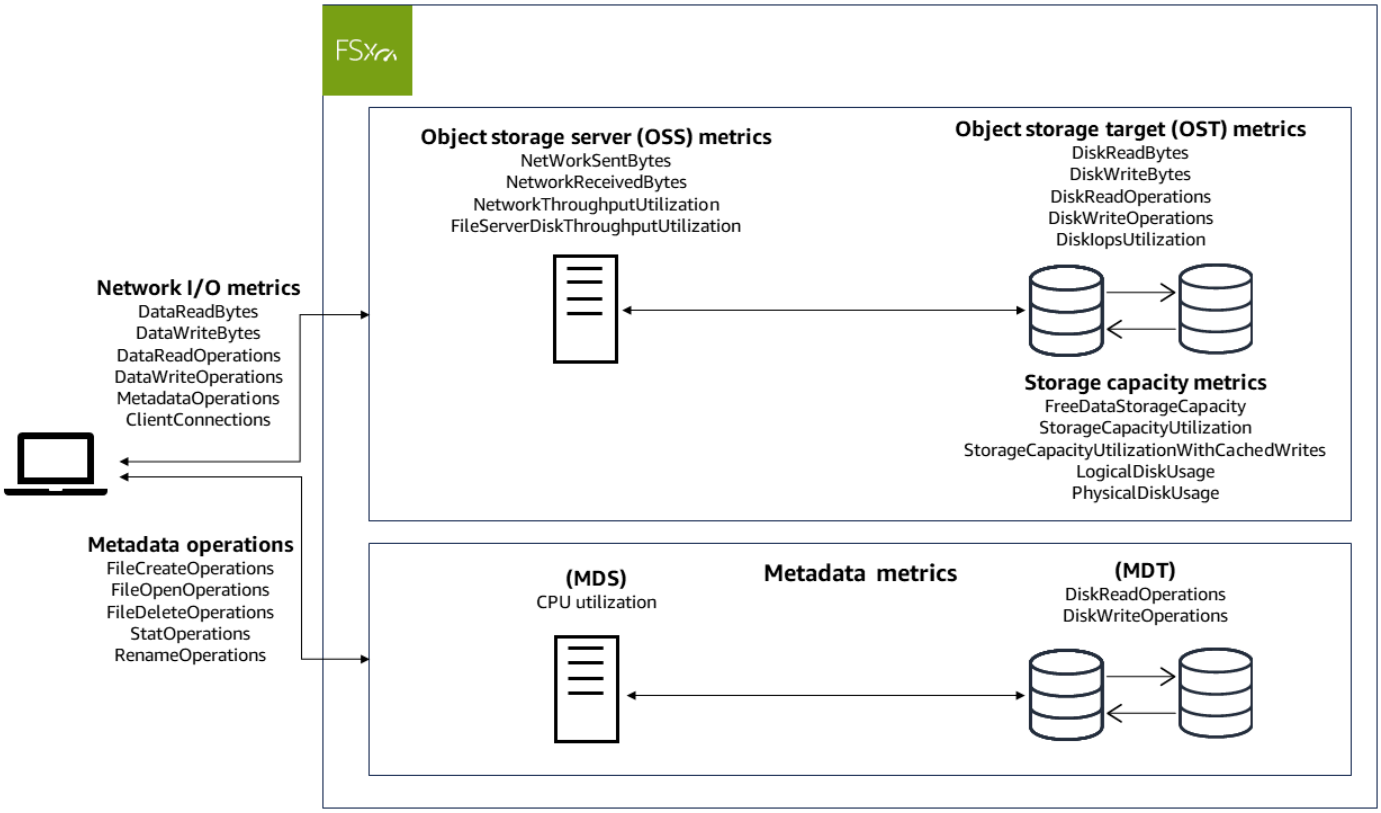
Argomenti

Come usare i parametri di Amazon FSx for Lustre CloudWatch

Esistono due componenti architettonici principali di ogni file system Amazon FSx for Lustre:

- Uno o più server di storage di oggetti (OSSs) che forniscono dati ai client che accedono al file system. Ogni OSS è collegato a uno o più volumi di storage, noti come object storage targets (OSTs), che ospitano i dati nel file system.
- Uno o più server di metadati (MDSs) che forniscono metadati ai client che accedono al file system. Ogni MDS è collegato a un volume di archiviazione, noto come metadata target (MDT), che archivia metadati come nomi di file, directory, autorizzazioni di accesso e layout di file.

FSx for Lustre riporta le metriche CloudWatch che tengono traccia delle prestazioni e dell'utilizzo delle risorse per i server di storage e metadati del file system e i volumi di storage associati.
Il diagramma seguente illustra un file system Amazon FSx for Lustre con i suoi componenti architettonici e le CloudWatch metriche di prestazioni e risorse disponibili per il monitoraggio.



Puoi utilizzare il pannello Monitoraggio e prestazioni sulla dashboard del tuo file system nella console Amazon FSx for Lustre per visualizzare le metriche descritte nelle tabelle seguenti. Per ulteriori informazioni, consulta Accesso alle CloudWatch metriche.

Attività del file system (nella scheda Riepilogo)

Come posso...	Grafico	Parametri rilevanti
... determinare la quantità di capacità di storage disponibile sul mio file system?	Capacità di archiviazione disponibile (byte)	`FreeDataStorageCapacity`
... determinare il throughput totale del client del mio file system?	Throughput totale del client (byte/sec)	SUM (`DataReadBytes +DataWriteBytes )`/ PERIOD (in secondi)

Come posso...	Grafico	Parametri rilevanti
... determinare gli IOPS totali del client del mio file system?	IOPS totali del client (operazioni/sec)	`SUM(DataReadOperations + DataWriteOperations + MetadataOperations )/PERIOD (in seconds)`
... determinare il numero di connessioni stabilite tra i client e il mio file server?	Connessioni client (numero)	`ClientConnections`
... determinare l'utilizzo delle prestazioni dei metadati del mio file system?	Utilizzo degli IOPS dei metadati (percentuale)	`MAX(MDT Disk IOPS)`

Scheda Archiviazione

Come posso...	Grafico	Parametri rilevanti
... determinare la quantità di spazio di archiviazione disponibile?	Capacità di archiviazione disponibile (byte)	`FreeDataStorageCapacity`
... determinare la percentuale di storage utilizzata per il mio file system, escluso lo spazio riservato alle scritture memorizzate nella cache sui client?	Utilizzo totale della capacità di storage (percentuale)	`StorageCapacityUtilization`

Come posso...	Grafico	Parametri rilevanti
... determinare la percentuale di storage utilizzata per il mio file system, incluso lo spazio riservato alle scritture memorizzate nella cache sui client?	Utilizzo totale della capacità di storage (percentuale)	`StorageCapacityUtilizationWithCachedWrites`
... determinare la percentuale di storage utilizzata per il mio file system OSTs escluso lo spazio riservato alle scritture memorizzate nella cache sui client?	Utilizzo totale della capacità di storage per OST (percentuale)	`StorageCapacityUtilization`
... determinare la percentuale di storage utilizzata per il mio file system OSTs, incluso lo spazio riservato alle scritture memorizzate nella cache sui client?	Utilizzo totale della capacità di storage per OST con concessioni ai clienti (percentuale)	`StorageCapacityUtilizationWithCachedWrites`
... determinare il rapporto di compressione dei dati del mio file system?	Risparmi sulla compressione	100* (`LogicalDiskUsage -PhysicalDiskUSage )/LogicalDiskUsage`

Prestazioni dello storage degli oggetti (nella scheda Prestazioni)

Come posso...	Grafico	Parametri rilevanti
... determinare il throughput di rete tra i client e OSSs la percentuale del limite fornito?	Throughput di rete (percentuale)	`NetworkThroughputUtilization`
... determinare la velocità effettiva del disco tra l'OSS e il relativo OSTs sistema operativo come percentuale del limite fornito?	Velocità effettiva del disco (percentuale)	`FileServerDiskThroughputUtilization`
... determinare gli IOPS per le operazioni che prevedono l'accesso OSTs come percentuale del limite previsto?	IOPS del disco (percentuale)	`DiskIopsUtilization`

Prestazioni dei metadati (nella scheda Prestazioni)

Come posso...	Grafico	Parametri rilevanti
... determinare la percentuale di utilizzo della CPU del server di metadati?	Utilizzo della CPU (percentuale)	`CPUUtilization`
... determinare l'utilizzo degli IOPS dei metadati come percentuale del limite fornito?	Utilizzo dei metadati (IOPS)	`MAX(MDT Disk IOPS)`

Accesso alle CloudWatch metriche

Puoi accedere ai parametri di Amazon FSx for Lustre per CloudWatch nei seguenti modi:

- La console Amazon FSx for Lustre.

- La CloudWatch console.
- L'interfaccia CloudWatch a riga di comando (CLI).
- L' CloudWatch API.

Le seguenti procedure mostrano come accedere alle metriche utilizzando questi strumenti.

Utilizzo della console Amazon FSx for Lustre

Per visualizzare i parametri utilizzando la console Amazon FSx for Lustre

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dal pannello di navigazione, scegli File system, quindi scegli il file system con le metriche che desideri visualizzare.
3. Nella pagina di riepilogo, scegli Monitoraggio e prestazioni per visualizzare le metriche relative al tuo file system.

   Nel pannello Monitoraggio e prestazioni sono presenti quattro schede.

   - Scegliete Riepilogo (la scheda predefinita) per visualizzare gli avvisi, gli CloudWatch allarmi e i grafici attivi relativi all'attività del file system.
   - Scegli Archiviazione per visualizzare la capacità di archiviazione, le metriche di utilizzo e gli avvisi attivi.
   - Scegli Performance per visualizzare le metriche delle prestazioni di file server e storage e gli avvisi attivi.
   - Scegli gli CloudWatch allarmi per visualizzare i grafici di tutti gli allarmi configurati per il tuo file system.

Utilizzo della console CloudWatch

Per visualizzare le metriche utilizzando la console CloudWatch

1. Apri la CloudWatch console.
2. Nel riquadro di navigazione, seleziona Parametri.
3. Selezionare lo spazio dei nomi FSx.
4. (Facoltativo) Per visualizzare un parametro, digita il suo nome nel campo di ricerca.

5. (Facoltativo) Per esplorare le metriche, seleziona la categoria che meglio corrisponde alla tua domanda.

Utilizzando il AWS CLI

Per accedere alle metriche da AWS CLI

- Utilizza il comando `list-metrics` con il namespace `--namespace "AWS/FSx"`. Per ulteriori informazioni, consulta la sezione relativa alle informazioni di riferimento ai comandi di AWS CLI.

Utilizzando l'API CloudWatch

Per accedere alle metriche dall'API CloudWatch

- Chiama `GetMetricStatistics`. Per ulteriori informazioni, consulta Amazon CloudWatch API Reference.

Metriche e dimensioni di Amazon FSx for Lustre

Amazon FSx for Lustre pubblica le metriche descritte nelle tabelle seguenti nello spazio dei `AWS/FSx` nomi di CloudWatch Amazon for FSx all for Lustre file system.

Argomenti

FSx I/O per le metriche di rete Lustre

Il `AWS/FSx` namespace include le seguenti metriche di rete. I/O Tutte queste metriche hanno una sola dimensione,. `FileSystemId`

Parametro	Descrizione
`DataReadBytes`	Il numero di byte provenienti dalle letture dei client sul file system. La `Sum` statistica è il numero totale di byte associati alle operazioni di lettura durante il periodo specificato. La `Minimum` statistica è il numero minimo di byte associati alle operazioni di lettura su un singolo OST. La `Maximum` statistica è il numero massimo di byte associati alle operazion i di lettura sull'OST. La `Average` statistica è il numero medio di byte associati alle operazioni di lettura per OST. La `SampleCount` statistica è il numero di. OSTs Per calcolare il throughput medio (byte al secondo) per un periodo, dividi la statistica `Sum` per il numero di secondi in quel periodo. Unità: • Byte per`Sum`,`Minimum`,`Maximum`. `Average` • Conteggio per `SampleCount` . Statistiche valide: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`
`DataWriteBytes`	Il numero di byte generati dalle scritture effettuate dai client sul file system. La statistica `Sum` è il numero totale di byte associato alle operazioni di scrittura. La `Minimum` statistica è il numero minimo di byte associati alle operazioni di scrittura su un singolo OST. La `Maximum` statistica è il numero massimo di byte associati alle operazioni di scrittura sull'OST. La `Average` statistica è il numero medio di byte associati alle operazioni di scrittura per OST. La `SampleCount` statistica è il numero di. OSTs Per calcolare il throughput medio (byte al secondo) per un periodo, dividi la statistica `Sum` per il numero di secondi in quel periodo. Unità: • Byte per`Sum`,`Minimum`,`Maximum`. `Average`

Parametro	Descrizione
	• Conteggio per `SampleCount` . Statistiche valide: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`
`DataRead0 perations`	Il numero di operazioni di lettura. La `Sum` statistica è il numero totale di operazioni di lettura. La `Minimum` statistica è il numero minimo di operazioni di lettura su un singolo OST. La `Maximum` statistica è il numero massimo di operazioni di lettura sull'OST. La `Average` statistica è il numero medio di operazioni di lettura per OST. La `SampleCount` statistica è il numero di. OSTs Per calcolare il numero medio di operazioni di lettura (operazioni al secondo) per un periodo, dividi la `Sum` statistica per il numero di secondi del periodo. Unità: • Conta per`Sum`,`Minimum`, `Maximum``Average`,`SampleCount` .  Statistiche valide: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Parametro	Descrizione
`DataWrite Operations`	Il numero di operazioni di scrittura. La `Sum` statistica è il numero totale di operazioni di scrittura. La `Minimum` statistica è il numero minimo di operazioni di scrittura su un singolo OST. La `Maximum` statistica è il numero massimo di operazion i di scrittura sull'OST. La `Average` statistica è il numero medio di operazioni di scrittura per OST. La `SampleCount` statistica è il numero di. OSTs Per calcolare il numero medio di operazioni di scrittura (operazioni al secondo) per un periodo, dividi la `Sum` statistica per il numero di secondi del periodo. Unità: • Conta per`Sum`,`Minimum`, `Maximum``Average`,`SampleCount` .  Statistiche valide: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`
`Metadata0 perations`	Il numero di operazioni sui metadati. La `Sum` statistica è il numero di operazioni sui metadati. La `Minimum` statistica è il numero minimo di operazioni sui metadati per MDT. La `Maximum` statistica è il numero massimo di operazioni sui metadati per MDT. La `Average` statistica è il numero medio di operazioni sui metadati per MDT. La `SampleCount` statistica è il numero di. MDTs Per calcolare il numero medio di operazioni sui metadati (operazioni al secondo) per un periodo, dividi la `Sum` statistica per il numero di secondi del periodo. Unità: • Conta per`Sum`,`Minimum`,`Maximum`,`Average`. `SampleCount` Statistiche valide: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Parametro	Descrizione
`ClientConnections`	Il numero di connessioni attive tra i client e il file system. Unità: numero

FSx per le metriche del server Lustre Object Storage

Lo spazio dei `AWS/FSx` nomi include le seguenti metriche dell'Object Storage Server (OSS). Tutte queste metriche hanno due dimensioni e. `FileSystemId` `FileServer`

- `FileSystemId`— ID di AWS risorsa del file system.
- `FileServer`— Il nome dell'object storage server (OSS) nel Lustre file system. Ogni OSS è dotato di uno o più obiettivi di storage di oggetti (OSTs). Gli OSS utilizzano la convenzione di denominazione OSS< HostIndex >, dove *`HostIndex`* rappresenta un valore esadecimale a 4 cifre (ad esempio,). `OSS0001` L'ID di un OSS è l'ID del primo OST ad esso allegato. Ad esempio, il primo OSS collegato a `OST0000` e`OST0001`, utilizzerà`OSS0000`, e il secondo OSS collegato a`OST0002`, `OST0003` utilizzerà`OSS0002`.

Parametro	Descrizione
`NetworkThroughputUtilization`	Utilizzo del throughput di rete come percentuale del throughput di rete disponibile per il file system. Questa metrica è equivalente alla somma `NetworkSentBytes` e in percentuale della capacità `NetworkReceivedBytes` di throughput di rete di un sistema operativo per il file system. Viene emessa una metrica ogni minuto per ogni file system. OSSs La `Average` statistica è l'utilizzo medio del throughput di rete per un determinato OSS nel periodo specificato. La `Minimum` statistica è l'utilizzo più basso del throughput di rete per un determinato OSS nell'arco di un minuto, per il periodo specificato.

Parametro	Descrizione
	La `Maximum` statistica è l'utilizzo massimo del throughput di rete per un determinato OSS nell'arco di un minuto, per il periodo specificato. Unità: percentuale Statistiche valide: `Average`, `Minimum`, `Maximum`
`NetworkSentBytes`	Il numero di byte inviati dal file system. Tutto il traffico viene considerato in questa metrica, incluso lo spostamento dei dati da e verso gli archivi di dati collegati . Ogni minuto viene emessa una metrica per ogni file system. OSSs La `Sum` statistica è il numero totale di byte inviati in rete dall'OSS specificato nel periodo specificato. La `Average` statistica è il numero medio di byte inviati in rete dall'OSS specificato nel periodo specificato. La `Minimum` statistica è il numero più basso di byte inviati in rete dall'OSS specificato nel periodo specificato. La `Maximum` statistica è il numero massimo di byte inviati in rete dall'OSS specificato nel periodo specificato. La `Maximum` statistica è il numero massimo di byte inviati in rete dall'OSS specificato nel periodo specificato. Per calcolare la velocità effettiva inviata (byte al secondo) per qualsiasi statistica, dividi la statistica per i secondi nel periodo specificato. Unità: byte Statistiche valide:,,, `Sum` `Average` `Minimum` `Maximum`

Parametro	Descrizione
`NetworkReceivedBytes`	Il numero di byte ricevuti dal file system. Tutto il traffico viene considerato in questa metrica, incluso lo spostamento dei dati da e verso gli archivi di dati collegati . Ogni minuto viene emessa una metrica per ogni file system. OSSs La `Sum` statistica è il numero totale di byte ricevuti in rete dall'OSS specificato nel periodo specificato. La `Average` statistica è il numero medio di byte ricevuti in rete da un determinato OSS nel periodo specificato. La `Minimum` statistica è il numero più basso di byte ricevuti in rete da un determinato OSS nel periodo specificato. La `Maximum` statistica è il numero massimo di byte ricevuti in rete dall'OSS specificato nel periodo specifica to. Per calcolare la velocità effettiva (byte al secondo) per qualsiasi statistica, dividi la statistica per i secondi nel periodo specificato. Unità: byte Statistiche valide:,,, `Sum` `Average` `Minimum` `Maximum`

Parametro	Descrizione
`FileServerDiskThroughputUtilization`	La velocità effettiva del disco tra il sistema operativo e quello associato OSTs, come percentuale del limite fornito determinato dalla capacità di throughput. Questa metrica è equivalente alla somma `DiskReadBytes` e in percentuale della capacità `DiskWriteBytes` di throughput del disco dell'OSS per il file system. Viene emessa una metrica ogni minuto per ogni file system. OSSs La `Average` statistica è l'utilizzo medio del throughput del disco OSS per un determinato OSS nel periodo specificato. La `Minimum` statistica è l'utilizzo più basso del throughput del disco OSS per un determinato OSS nel periodo specificato. La `Maximum` statistica è il massimo utilizzo del throughput del disco OSS per un determinato OSS nel periodo specificato. Unità: percentuale Statistiche valide: `Average`, `Minimum`, `Maximum`

FSx per le metriche di destinazione dello storage di oggetti Lustre

Il `AWS/FSx` namespace include le seguenti metriche OST (Object Storage Target). Tutte queste metriche hanno due dimensioni e. `FileSystemId` `StorageTargetId`

> **Note**
>
> `DiskReadOperationse` le `DiskWriteOperations` metriche non sono disponibili sui file system Scratch e le `DiskIopsUtilization` metriche non sono disponibili sui file system Scratch e Persistent HDD.

Parametro	Descrizione
`DiskReadBytes`	Il numero di byte (disco IO) di qualsiasi disco letti da questo OST. Viene emessa una metrica ogni minuto per ogni file system. OSTs La `Sum` statistica è il numero totale di byte letti in un minuto dall'OST specificato nel periodo specificato. La `Average` statistica è il numero medio di byte letti ogni minuto dall'OST specificato nel periodo specificato. La `Minimum` statistica è il numero più basso di byte letti ogni minuto dall'OST specificato nel periodo specificato. La `Maximum` statistica è il numero massimo di byte letti ogni minuto dall'OST specificato nel periodo specificato. Per calcolare la velocità effettiva del disco di lettura (byte al secondo) per qualsiasi statistica, dividi la statistica per i secondi del periodo. Unità: byte Statistiche valide:`Sum`,, e, `Average` `Minimum` `Maximum`
`DiskWriteBytes`	Il numero di byte (I/O del disco) di qualsiasi disco scritto da questo OST. Viene emessa una metrica ogni minuto per ogni file system. OSTs La `Sum` statistica è il numero totale di byte scritti ogni minuto dall'OST specificato nel periodo specificato. La `Average` statistica è il numero medio di byte scritti ogni minuto dall'OST specificato nel periodo specificato. La `Minimum` statistica è il numero più basso di byte scritti ogni minuto dall'OST specificato nel periodo specificato. La `Maximum` statistica è il numero massimo di byte scritti ogni minuto dall'OST specificato nel periodo specificato.

Parametro	Descrizione
	Per calcolare la velocità effettiva del disco di lettura (byte al secondo) per qualsiasi statistica, dividi la statistica per i secondi del periodo Unità: byte Statistiche valide:`Sum`,, e, `Average` `Minimum` `Maximum`
`DiskRead0perations`	Il numero di operazioni di lettura (IO del disco) su questo OST. Viene emessa una metrica ogni minuto per ogni file system. OSTs La `Sum` statistica è il numero totale di operazioni di lettura eseguite dall'OST specificato nel periodo specificato. La `Average` statistica è il numero medio di operazioni di lettura eseguite ogni minuto dall'OST specificato nel periodo specificato. La `Minimum` statistica è il numero più basso di operazioni di lettura eseguite ogni minuto dall'OST specificato nel periodo specificato. La `Maximum` statistica è il numero massimo di operazioni di lettura eseguite ogni minuto dall'OST specificato nel periodo specificato. Per calcolare gli IOPS medi su disco nel periodo, utilizzate la `Average` statistica e dividete il risultato per 60 (secondi). Unità: numero Statistiche valide:`Sum`,`Average`, e `Minimum` `Maximum`

Parametro	Descrizione
`DiskWriteOperations`	Il numero di operazioni di scrittura (I/O del disco) su questo OST. Viene emessa una metrica ogni minuto per ogni file system. OSTs La `Sum` statistica è il numero totale di operazioni di scrittura eseguite dall'OST specificato nel periodo specificato. La `Average` statistica è il numero medio di operazioni di scrittura eseguite ogni minuto dall'OST specificato nel periodo specificato. La `Minimum` statistica è il numero più basso di operazioni di scrittura eseguite ogni minuto dall'OST specificato nel periodo specificato. La `Maximum` statistica è il numero massimo di operazioni di scrittura eseguite ogni minuto dall'OST specificato nel periodo specificato. Per calcolare gli IOPS medi su disco nel periodo, utilizzate la `Average` statistica e dividete il risultato per 60 (secondi). Unità: numero Statistiche valide:`Sum`,`Average`, e `Minimum` `Maximum`
`DiskIopsUtilization`	L'utilizzo degli IOPS su disco di un OST, come percentuale del limite di IOPS su disco dell'OST. Ogni minuto viene emessa una metrica per ogni file system. OSTs La `Average` statistica è l'utilizzo medio degli IOPS del disco per un determinato OST nel periodo specificato. La `Minimum` statistica è l'utilizzo più basso degli IOPS del disco per un dato OST nel periodo specificato. La `Maximum` statistica è il massimo utilizzo di IOPS del disco per un dato OST nel periodo specificato. Unità: percentuale Statistiche valide:`Average`, e `Minimum` `Maximum`

FSx per le metriche dei metadati Lustre

Il `AWS/FSx` namespace include le seguenti metriche dei metadati. La `CPUUtilization` metrica utilizza le `FileServer` dimensioni `FileSystemId` and, mentre le altre metriche utilizzano le dimensioni and. `FileSystemId` `StorageTargetId`

- `FileSystemId`— ID di AWS risorsa del file system.
- `StorageTargetId`— Il nome del target dei metadati (MDT). MDTs utilizza la convenzione di denominazione di MDT< MDTIndex > (ad esempio,). `MDT0001`
- `FileServer`— Il nome del server di metadati (MDS) nel file system. Lustre Ogni MDS è dotato di un target di metadati (MDT). MDS utilizza la convenzione di denominazione MDS< HostIndex >, dove `HostIndex` rappresenta un valore esadecimale a 4 cifre derivato utilizzando l'indice MDT sul server. Ad esempio, verrà utilizzato il primo MDS con provisioning with e il secondo MDS con provisioning with`MDT0000`. `MDS0000` `MDT0001` `MDS0001` Il file system contiene più server di metadati se è stata specificata una configurazione di metadati.

Parametro	Descrizione
`CPUUtilization`	La percentuale di utilizzo delle risorse della CPU MDS del file system. Ogni minuto viene emessa una metrica per ogni file system. MDSs La `Average` statistica è l'utilizzo medio della CPU dell'MDS in un periodo specificato. La `Minimum` statistica è l'utilizzo più basso della CPU per un determinato MDS nel periodo specificato. La `Maximum` statistica è l'utilizzo massimo della CPU per il dato MDS nel periodo specificato. Unità: percentuale

Parametro	Descrizione
	Statistiche valide: e `Average` `Minimum` `Maximum`
`FileCreateOperations`	Numero totale di operazioni di creazione di file. Unità: numero
`FileOpenOperations`	Numero totale di operazioni di apertura dei file. Unità: numero
`FileDeleteOperations`	Numero totale di operazioni di eliminazione dei file. Unità: numero
`StatOperations`	Numero totale di operazioni di statistica. Unità: numero
`RenameOperations`	Numero totale di ridenominazioni di directory, che si tratti di ridenominazioni di directory sul posto o ridenominazioni tra directory. Unità: numero

FSx per i parametri della capacità di archiviazione di Lustre

Il `AWS/FSx` namespace include le seguenti metriche della capacità di archiviazione. Tutte queste metriche hanno due dimensioni, `FileSystemId` `StorageTargetId` ad eccezione delle `PhysicalDiskUsage` quali `LogicalDiskUsage` la dimensione. `FileSystemId`

Parametro	Descrizione
`FreeDataStorageCapacity`	La quantità di capacità di archiviazione disponibile in questo OST. Ogni minuto viene emessa una metrica per ogni file system. OSTs La `Sum` statistica è il numero totale di byte disponibili nell'OST specificato nel periodo specificato. La `Average` statistica è il numero medio di byte disponibi li nell'OST specificato nel periodo specificato. La `Minimum` statistica è il numero più basso di byte disponibili nell'OST specificato nel periodo specificato. La `Maximum` statistica è il numero massimo di byte disponibili nell'OST specificato nel periodo specificato. Unità: byte Statistiche valide:`Sum`,`Average`, e `Minimum` `Maximum`
`StorageCapacityUtilization`	L'utilizzo della capacità di archiviazione per un determina to file system OST. Viene emessa una metrica ogni minuto per ogni file system. OSTs La `Average` statistica è la quantità media di utilizzo della capacità di storage per un determinato OST in un determinato periodo. La `Minimum` statistica è la quantità minima di utilizzo della capacità di storage per un determinato OST in un determinato periodo. La `Maximum` statistica è la quantità massima di utilizzo della capacità di archiviazione per un determinato OST in un periodo specificato. Unità: percentuale

Parametro	Descrizione
	Statistiche valide: `Average`, `Minimum`, `Maximum`
`StorageCapacityUtilizationWithCachedWrites`	L'utilizzo della capacità di archiviazione per un determinato file system OST, incluso lo spazio riservato alle scritture memorizzate nella cache sul client. Ogni minuto viene emessa una metrica per ogni file system. OSTs La `Average` statistica è la quantità media di utilizzo della capacità di storage per un determinato OST in un determinato periodo. La `Minimum` statistica è la quantità minima di utilizzo della capacità di storage per un determinato OST in un determinato periodo. La `Maximum` statistica è la quantità massima di utilizzo della capacità di archiviazione per un determinato OST in un periodo specificato. Unità: percentuale Statistiche valide: `Average`, `Minimum`, `Maximum`

Parametro	Descrizione
`LogicalDiskUsage`	La quantità di dati logici archiviati (non compressi). La `Sum` statistica è il numero totale di byte logici memorizzati nel file system. La `Minimum` statistica è il numero minimo di byte logici memorizzati in un OST nel file system. La `Maximum` statistica è il maggior numero di byte logici memorizzati in un OST nel file system. La `Average` statistica è il numero medio di byte logici memorizzati per OST. La `SampleCount` statistica è il numero di. OSTs Unità: • Byte per`Sum`,`Minimum`. `Maximum` • Conteggio per `SampleCount` . Statistiche valide: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

Parametro	Descrizione
`PhysicalDiskUsage`	La quantità di storage occupata fisicamente dai dati del file system (compressi). La `Sum` statistica è il numero totale di byte occupati OSTs nel file system. La `Minimum` statistica è il numero totale di byte occupati nell'OST più vuoto. La `Maximum` statistica è il numero totale di byte occupati nell'OST più completo. La `Average` statistica è il numero medio di byte occupati per OST. La `SampleCount` statistica è il numero di. OSTs Unità: • Byte per`Sum`,`Minimum`. `Maximum` • Conteggio per `SampleCount` . Statistiche valide: `Sum`, `Minimum`, `Maximum`, `Average`, `SampleCount`

FSx per le metriche del repository Lustre S3

FSx for Lustre pubblica le seguenti metriche `AutoImport` (importazione automatica) e `AutoExport` (esportazione automatica) nello spazio dei nomi in. `FSx` CloudWatch Queste metriche utilizzano le dimensioni per consentire misurazioni più granulari dei dati. Tutte `AutoImport` le `AutoExport` metriche hanno le dimensioni e. `FileSystemId` `Publisher`

Parametro	Descrizione
`AgeOfOldestQueuedMessage` Dimensione: `AutoExport`	L'età, in secondi, del messaggio più vecchio in attesa di essere esportato. La `Average` statistica è l'età media del messaggio più vecchio in attesa di essere esportato. La `Maximum` statistica è il numero massimo di secondi di permanenza di un

Parametro	Descrizione
	messaggio nella coda di esportazione. La `Minimum` statistica è il numero minimo di secondi di permanenza di un messaggio nella coda di esportazione. Il valore zero indica che nessun messaggio è in attesa di essere esportato. Unità: secondi Statistiche valide: `Average`, `Minimum`, `Maximum`
`RepositoryRenameOperations` Dimensione: `AutoExport`	Il numero di ridenominazioni elaborate dal file system in risposta a una ridenominazione di directory più grande. La `Sum` statistica è il numero totale di operazioni di ridenominazione risultant i dalla ridenominazione di una directory. La `Average` statistica è il numero medio di operazioni di ridenominazione per il file system. La `Maximum` statistica è il numero massimo di operazioni di ridenomin azione associate alla ridenominazione di una directory nel file system. La `Minimum` statistica è il numero minimo di ridenomin azioni associate alla ridenominazione di una directory nel file system. Unità: numero Statistiche valide:`Sum`,,,, `Average` `Minimum` `Maximum`

Parametro	Descrizione
`AgeOfOldestQueuedMessage` Dimensione: `AutoImport`	L'età, in secondi, del messaggio più vecchio in attesa di essere importato. La `Average` statistica è l'età media del messaggio più vecchio in attesa di essere importato. La `Maximum` statistica è il numero massimo di secondi di permanenza di un messaggio nella coda di importazione. La `Minimum` statistica è il numero minimo di secondi di permanenza di un messaggio nella coda di importazione. Il valore zero indica che nessun messaggio è in attesa di essere importato. Unità: secondi Statistiche valide: `Average`, `Minimum`, `Maximum`

FSx per le dimensioni Lustre

Le metriche di Amazon FSx for Lustre utilizzano lo spazio dei `AWS/FSx` nomi e utilizzano le seguenti dimensioni.

- La `FileSystemId` dimensione indica l'ID di un file system e filtra le metriche richieste per quel singolo file system. Puoi trovare l'ID sulla FSx console Amazon nel pannello Riepilogo della pagina dei dettagli del file system, nel campo ID del file system. L'ID del file system assume la forma di*`fs-01234567890123456`*. Puoi anche vedere l'ID nella risposta di un comando `describe-file-systems`CLI (l'azione API equivalente è `DescribeFileSystems`).
- La `StorageTargetId` dimensione indica quale OST (object storage target) o MDT (metadata target) ha pubblicato le metriche dei metadati. A `StorageTargetId` assume la forma di `OSTxxxx` (ad esempio,`OST0001`) o `MDTxxxx` (ad esempio,). `MDT0001`
- La `FileServer` dimensione indica quanto segue
  - Per le metriche OSS: il nome dell'object storage server (OSS). Gli OSS utilizzano la convenzione `OSSxxxx` di denominazione (ad esempio,`OSS0002`).

  - Per la CPUUtilization metrica: il nome di un server di metadati (MDS). MDS utilizza la convenzione di `MDSxxxx` denominazione (ad esempio,). `MDS0002`
- La `Publisher` dimensione è disponibile in CloudWatch e AWS CLI per le `AutoImport` metriche `AutoImport` and per indicare quale servizio ha pubblicato le metriche.

Per ulteriori informazioni sulle dimensioni, consulta Dimensions nella Amazon CloudWatch User Guide.

Avvertenze e consigli sulle prestazioni

FSx for Lustre visualizza un avviso relativo alle CloudWatch metriche quando una di queste metriche si avvicina o supera una soglia predeterminata per più punti dati consecutivi. Questi avvisi forniscono consigli pratici che è possibile utilizzare per ottimizzare le prestazioni del file system.

Gli avvisi sono accessibili in diverse aree della dashboard di monitoraggio e prestazioni sulla console Amazon FSx for Lustre. Tutti gli avvisi e gli CloudWatch allarmi FSx sulle prestazioni di Amazon attivi o recenti configurati per il file system che si trovano in uno stato di allarme vengono visualizzati nel pannello Monitoraggio e prestazioni nella sezione Riepilogo. L'avviso viene visualizzato anche nella sezione del pannello di controllo in cui è visualizzato il grafico metrico. Questi avvisi scompaiono automaticamente dalla dashboard 24 ore dopo che le metriche sottostanti scendono al di sotto della soglia di avviso.

Puoi creare CloudWatch allarmi per qualsiasi parametro di Amazon FSx . Per ulteriori informazioni, consulta Creazione di CloudWatch allarmi per monitorare le metriche.

Utilizza gli avvisi sulle prestazioni per migliorare le prestazioni del file system

Amazon FSx fornisce consigli pratici che puoi utilizzare per ottimizzare le prestazioni del tuo file system. Puoi intraprendere l'azione consigliata se prevedi che il problema persista o se sta causando un impatto sulle prestazioni del tuo file system. A seconda del parametro che ha generato un avviso, puoi risolverlo aumentando la capacità di throughput, la capacità di archiviazione o gli IOPS dei metadati del file system, come descritto nella tabella seguente.

Sezione Dashboard	Se è presente un avviso per questa metrica	Esegui questa operazione
Storage	`Storage capacity utilization`	Aumenta la capacità di archiviazione del file system.

Sezione Dashboard	Se è presente un avviso per questa metrica	Esegui questa operazione
		Se l'utilizzo della capacità di storage è superiore solo per un sottoinsieme degli Object Storage Targets (OSTs) del file system, puoi anche ribilanciare il carico di lavoro in modo che l'utilizzo della capacità di storage sia bilanciato in modo più uniforme su tutto il file system.
	`Storage capacity utilization with cached writes`	Riducete le dimensioni della cache di scrittura del client configurando il parametro max_dirty_mb sui client.
Prestazioni dello storage degli oggetti	`Network throughput`	Aumenta la capacità di trasmissione del file system. Se l'utilizzo della velocità effettiva è maggiore per un sottoinsieme degli Object Storage Server (OSSs) del file system, è possibile anche ribilanciare il carico di lavoro in modo che l'utilizzo della velocità effettiva sia bilanciato in modo più uniforme su tutto il file system.

Sezione Dashboard	Se è presente un avviso per questa metrica	Esegui questa operazione
	`Disk throughput`	Aumentate la capacità di throughput del file system. Se l'utilizzo della velocità effettiva del disco è maggiore per un sottoinsieme degli Object Storage Server (OSSs) del file system, è anche possibile ribilanciare il carico di lavoro in modo che l'utilizzo della velocità effettiva del disco sia bilanciato in modo più uniforme su tutto il file system.
	`Disk IOPS`	Aumentate la capacità di storage del file system. Se l'utilizzo degli IOPS su disco è maggiore per un sottoinsieme degli Object Storage Targets (OSTs) del file system, puoi anche ribilanciare il carico di lavoro in modo che l'utilizzo degli IOPS del disco sia bilanciato in modo più uniforme su tutto il file system.

Sezione Dashboard	Se è presente un avviso per questa metrica	Esegui questa operazione
Prestazioni dei metadati	`CPU utilization`	Aumenta la capacità di archiviazione del file system. Se è necessario scalare le prestazioni dei metadati indipendentemente dalla capacità di storage, è possibile migrare a un nuovo file system che supporti il provisioning delle prestazioni dei metadati indipendentemente dalla capacità di storage utilizzata dal parametro. MetadataConfiguration
	`Metadata IOPS`	Aumentate gli IOPS dei metadati del file system.

Per ulteriori informazioni sulle prestazioni del file system, consulta. Prestazioni FSx di Amazon for Lustre

Creazione di CloudWatch allarmi per monitorare le metriche

Puoi creare un CloudWatch allarme che invia un messaggio Amazon SNS quando l'allarme cambia stato. Un allarme controlla una singola metrica in un periodo di tempo specificato ed esegue una o più azioni in base al valore della metrica rispetto a una determinata soglia in un periodo di tempo specificato. L'azione è una notifica inviata a un argomento di Amazon SNS o a una policy di Auto Scaling.

Gli allarmi richiamano azioni solo per modifiche di stato sostenute. CloudWatch gli allarmi non richiamano azioni perché si trovano in uno stato particolare. Lo stato deve cambiare e rimanere tale per un periodo di tempo specificato. Puoi creare un allarme sulla FSx console Amazon o sulla CloudWatch console.

Le seguenti procedure descrivono come creare allarmi per Amazon FSx for Lustre utilizzando la console e AWS CLI l'API.

Per impostare allarmi utilizzando la console Amazon FSx for Lustre

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dal pannello di navigazione, scegli File system, quindi scegli il file system per cui desideri creare l'allarme.
3. Nella pagina di riepilogo, scegli Monitoraggio e prestazioni.
4. Scegli Crea CloudWatch allarme. Sarai reindirizzato alla console CloudWatch.
5. Scegli Seleziona metriche e scegli Avanti.
6. Nella sezione Metriche, scegli FSX.
7. Scegli Metriche del file system, scegli la metrica per cui desideri impostare l'allarme, quindi scegli Seleziona metrica.
8. Nella sezione Condizioni, scegli le condizioni per l'allarme e scegli Avanti.

   > **Note**
   >
   > Le metriche potrebbero non essere pubblicate durante la manutenzione del file system. Per evitare modifiche non necessarie e fuorvianti delle condizioni di allarme e per configurare gli allarmi in modo che siano resistenti ai punti dati mancanti, consulta Configurazione del modo in cui gli CloudWatch allarmi trattano i dati mancanti nella Amazon User Guide. CloudWatch

9. Se desideri CloudWatch inviarti un'e-mail o una notifica SNS quando lo stato di allarme attiva l'azione, scegli Ogni volta che si verifica questo stato di allarme.

   Per Seleziona un argomento SNS, scegli un argomento SNS esistente. Se selezioni Crea argomento, puoi impostare il nome e gli indirizzi e-mail per un nuovo elenco di sottoscrizioni e-mail. Questo elenco viene salvato e visualizzato nel campo per allarmi futuri. Scegli Next (Successivo).

   > **Warning**
   >
   > Se usi Crea argomento per creare un nuovo argomento Amazon SNS, gli indirizzi e-mail devono essere verificati prima di poter ricevere le notifiche. Le e-mail sono inviate solo

quando viene attivato lo stato di allarme. Se lo stato cambia prima della verifica degli indirizzi e-mail, questi non riceveranno una notifica.

10. Inserisci i valori Name, Description e Whenever per la metrica e scegli Avanti.
11. Nella pagina di anteprima e creazione, esamina l'avviso e scegli Crea allarme.

Per impostare allarmi utilizzando la console CloudWatch

1. Accedi a AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegli Crea allarme per avviare la procedura guidata di creazione di allarme.
3. Scegli FSx Metriche per individuare una metrica. Per restringere i risultati, puoi cercare l'ID del tuo file system. Seleziona la metrica per cui desideri creare un allarme e scegli Avanti.
4. Inserisci un nome e una descrizione e scegli un valore Whenever per la metrica.
5. Se desideri CloudWatch inviarti un'e-mail quando viene raggiunto lo stato di allarme, scegli State is ALARM per Ogni volta che si verifica questo allarme. Per Invia notifica a:, scegliere un argomento SNS esistente. Se selezioni Crea argomento, puoi impostare i nomi e gli indirizzi e-mail per un nuovo elenco di abbonamenti e-mail. Questo elenco viene salvato e visualizzato nel campo per allarmi futuri.

   > **Warning**
   >
   > Se usi Crea argomento per creare un nuovo argomento Amazon SNS, gli indirizzi e-mail devono essere verificati prima di poter ricevere le notifiche. Le e-mail sono inviate solo quando viene attivato lo stato di allarme. Se lo stato cambia prima della verifica degli indirizzi e-mail, questi non riceveranno una notifica.

6. Visualizza l'anteprima dell'avviso, quindi scegli Crea allarme o torna indietro per apportare modifiche.

Per impostare una sveglia usando il AWS CLI

- Chiamare `put-metric-alarm`. Per ulteriori informazioni, consulta il Riferimento ai comandi AWS CLI.

Per impostare una sveglia utilizzando il CloudWatch

- Chiama `PutMetricAlarm`. Per ulteriori informazioni, consulta Amazon CloudWatch API Reference.

Registrazione con Amazon CloudWatch Logs

FSx for Lustre supporta la registrazione di eventi di errore e avviso per gli archivi di dati associati al tuo file system su Amazon Logs. CloudWatch

> **Note**
>
> La registrazione con Amazon CloudWatch Logs è disponibile solo sui file system Amazon FSx for Lustre creati dopo le 15:00 PST del 30 novembre 2021.

Argomenti

Panoramica sulla registrazione

Se disponi di repository di dati collegati al file system FSx for Lustre, puoi abilitare la registrazione degli eventi del repository di dati su Amazon Logs. CloudWatch Gli eventi di errore e avviso possono essere registrati dalle seguenti operazioni di archiviazione dei dati:

- Esportazione automatica
- Attività di archiviazione dei dati

Per ulteriori informazioni su queste operazioni e sul collegamento agli archivi di dati, vedere. Utilizzo di repository di dati con Amazon FSx for Lustre

Puoi configurare i livelli di registro registrati da Amazon FSx , ovvero se Amazon FSx registrerà solo gli eventi di errore, solo gli eventi di avviso o entrambi gli eventi di errore e di avviso. Puoi anche disattivare la registrazione degli eventi in qualsiasi momento.

> **Note**
>
> Si consiglia vivamente di abilitare i log per i file system a cui sono associati qualsiasi livello di funzionalità critiche.

Destinazioni dei log

Quando la registrazione è abilitata, FSx for Lustre deve essere configurato con una destinazione Amazon CloudWatch Logs. La destinazione del registro degli eventi è un gruppo di log Amazon CloudWatch Logs e Amazon FSx crea un flusso di log per il tuo file system all'interno di questo gruppo di log. CloudWatch Logs consente di archiviare, visualizzare e cercare i log degli eventi di controllo nella CloudWatch console Amazon, eseguire query sui log utilizzando CloudWatch Logs Insights e attivare CloudWatch allarmi o funzioni Lambda.

Scegli la destinazione del registro quando crei il file system FSx for Lustre o successivamente aggiornandolo. Per ulteriori informazioni, consulta Gestione della registrazione.

Per impostazione predefinita, Amazon FSx creerà e utilizzerà un gruppo di log CloudWatch Logs predefinito nel tuo account come destinazione del registro degli eventi. Se desideri utilizzare un gruppo di log CloudWatch Logs personalizzato come destinazione del registro degli eventi, ecco i requisiti per il nome e la posizione della destinazione del registro degli eventi:

- Il nome del gruppo di CloudWatch log Logs deve iniziare con il `/aws/fsx/` prefisso.
- Se non disponi di un gruppo di log CloudWatch Logs esistente quando crei o aggiorni un file system sulla console, Amazon FSx for Lustre può creare e utilizzare un flusso di log predefinito nel gruppo di log CloudWatch Logs. `/aws/fsx/lustre` Il flusso di log verrà creato con il formato `datarepo_`*`file_system_id`* (ad esempio,). `datarepo_fs-0123456789abcdef0`
- Se non si desidera utilizzare il gruppo di log predefinito, l'interfaccia utente di configurazione consente di creare un gruppo di log CloudWatch Logs quando si crea o si aggiorna il file system sulla console.
- Il gruppo di log CloudWatch Logs di destinazione deve trovarsi nella stessa AWS partizione e nel file Account AWS system Amazon FSx for Lustre. Regione AWS

Puoi modificare la destinazione del registro degli eventi in qualsiasi momento. Quando si esegue questa operazione, i nuovi registri degli eventi vengono inviati solo alla nuova destinazione.

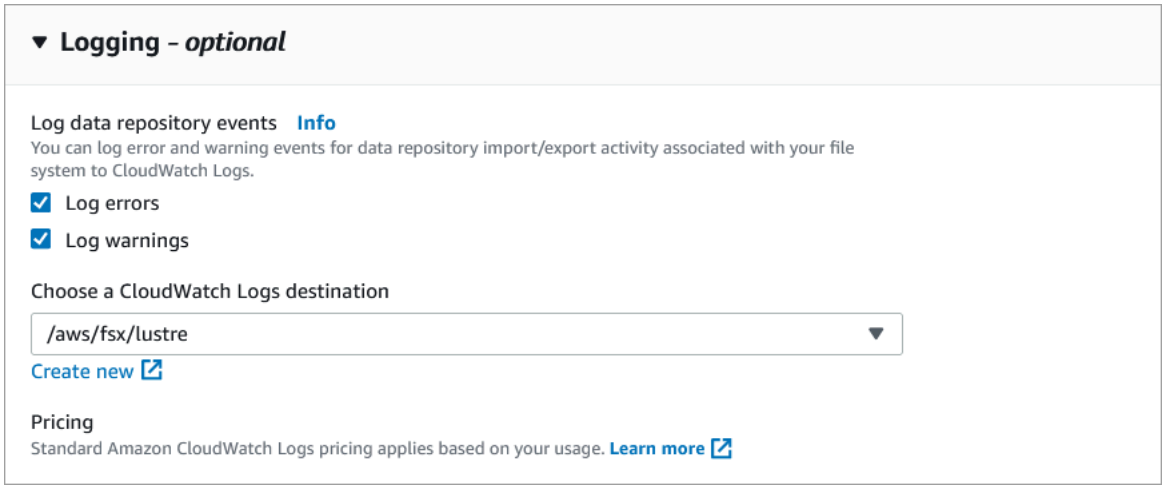
Gestione della registrazione

È possibile abilitare la registrazione quando si crea un nuovo file system FSx for Lustre o successivamente aggiornandolo. La registrazione è attivata per impostazione predefinita quando crei un file system dalla console Amazon FSx . Tuttavia, la registrazione è disattivata per impostazione predefinita quando si crea un file system con l'API o AWS CLI Amazon FSx .

Sui file system esistenti che hanno la registrazione abilitata, puoi modificare le impostazioni di registrazione degli eventi, incluso il livello di registro per cui registrare gli eventi e la destinazione del registro. Puoi eseguire queste attività utilizzando la FSx console Amazon o AWS CLI l' FSx API Amazon.

Per abilitare la registrazione durante la creazione di un file system (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo file system descritta Passaggio 1: crea il tuo FSx file system for Lustre nella sezione Guida introduttiva.
3. Apri la sezione Registrazione (opzionale). La registrazione è abilitata per impostazione predefinita.



4. Continuare con la sezione successiva della procedura guidata per la creazione del file system.

Quando il file system diventa Disponibile, la registrazione verrà abilitata.

Per abilitare la registrazione durante la creazione di un file system (CLI)

1. Quando si crea un nuovo file system, utilizzate la `LogConfiguration` proprietà con l'CreateFileSystemoperazione per abilitare la registrazione per il nuovo file system.

```
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. Quando il file system diventa Disponibile, la funzionalità di registrazione verrà abilitata.

Per modificare la configurazione di registrazione (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli Lustre file system per cui desideri gestire la registrazione.
3. Scegli la scheda Archivio dati.
4. Nel pannello Registrazione, scegliete Aggiorna.
5. Nella finestra di dialogo di configurazione della registrazione degli aggiornamenti, modificate le impostazioni desiderate.
   a. Scegliete Registra errori per registrare solo gli eventi di errore o Registra avvisi per registrare solo gli eventi di avviso o entrambi. La registrazione è disattivata se non effettui una selezione.
   b. Scegli una destinazione di registro CloudWatch dei registri esistente o creane una nuova.
6. Seleziona Salva.

Per modificare la configurazione di registrazione (CLI)

- Utilizza il comando `update-file-system`CLI o l'operazione `UpdateFileSystem`API equivalente.

```
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"}"
```

Visualizzazione dei registri

Puoi visualizzare i log dopo che Amazon FSx ha iniziato a emetterli. Puoi visualizzare i log come segue:

- Puoi visualizzare i log accedendo alla CloudWatch console Amazon e scegliendo il gruppo di log e il flusso di log a cui vengono inviati i log degli eventi. Per ulteriori informazioni, consulta Visualizza i dati di log inviati a CloudWatch Logs nella Amazon CloudWatch Logs User Guide.
- Puoi utilizzare CloudWatch Logs Insights per cercare e analizzare in modo interattivo i tuoi dati di log. Per ulteriori informazioni, consulta Analyzing log data with CloudWatch Logs Insights, nella Amazon CloudWatch Logs User Guide.
- Puoi anche esportare i log in Amazon S3. Per ulteriori informazioni, consulta Esportazione dei dati di log in Amazon S3, nella CloudWatch Amazon Logs User Guide.

Per ulteriori informazioni sui motivi dell'errore, consulta. Registri degli eventi del data repository

Registrazione FSx per le chiamate dell'API Lustre con AWS CloudTrail

Amazon FSx for Lustre è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon FSx for Lustre. CloudTrail acquisisce tutte le chiamate API per Amazon FSx for Lustre come eventi. Le chiamate acquisite includono le chiamate dalla console Amazon FSx for Lustre e le chiamate in codice alle operazioni dell'API Amazon FSx for Lustre.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon FSx for Lustre. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console in Cronologia eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata ad Amazon FSx for Lustre. Puoi determinare l'indirizzo IP da cui è stata effettuata la richiesta, l'autore della richiesta, il momento in cui è stata effettuata e i dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la Guida per l'AWS CloudTrail utente.

Informazioni su Amazon FSx for Lustre in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività dell'API in Amazon FSx for Lustre, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Amazon FSx for Lustre, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il trail registra gli eventi di tutte le AWS regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente di AWS CloudTrail :

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le chiamate API Amazon FSx for Lustre vengono registrate da. CloudTrail Ad esempio, le chiamate alle `TagResource` operazioni `CreateFileSystem` and generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail UserIdentity nella Guida per l'AWS CloudTrail utente.

Informazioni sulle voci dei file di registro di Amazon FSx for Lustre

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra il `TagResource` funzionamento quando viene creato un tag per un file system dalla console.

```
{
    "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”
}
```

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`UntagResource`azione che si verifica quando un tag per un file system viene eliminato dalla console.

```
{
    "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"
}
```

Migrazione ad Amazon FSx for Lustre utilizzando AWS DataSync

È possibile utilizzarlo AWS DataSync per trasferire dati tra i file FSx system Lustre. DataSync è un servizio di trasferimento dati che semplifica, automatizza e accelera lo spostamento e la replica dei dati tra sistemi di archiviazione autogestiti e AWS servizi di archiviazione su Internet o. AWS Direct Connect DataSync può trasferire i dati e i metadati del file system, come proprietà, timestamp e autorizzazioni di accesso.

Come migrare i file esistenti su for Lustre utilizzando FSx AWS DataSync

Puoi utilizzare i file system DataSync with FSx for Lustre per eseguire migrazioni di dati una tantum, importare periodicamente dati per carichi di lavoro distribuiti e pianificare la replica per la protezione e il ripristino dei dati. Per informazioni su scenari di trasferimento specifici, vedi Dove posso trasferire i miei dati? AWS DataSync nella Guida AWS DataSync per l'utente.

Prerequisiti

Per migrare i dati nella configurazione di FSx for Lustre, sono necessari un server e una rete che soddisfino i DataSync requisiti. Per ulteriori informazioni, consulta Configurazione con AWS DataSync nella Guida per l'AWS DataSync utente.

- È stata creata una destinazione FSx per il file system Lustre. Per ulteriori informazioni, consulta Passaggio 1: crea il tuo FSx file system for Lustre.
- I file system di origine e di destinazione sono collegati nello stesso cloud privato virtuale (VPC). Il file system di origine può trovarsi in locale o in un altro Amazon VPC Account AWS, Regione AWS oppure, ma deve trovarsi in una rete peerizzata con quella del file system di destinazione utilizzando Amazon VPC Peering, Transit Gateway o. AWS Direct Connect AWS VPN Per ulteriori informazioni, consulta Che cos'è il peering di VPC? nella Amazon VPC Peering Guide.

> **Note**
>
> DataSync può effettuare il trasferimento da o Account AWS verso FSx For Lustre solo se l'altra sede di trasferimento è Amazon S3.

Passaggi di base per la migrazione dei file utilizzando DataSync

Il trasferimento di file da un'origine a una destinazione utilizzando DataSync prevede i seguenti passaggi di base:

1. Scaricate e installate un agente nel vostro ambiente e attivatelo (non necessario in caso di trasferimento da un ambiente all'altro). Servizi AWS
2. Crea una posizione di origine e una di destinazione.
3. Creare un'attività.
4. Eseguire l'attività per trasferire i file dall'origine alla destinazione.

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente AWS DataSync :

- Trasferimento tra storage locale e AWS
- Configurazione dei AWS DataSync trasferimenti con Amazon FSx for Lustre.
- Implementazione del tuo agente Amazon EC2

Sicurezza in Amazon FSx for Lustre

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Amazon Web Services Cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per saperne di più sui programmi di conformità che si applicano a Amazon FSx for Lustre, vedi AWS Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa durante l'utilizzo Amazon FSx for Lustre. I seguenti argomenti mostrano come configurare Amazon per FSx soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri servizi Amazon che ti aiutano a monitorare e proteggere i tuoi Amazon FSx for Lustre risorse.

Di seguito, è possibile trovare una descrizione delle considerazioni relative alla sicurezza con cui lavorare Amazon FSx.

Argomenti

Protezione dei dati in Amazon FSx for Lustre

Il modello di responsabilità AWS condivisa modello di si applica alla protezione dei dati in Amazon FSx for Lustre. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon FSx o altro Servizi AWS utilizzando la console AWS CLI, l'API o AWS SDKs. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Argomenti

Crittografia dei dati in Amazon FSx for Lustre

Amazon FSx for Lustre supporta due forme di crittografia per i file system, la crittografia dei dati inattivi e la crittografia in transito. La crittografia dei dati inattivi viene abilitata automaticamente durante la creazione di un FSx file system Amazon. La crittografia dei dati in transito viene abilitata automaticamente quando accedi a un FSx file system Amazon da EC2 istanze Amazon che supportano questa funzionalità.

Quando usare la crittografia

Se la tua organizzazione è soggetta a politiche aziendali o normative che richiedono la crittografia dei dati e dei metadati inattivi, ti consigliamo di creare un file system crittografato e di montare il file system utilizzando la crittografia dei dati in transito.

Per ulteriori informazioni sulla creazione di un file system crittografato a riposo utilizzando la console, consulta Create your Amazon FSx for Lustre file system.

Argomenti

Crittografia dei dati a riposo

La crittografia dei dati inattivi viene abilitata automaticamente quando crei un Amazon FSx for Lustre file system tramite AWS Management Console AWS CLI, il o programmaticamente tramite l' FSx API Amazon o uno dei. AWS SDKs Un'azienda potrebbe richiedere la crittografia di tutti i dati che soddisfano una determinata classificazione o sono associati a una determinata applicazione, carico di lavoro o ambiente. Se crei un file system persistente, puoi specificare la AWS KMS chiave con cui crittografare i dati. Se crei un file system scratch, i dati vengono crittografati utilizzando chiavi gestite da Amazon FSx. Per ulteriori informazioni sulla creazione di un file system crittografato a riposo utilizzando la console, consulta Create your Amazon FSx for Lustre file system.

> **Note**
>
> L'infrastruttura di gestione delle AWS chiavi utilizza algoritmi crittografici approvati dal Federal Information Processing Standards (FIPS) 140-2. L'infrastruttura è compatibile con le raccomandazioni National Institute of Standards and Technology (NIST) 800-57.

Per ulteriori informazioni sulle modalità di utilizzo di Lustre, FSx vedere. AWS KMSIn che modo Amazon FSx for Lustre utilizza AWS KMS

Come funziona la crittografia dei dati memorizzati su disco

In un file system crittografato, i dati e i metadati vengono automaticamente crittografati prima di essere scritti sul file system. Analogamente, quando i dati e i metadati vengono letti, sono automaticamente decifrati prima di essere presentati all'applicazione. Questi processi sono gestiti in modo trasparente da Amazon FSx for Lustre, quindi non è necessario modificare le applicazioni.

Amazon FSx for Lustre utilizza l'algoritmo di crittografia AES-256 standard del settore per crittografare i dati del file system inattivi. Per ulteriori informazioni, consulta Elementi di base di crittografia nella Guida per sviluppatori di AWS Key Management Service .

In che modo Amazon FSx for Lustre utilizza AWS KMS

Amazon FSx for Lustre crittografa automaticamente i dati prima che vengano scritti nel file system e decrittografa automaticamente i dati man mano che vengono letti. I dati vengono crittografati utilizzando un codice a blocchi XTS-AES-256. Tutti i file system di scratch FSx for Lustre sono crittografati quando sono inattivi con chiavi gestite da. AWS KMSAmazon FSx for Lustre si integra con AWS KMS per la gestione delle chiavi. Le chiavi utilizzate per crittografare i file system scratch inattivi sono uniche per ogni file system e vengono distrutte dopo l'eliminazione del file system. Per i file system persistenti, scegli la chiave KMS utilizzata per crittografare e decrittografare i dati. È necessario specificare la chiave da utilizzare quando si crea un file system persistente. Puoi abilitare, disabilitare o revocare le concessioni su questa chiave KMS. Questa chiave KMS può essere di uno dei due tipi seguenti:

- Chiave gestita da AWS per Amazon FSx: questa è la chiave KMS predefinita. Non ti viene addebitato alcun costo per creare e archiviare una chiave KMS, ma ci sono costi di utilizzo. Per ulteriori informazioni, consulta Prezzi di AWS Key Management Service.
- Chiave gestita dal cliente – Questa è la chiave KMS più flessibile da usare, perché è possibile configurare le policy della chiave e i permessi per più utenti o servizi. Per ulteriori informazioni sulla

creazione di chiavi gestite dai clienti, consulta Creazione di chiavi nella Guida per gli AWS Key Management Service sviluppatori.

Se utilizzi una chiave gestita dal cliente come chiave KMS per la crittografia e la decrittografia dei dati dei file, puoi abilitare la rotazione delle chiavi. Quando abiliti la rotazione delle chiavi, la ruota AWS KMS automaticamente una volta all'anno. Inoltre, con una chiave gestita dal cliente, è possibile scegliere quando disattivare, riattivare, eliminare o revocare l'accesso alla chiave gestita dal cliente in qualsiasi momento.

> **Important**
>
> Amazon FSx accetta solo chiavi KMS con crittografia simmetrica. Non puoi utilizzare chiavi KMS asimmetriche con Amazon. FSx

Politiche FSx chiave di Amazon per AWS KMS

Le policy chiave sono lo strumento principale per controllare l'accesso alle chiavi KMS. Per ulteriori informazioni sulle politiche chiave, consulta Using key policy AWS KMS nella AWS Key Management Service Developer Guide.L'elenco seguente descrive tutte le autorizzazioni AWS KMS correlate supportate da Amazon FSx per i file system crittografati a riposo:

- kms:Encrypt - (Facoltativa) Crittografa testo normale in testo criptato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms:Decrypt - (Obbligatoria) Decifra il testo criptato. Il testo cifrato è un testo normale che è stato precedentemente crittografato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: ReEncrypt — (Facoltativo) Crittografa i dati sul lato server con una nuova chiave KMS, senza esporre il testo in chiaro dei dati sul lato client. I dati sono prima decifrati e quindi nuovamente crittografati. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: GenerateDataKeyWithoutPlaintext — (Obbligatorio) Restituisce una chiave di crittografia dei dati crittografata con una chiave KMS. Questa autorizzazione è inclusa nella politica delle chiavi predefinita in kms: *. GenerateDataKey
- kms: CreateGrant — (Obbligatorio) Aggiunge una concessione a una chiave per specificare chi può utilizzare la chiave e in quali condizioni. I grant sono meccanismi di autorizzazioni alternative alle policy sulle chiavi. Per ulteriori informazioni sulle sovvenzioni, consulta Using grants nella Developer Guide.AWS Key Management Service Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

- kms: DescribeKey — (Obbligatorio) Fornisce informazioni dettagliate sulla chiave KMS specificata. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: ListAliases — (Facoltativo) Elenca tutti gli alias chiave dell'account. Quando usi la console per creare un file system crittografato, questa autorizzazione compila l'elenco per selezionare la chiave KMS. Consigliamo di usare questa autorizzazione per garantire la migliore esperienza utente. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

Crittografia dei dati in transito

Scratch 2 e i file system persistenti possono crittografare automaticamente i dati in transito quando si accede al file system da EC2 istanze Amazon che supportano la crittografia in transito e anche per tutte le comunicazioni tra host all'interno del file system. Per sapere quali EC2 istanze supportano la crittografia in transito, consulta Encryption in transit nella Amazon EC2 User Guide.

Per un elenco dei prodotti Regioni AWS in cui è disponibile Amazon FSx for Lustre, consultaDisponibilità del tipo di implementazione.

Riservatezza del traffico Internet

Questo argomento descrive come Amazon FSx protegge le connessioni dal servizio ad altre località.

Traffico tra Amazon FSx e i clienti locali

Hai due opzioni di connettività tra la tua rete privata e AWS:

- Una AWS Site-to-Site VPN connessione. Per ulteriori informazioni, vedi Cos'è AWS Site-to-Site VPN?
- Una AWS Direct Connect connessione. Per ulteriori informazioni, vedi Cos'è AWS Direct Connect?

È possibile accedere a Lustre tramite la rete FSx per accedere alle operazioni API AWS pubblicate per eseguire attività amministrative e Lustre porte per interagire con il file system.

Crittografia del traffico API

Per accedere alle operazioni API AWS pubblicate, i client devono supportare Transport Layer Security (TLS) 1.2 o versione successiva. È richiesto TLS 1.2 ed è consigliato TLS 1.3. I client devono inoltre supportare le suite di cifratura con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Diffie-Hellman Ephemeral (ECDHE). La maggior

parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità. Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. Oppure puoi utilizzare AWS Security Token Service (STS) per generare credenziali di sicurezza temporanee per firmare le richieste.

Crittografia del traffico dati

La crittografia dei dati in transito è abilitata dalle EC2 istanze supportate che accedono ai file system dall'interno di. Cloud AWS Per ulteriori informazioni, vedereCrittografia dei dati in transito. FSx for Lustre non offre in modo nativo la crittografia in transito tra client locali e file system.

Gestione delle identità e degli accessi per Amazon FSx for Lustre

AWS Identity and Access Management (IAM) è un programma Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Amazon. FSx IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come funziona Amazon FSx for Lustre con IAM
- Esempi di policy basate sull'identità per Amazon for Lustre FSx
- AWS politiche gestite per Amazon FSx for OpenZFS
- Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon FSx for Lustre
- Usare i tag con Amazon FSx
- Utilizzo di ruoli collegati ai servizi per Amazon FSx

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon FSx.

Utente del servizio: se utilizzi il FSx servizio Amazon per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più FSx funzionalità di Amazon per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Amazon FSx, consultaRisoluzione dei problemi relativi all'identità e all'accesso ad Amazon FSx for Lustre.

Amministratore del servizio: se sei responsabile delle FSx risorse Amazon della tua azienda, probabilmente hai pieno accesso ad Amazon FSx. È tuo compito determinare a quali FSx funzionalità e risorse di Amazon devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon FSx, consultaCome funziona Amazon FSx for Lustre con IAM.

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso ad Amazon FSx. Per visualizzare esempi di policy FSx basate sull'identità di Amazon che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Amazon for Lustre FSx

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se

non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA)AWS in IAM nella Guida per l'utente IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzale per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, se si hanno casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, potresti avere un gruppo denominato IAMAdminse concedere a quel gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Create a role for a third-party identity provider (federation) nella Guida per l'utente IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM

per controllare a cosa possono accedere le identità dopo l'autenticazione. Per informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è normale che quel servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso inoltrato (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una

policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzionalità avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a

un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal`sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente IAM.

- Politiche di controllo del servizio (SCPs): SCPs sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta la logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon FSx for Lustre con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon FSx, scopri quali funzionalità IAM sono disponibili per l'uso con Amazon FSx.

Funzionalità IAM che puoi utilizzare con Amazon FSx for Lustre

Funzionalità IAM	FSx Assistenza Amazon
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come Amazon FSx e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Amazon FSx

Supporta le policy basate su identità: sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate sull'identità per Amazon FSx

Per visualizzare esempi di politiche FSx basate sull'identità di Amazon, consulta. Esempi di policy basate sull'identità per Amazon for Lustre FSx

Politiche basate sulle risorse all'interno di Amazon FSx

Supporta le policy basate su risorse: no

Azioni politiche per Amazon FSx

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le operazioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di FSx azioni Amazon, consulta Azioni definite da Amazon FSx for Lustre nel Service Authorization Reference.

Le azioni politiche in Amazon FSx utilizzano il seguente prefisso prima dell'azione:

```
fsx
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Per visualizzare esempi di politiche FSx basate sull'identità di Amazon, consulta. Esempi di policy basate sull'identità per Amazon for Lustre FSx

Risorse relative alle policy per Amazon FSx

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Le istruzioni devono includere un elemento `Resource`o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). È possibile eseguire questa operazione per operazioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le operazioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di FSx risorse Amazon e relativi ARNs, consulta Resources defined by Amazon FSx for Lustre nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon FSx for Lustre.

Per visualizzare esempi di politiche FSx basate sull'identità di Amazon, consulta. Esempi di policy basate sull'identità per Amazon for Lustre FSx

Chiavi relative alle condizioni delle politiche per Amazon FSx

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND`logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di FSx condizione di Amazon, consulta Condition keys for Amazon FSx for Lustre nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon FSx for Lustre.

Per visualizzare esempi di politiche FSx basate sull'identità di Amazon, consulta. Esempi di policy basate sull'identità per Amazon for Lustre FSx

Elenchi di controllo degli accessi (ACLs) in Amazon FSx

Supporti ACLs: No

Controllo degli accessi basato sugli attributi (ABAC) con Amazon FSx

Supporta ABAC (tag nelle policy): sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Per ulteriori informazioni sull'etichettatura FSx delle risorse Amazon, consultaEtichetta le tue risorse Amazon FSx for Lustre.

Per visualizzare una policy basata sulle identità di esempio per limitare l'accesso a una risorsa basata su tag su tale risorsa, consulta Utilizzo dei tag per controllare l'accesso alle FSx risorse Amazon.

Utilizzo di credenziali temporanee con Amazon FSx

Supporta le credenziali temporanee: sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente

e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per Amazon FSx

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un preside. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per Amazon FSx

Supporta i ruoli di servizio: no

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la FSx funzionalità di Amazon. Modifica i ruoli di servizio solo quando Amazon FSx fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Amazon FSx

Supporta ruoli collegati ai servizi: Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni sulla creazione e la gestione dei ruoli FSx collegati ai servizi Amazon, consulta. Utilizzo di ruoli collegati ai servizi per Amazon FSx

Esempi di policy basate sull'identità per Amazon for Lustre FSx

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare FSx risorse Amazon. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti l'autorizzazione a eseguire operazioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da Amazon FSx, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon FSx for Lustre nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della FSx console Amazon
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare FSx risorse Amazon nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti

consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.

- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Protezione dell'accesso API con MFA nella Guida per l'utente IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della FSx console Amazon

Per accedere alla console Amazon FSx for Lustre, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle FSx risorse Amazon presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario concedere autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la FSx console Amazon, allega anche la policy `AmazonFSxConsoleReadOnlyAccess` AWS gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Puoi vedere le politiche `AmazonFSxConsoleReadOnlyAccess` e le altre politiche dei servizi FSx gestiti di Amazon inAWS politiche gestite per Amazon FSx for OpenZFS.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

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

```
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS politiche gestite per Amazon FSx for OpenZFS

Una politica AWS gestita è una politica autonoma creata e amministrata da. AWS AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

Amazon FSx ServiceRolePolicy

Consente FSx ad Amazon di gestire AWS le risorse per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

AWS politica gestita: Amazon FSx DeleteServiceLinkedRoleAccess

Non è possibile collegare `AmazonFSxDeleteServiceLinkedRoleAccess`alle entità IAM. Questa politica è collegata a un servizio e utilizzata solo con il ruolo collegato al servizio per quel servizio. Non è possibile collegare, scollegare, modificare o eliminare questa policy. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

Questa politica concede autorizzazioni amministrative che consentono FSx ad Amazon di eliminare il suo Service Linked Role per l'accesso ad Amazon S3, utilizzato solo da Amazon FSx for Lustre.

Dettagli dell'autorizzazione

Questa policy include le autorizzazioni `iam` per consentire FSx ad Amazon di visualizzare, eliminare e visualizzare lo stato di eliminazione per i FSx Service Linked Roles for Amazon S3 access.

Per visualizzare le autorizzazioni per questa politica, consulta Amazon FSx DeleteServiceLinkedRoleAccess nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx FullAccess

Puoi collegare Amazon FSx FullAccess alle tue entità IAM. Amazon attribuisce questa politica FSx anche a un ruolo di servizio che consente FSx ad Amazon di eseguire azioni per tuo conto.

Fornisce accesso completo ad Amazon FSx e accesso ai AWS servizi correlati.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai mandanti l'accesso completo per eseguire tutte le FSx azioni di Amazon, ad eccezione `BypassSnaplockEnterpriseRetention` di.
- `ds`— Consente ai dirigenti di visualizzare le informazioni sulle AWS Directory Service directory.
- `ec2`
  - Consente ai mandanti di creare tag nelle condizioni specificate.
  - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
- `iam`— Consente ai principi di creare un ruolo collegato al FSx servizio Amazon per conto dell'utente. Ciò è necessario affinché Amazon FSx possa gestire AWS le risorse per conto dell'utente.
- `firehose`— Consente ai mandanti di scrivere record su un Amazon Data Firehose. Ciò è necessario FSx per consentire agli utenti di monitorare l'accesso al file system di Windows File Server inviando registri di accesso di controllo a Firehose.
- `logs`— Consente ai responsabili di creare gruppi di log, flussi di log e scrivere eventi nei flussi di log. Ciò è necessario FSx per consentire agli utenti di monitorare l'accesso al file system di Windows File Server inviando i registri di accesso di controllo a Logs. CloudWatch

Per visualizzare le autorizzazioni per questa politica, consulta Amazon FSx FullAccess nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx ConsoleFullAccess

È possibile allegare la policy `AmazonFSxConsoleFullAccess` alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo ad Amazon FSx e l'accesso ai AWS servizi correlati tramite. AWS Management Console

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai responsabili di eseguire tutte le azioni nella console di FSx gestione Amazon, ad eccezione `BypassSnaplockEnterpriseRetention` di.
- `cloudwatch`— Consente ai responsabili di visualizzare CloudWatch allarmi e metriche nella console di gestione Amazon FSx .
- `ds`— Consente ai responsabili di elencare le informazioni su una directory. AWS Directory Service
- `ec2`
  - Consente ai mandanti di creare tag sulle tabelle di routing, elencare le interfacce di rete, le tabelle di routing, i gruppi di sicurezza, le sottoreti e il VPC associato a un file system Amazon. FSx
  - Consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
  - Consente ai responsabili di visualizzare le interfacce di rete elastiche associate a un FSx file system Amazon.
- `kms`— Consente ai principali di elencare gli alias per le chiavi. AWS Key Management Service
- `s3`— Consente ai responsabili di elencare alcuni o tutti gli oggetti in un bucket Amazon S3 (fino a 1000).
- `iam`— Concede l'autorizzazione a creare un ruolo collegato al servizio che consente FSx ad Amazon di eseguire azioni per conto dell'utente.

Per visualizzare le autorizzazioni per questa politica, consulta Amazon FSx ConsoleFullAccess nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx ConsoleReadOnlyAccess

È possibile allegare la policy `AmazonFSxConsoleReadOnlyAccess` alle identità IAM.

Questa politica concede autorizzazioni di sola lettura ad FSx Amazon e ai servizi AWS correlati in modo che gli utenti possano visualizzare le informazioni su questi servizi in. AWS Management Console

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai responsabili di visualizzare le informazioni sui FSx file system Amazon, inclusi tutti i tag, nella Console di FSx gestione Amazon.
- `cloudwatch`— Consente ai responsabili di visualizzare CloudWatch allarmi e metriche nella Console di gestione Amazon FSx .
- `ds`— Consente ai responsabili di visualizzare le informazioni su una AWS Directory Service directory nella Console di FSx gestione Amazon.
- `ec2`
  - Consente ai responsabili di visualizzare interfacce di rete, gruppi di sicurezza, sottoreti e il VPC associato a un FSx file system Amazon nella Console di gestione Amazon. FSx
  - Consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
  - Consente ai responsabili di visualizzare le interfacce di rete elastiche associate a un FSx file system Amazon.
- `kms`— Consente ai mandanti di visualizzare gli alias per le AWS Key Management Service chiavi nella Console di FSx gestione Amazon.
- `log`— Consente ai responsabili di descrivere i gruppi di log di Amazon CloudWatch Logs associati all'account che effettua la richiesta. Ciò è necessario per consentire ai responsabili di visualizzare la configurazione esistente di controllo degli accessi ai file per un file system FSx per Windows File Server.
- `firehose`— Consente ai mandanti di descrivere i flussi di distribuzione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano visualizzare la configurazione esistente di controllo dell'accesso ai file per un file system FSx per Windows File Server.

Per visualizzare le autorizzazioni per questa politica, consulta Amazon FSx ConsoleReadOnlyAccess nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx ReadOnlyAccess

È possibile allegare la policy `AmazonFSxReadOnlyAccess` alle identità IAM.

- `fsx`— Consente ai responsabili di visualizzare le informazioni sui FSx file system Amazon, inclusi tutti i tag, nella Console di FSx gestione Amazon.
- `ec2`— Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.

Per visualizzare le autorizzazioni per questa politica, consulta Amazon FSx ReadOnlyAccess nella AWS Managed Policy Reference Guide.

FSx Aggiornamenti Amazon alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon FSx da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS sulla pagina Amazon FSx Cronologia dei documenti.

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:CreateAndAttachS3AccessPoint` che consente ai responsabili di creare un S3 e collegarlo a un FSx volume.	14 aprile 2025
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:DescribeS3AccessPointAttachments` che consente ai responsabili di	14 aprile 2025

Modifica	Descrizione	Data
	elencare tutti gli S3 in un unico Account AWS Regione AWS	
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:UpdateS3AccessPointAttachments` che consente ai responsabili di modificare un S3 esistente.	14 aprile 2025
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:DetachAndDeleteS3AccessPoint` che consente ai responsabili di eliminare un S3.	14 aprile 2025
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:CreateAndAttachS3AccessPoint` che consente ai responsabili di creare un S3 e collegarlo a un FSx volume.	14 aprile 2025
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:DescribeS3AccessPointAttachments` che consente ai responsabili di elencare tutti gli S3 in un unico Account AWS Regione AWS	14 aprile 2025

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:UpdateS3Access PointAttachments` che consente ai responsabili di modificare un S3 esistente.	14 aprile 2025
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:DetachAndDelet eS3AccessPoint` che consente ai responsabili di eliminare un S3.	14 aprile 2025
Amazon FSx ConsoleRe adOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:DescribeNetwor kInterfaces` che consente ai responsabili di visualizzare le interfacce di rete elastiche associate al proprio file system.	25 febbraio 2025
Amazon FSx ConsoleFu llAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:DescribeNetwor kInterfaces` che consente ai responsabili di visualizzare le interfacce di rete elastiche associate al proprio file system.	07 febbraio 2025

Modifica	Descrizione	Data
Amazon FSx ServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx ReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx ConsoleReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica dei dati tra regioni e account FSx per i file system OpenZFS.	20 dicembre 2023
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica dei dati tra regioni e account FSx per i file system OpenZFS.	20 dicembre 2023

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica su richiesta dei volumi FSx per i file system OpenZFS.	26 novembre 2023
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica su richiesta dei volumi FSx per i file system OpenZFS.	26 novembre 2023
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare, abilitare e disabilitare il supporto VPC condiviso FSx per i file system ONTAP Multi-AZ.	14 novembre 2023
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare, abilitare e disabilitare il supporto VPC condiviso FSx per i file system ONTAP Multi-AZ.	14 novembre 2023

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx gestire le configurazioni di rete FSx per i file system OpenZFS Multi-AZ.	9 agosto 2023
AWS politica gestita: Amazon FSx ServiceRolePolicy — Aggiornamento a una politica esistente	Amazon ha FSx modificato l'`cloudwatch:PutMetricData` autorizzazione esistente in modo che Amazon FSx pubblichi le CloudWatch metriche nel namespace. `AWS/FSx`	24 luglio 2023
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiornato la politica per rimuovere l'`fsx:*`autorizzazione e aggiungere `fsx` azioni specifiche.	13 luglio 2023
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiornato la politica per rimuovere l'`fsx:*`autorizzazione e aggiungere `fsx` azioni specifiche.	13 luglio 2023
Amazon FSx ConsoleReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare metriche di prestazioni migliorate e azioni consigliate FSx per i file system Windows File Server nella console Amazon FSx .	21 settembre 2022

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare metriche di prestazioni migliorate e azioni consigliate FSx per i file system Windows File Server nella console Amazon FSx .	21 settembre 2022
Amazon FSx ReadOnlyAccess — Avviata la politica di tracciamento	Questa politica garantisce l'accesso in sola lettura a tutte le FSx risorse Amazon e a tutti i tag ad esse associati.	4 febbraio 2022
Amazon FSx DeleteServiceLinkedRoleAccess — Avviata la politica di tracciamento	Questa politica concede autorizzazioni amministrative che consentono FSx ad Amazon di eliminare il suo Service Linked Role per l'accesso ad Amazon S3.	7 gennaio 2022
Amazon FSx ServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx gestire le configurazioni di rete per i file system Amazon FSx for NetApp ONTAP.	2 settembre 2021
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare tag nelle tabelle di EC2 routing per chiamate circoscritte.	2 settembre 2021

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx creare file system Amazon FSx for NetApp ONTAP Multi-AZ.	2 settembre 2021
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare tag nelle tabelle di EC2 routing per chiamate circoscritte.	2 settembre 2021
Amazon FSx ServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx descrivere e scrivere su CloudWatch Logs i flussi di log. Ciò è necessario per consentire e agli utenti di visualizzare i registri di controllo degli accessi ai file FSx per i file system Windows File Server utilizzando Logs. CloudWatch	8 giugno 2021

Modifica	Descrizione	Data
Amazon FSx ServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx descrivere e scrivere nei flussi di distribuzione di Amazon Data Firehose. Ciò è necessario per consentire agli utenti di visualizzare i log di controllo degli accessi ai file FSx per un file system Windows File Server utilizzando Amazon Data Firehose.	8 giugno 2021
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere e creare gruppi di log di CloudWatch Logs, log stream e scrivere eventi nei flussi di log. Ciò è necessario affinché i responsabili possano visualizzare i log di controllo degli accessi ai file FSx per i file system di Windows File Server utilizzando Logs. CloudWatch	8 giugno 2021

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere e scrivere record su Amazon Data Firehose. Ciò è necessario per consentir e agli utenti di visualizzare i log di controllo degli accessi ai file FSx per un file system Windows File Server utilizzan do Amazon Data Firehose.	8 giugno 2021
Amazon FSx ConsoleFu llAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere i gruppi di log di Amazon CloudWatch Logs associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano scegliere un gruppo di log CloudWatc h Logs esistente durante la configurazione del controllo dell'accesso ai file per un FSx file system per Windows File Server.	8 giugno 2021

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere i flussi di distribuzione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano scegliere un flusso di distribuzione Firehose esistente durante la configurazione del controllo dell'accesso ai file per FSx un file system Windows File Server.	8 giugno 2021
Amazon FSx ConsoleReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere i gruppi di log di Amazon CloudWatch Logs associati all'account che effettua la richiesta. Ciò è necessario per consentire ai responsabili di visualizzare la configurazione esistente di controllo dell'accesso ai file per un file system FSx per Windows File Server.	8 giugno 2021

Modifica	Descrizione	Data
Amazon FSx ConsoleReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere i flussi di distribuzione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario per consentire ai responsabili di visualizzare la configurazione esistente di controllo dell'accesso ai file per un FSx file system per Windows File Server.	8 giugno 2021
Amazon FSx ha iniziato a tracciare le modifiche	Amazon FSx ha iniziato a tracciare le modifiche alle sue politiche AWS gestite.	8 giugno 2021

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon FSx for Lustre

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon FSx e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Amazon FSx
- Non sono autorizzato a eseguire iam: PassRole
- Voglio consentire a persone esterne Account AWS a me di accedere alle mie FSx risorse Amazon

Non sono autorizzato a eseguire un'azione in Amazon FSx

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `fsx:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `fsx:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon FSx.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon FSx. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne Account AWS a me di accedere alle mie FSx risorse Amazon

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon FSx supporta queste funzionalità, consultaCome funziona Amazon FSx for Lustre con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Usare i tag con Amazon FSx

Puoi utilizzare i tag per controllare l'accesso alle FSx risorse Amazon e implementare il controllo degli accessi basato sugli attributi (ABAC). Per applicare tag alle FSx risorse Amazon durante la creazione, gli utenti devono disporre di determinate autorizzazioni AWS Identity and Access Management (IAM).

Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione

Con alcune azioni dell'API FSx Amazon for Lustre che creano risorse, puoi specificare i tag quando crei la risorsa. Puoi utilizzare questi tag di risorse per implementare il controllo degli accessi basato sugli attributi (ABAC). Per ulteriori informazioni, consulta A cosa serve ABAC? AWS nella Guida per l'utente di IAM.

Affinché gli utenti possano taggare le risorse al momento della creazione, devono disporre dell'autorizzazione a utilizzare l'azione che crea la risorsa, ad esempio`fsx:CreateFileSystem`. Se i tag sono specificati nell'azione di creazione della risorsa, IAM esegue un'autorizzazione aggiuntiva sull'`fsx:TagResource`azione per verificare se gli utenti dispongono delle autorizzazioni per creare tag. Pertanto, gli utenti devono disporre anche delle autorizzazioni esplicite per utilizzare l'operazione `fsx:TagResource`.

La seguente politica di esempio consente agli utenti di creare file system e applicare loro tag durante la creazione in uno specifico. Account AWS

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

Analogamente, la seguente politica consente agli utenti di creare backup su un file system specifico e di applicare qualsiasi tag al backup durante la creazione del backup.

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

L'`fsx:TagResource`azione viene valutata solo se i tag vengono applicati durante l'azione di creazione della risorsa. Pertanto, un utente che dispone delle autorizzazioni per creare una risorsa (presupponendo che non vi siano condizioni di etichettatura) non necessita dell'autorizzazione per utilizzare l'`fsx:TagResource`azione se nella richiesta non sono specificati tag. Tuttavia, se l'utente tenta di creare una risorsa con tag, la richiesta ha esito negativo se non dispone delle autorizzazioni per utilizzare l'operazione `fsx:TagResource`.

Per ulteriori informazioni sull'etichettatura FSx delle risorse Amazon, consultaEtichetta le tue risorse Amazon FSx for Lustre. Per ulteriori informazioni sull'uso dei tag per controllare l'accesso alle risorse di Amazon FSx for Lustre, consultaUtilizzo dei tag per controllare l'accesso alle FSx risorse Amazon.

Utilizzo dei tag per controllare l'accesso alle FSx risorse Amazon

Per controllare l'accesso alle FSx risorse e alle azioni di Amazon, puoi utilizzare le policy IAM basate sui tag. È possibile fornire il controllo in due modi:

- Puoi controllare l'accesso alle FSx risorse Amazon in base ai tag presenti su tali risorse.
- Puoi controllare quali tag possono essere trasferiti in una condizione di richiesta IAM.

Per informazioni su come utilizzare i tag per controllare l'accesso alle AWS risorse, consulta Controlling access using tags nella IAM User Guide. Per ulteriori informazioni sull'etichettatura FSx delle risorse Amazon al momento della creazione, consultaConcessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione. Per ulteriori informazioni sull'assegnazione di tag alle risorse, consulta Etichetta le tue risorse Amazon FSx for Lustre.

Controllo dell'accesso in base ai tag di una risorsa

Per controllare quali azioni un utente o un ruolo può eseguire su una FSx risorsa Amazon, puoi utilizzare i tag sulla risorsa. Ad esempio, è possibile consentire o negare operazioni API specifiche su una risorsa di gateway di file in base alla coppia chiave-valore del tag sulla risorsa.

Example Politica di esempio: crea un file system attivo quando fornisci un tag specifico

Questa politica consente all'utente di creare un file system solo quando lo contrassegna con una coppia chiave-valore specifica, in questo esempio`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 Politica di esempio: crea backup solo su file system con un tag specifico

Questa politica consente agli utenti di creare backup solo su file system etichettati con la coppia `key=Department, value=Finance` chiave-valore e il backup verrà creato con il tag. `Deparment=Finance`

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

```
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example Politica di esempio: crea un file system con un tag specifico partendo da backup con un tag specifico

Questa politica consente agli utenti di creare file system etichettati con `Department=Finance` solo a partire da backup contrassegnati con. `Department=Finance`

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

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Politica di esempio: eliminare i file system con tag specifici

Questa politica consente a un utente di eliminare solo i file system contrassegnati con`Department=Finance`. Se creano un backup finale, deve essere contrassegnato con`Department=Finance`. FSx Per quanto riguarda i file system Lustre, gli utenti devono avere il `fsx:CreateBackup` privilegio di creare il backup finale.

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

```
        }
    ]
}
```

Example Politica di esempio: creazione di attività di archiviazione dei dati su file system con tag specifici

Questa politica consente agli utenti di creare attività di archivio di dati contrassegnate con `Department=Finance` e solo su file system contrassegnati con. `Department=Finance`

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

Utilizzo di ruoli collegati ai servizi per Amazon FSx

Amazon FSx utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ad Amazon. FSx I ruoli collegati ai servizi sono predefiniti da Amazon FSx e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

Un ruolo collegato al servizio semplifica la configurazione di Amazon FSx perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Amazon FSx definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Amazon FSx può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi le tue FSx risorse Amazon perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni su altri servizi che supportano ruoli collegati ai servizi, consulta i AWS servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato al servizio per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per Amazon FSx

Amazon FSx utilizza due ruoli collegati ai servizi denominati `AWSServiceRoleForAmazonFSx` e `AWSServiceRoleForFSxS3Access_`*`fs-01234567890`* che eseguono determinate azioni nel tuo account. Esempi di queste azioni sono la creazione di interfacce di rete elastiche per i tuoi file system nel tuo VPC e l'accesso al tuo repository di dati in un bucket Amazon S3. Infatti`AWSServiceRoleForFSxS3Access_`*`fs-01234567890`*, questo ruolo collegato al servizio viene creato per ogni file system Amazon FSx for Lustre creato che è collegato a un bucket S3.

AWSServiceRoleForAmazonFSx dettagli sulle autorizzazioni

Infatti`AWSServiceRoleForAmazonFSx`, la politica di autorizzazione dei ruoli consente FSx ad Amazon di completare le seguenti azioni amministrative per conto dell'utente su tutte le AWS risorse applicabili:

Per gli aggiornamenti a questa politica, vedi Amazon FSx ServiceRolePolicy

> **Note**
>
> AWSServiceRoleForAmazonFSx Viene utilizzato da tutti i tipi di FSx file system di Amazon; alcune delle autorizzazioni elencate non sono applicabili a FSx Lustre.

- `ds`— Consente FSx ad Amazon di visualizzare, autorizzare e non autorizzare le applicazioni nella tua directory. AWS Directory Service
- `ec2`— Consente FSx ad Amazon di effettuare le seguenti operazioni:
  - Visualizza, crea e dissocia le interfacce di rete associate a un FSx file system Amazon.
  - Visualizza uno o più indirizzi IP elastici associati a un FSx file system Amazon.
  - Visualizza Amazon VPCs, i gruppi di sicurezza e le sottoreti associati a un FSx file system Amazon.
  - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
  - Crea un'autorizzazione per un utente AWS autorizzato a eseguire determinate operazioni su un'interfaccia di rete.
- `cloudwatch`— Consente FSx ad Amazon di pubblicare punti dati metrici nello CloudWatch spazio dei FSx nomi AWS/.
- `route53`— Consente FSx ad Amazon di associare un Amazon VPC a una zona ospitata privata.
- `logs`— Consente FSx ad Amazon di descrivere e scrivere su CloudWatch Logs i flussi di log. In questo modo gli utenti possono inviare i registri di controllo degli accessi ai file per un file system FSx per Windows File Server a un CloudWatch flusso di log.
- `firehose`— Consente FSx ad Amazon di descrivere e scrivere sui flussi di distribuzione di Amazon Data Firehose. In questo modo gli utenti possono pubblicare i log di controllo degli accessi ai file per un file system FSx per Windows File Server su un flusso di distribuzione di Amazon Data Firehose.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
```

```
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
```

```
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        },
        {
```

```
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Eventuali aggiornamenti a questa politica sono descritti in. FSx Aggiornamenti Amazon alle politiche AWS gestite

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Service-Linked Role Permissions nella IAM User Guide.

AWSServiceRoleForFSxDettagli sulle autorizzazioni S3Access

InfattiAWSServiceRoleForFSxS3Access_*file-system-id*, la politica di autorizzazione dei ruoli consente FSx ad Amazon di completare le seguenti azioni su un bucket Amazon S3 che ospita il repository di dati per un file system FSx Amazon for Lustre.

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:Get*`
- `s3:List*`
- `s3:PutBucketNotification`
- `s3:PutObject`

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Amazon FSx

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un file system nella AWS Management Console, la AWS CLI o l' AWS API, Amazon FSx crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato ai servizi può apparire nell'account se è stata completata un'operazione in un altro servizio che utilizza le funzionalità supportate dal ruolo. Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un file system, Amazon FSx crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato ai servizi per Amazon FSx

Amazon FSx non consente di modificare questi ruoli collegati ai servizi. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Amazon FSx

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, devi eliminare tutti i file system e i backup prima di poter eliminare manualmente il ruolo collegato al servizio.

> **Note**
>
> Se il FSx servizio Amazon utilizza il ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Usa la console IAM, la CLI IAM oppure l'API IAM per eliminare il ruolo collegato ai servizi AWSServiceRoleForAmazonFSx. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati FSx ai servizi Amazon

Amazon FSx supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

Controllo degli accessi ai file system con Amazon VPC

Un FSx file system Amazon è accessibile tramite un'interfaccia di rete elastica che risiede nel cloud privato virtuale (VPC) basata sul servizio Amazon VPC associato al file system. Puoi accedere al tuo FSx file system Amazon tramite il suo nome DNS, che corrisponde all'interfaccia di rete del file system. Solo le risorse all'interno del VPC associato o di un VPC peer-to-peer possono accedere all'interfaccia di rete del file system. Per ulteriori informazioni, consultare Che cos'è Amazon VPC? nella Guida per l'utente di Amazon VPC

> **Warning**
>
> Non devi modificare o eliminare l'interfaccia di rete FSx elastica di Amazon. La modifica o l'eliminazione dell'interfaccia di rete può causare una perdita permanente della connessione tra il VPC e il file system.

Gruppi di sicurezza Amazon VPC

Per controllare ulteriormente il traffico di rete che attraversa l'interfaccia di rete del file system all'interno del VPC, utilizzate i gruppi di sicurezza per limitare l'accesso ai file system. Un gruppo di sicurezza funge da firewall virtuale per controllare il traffico delle risorse associate. In questo caso, la risorsa associata è l'interfaccia di rete del file system. Utilizzi anche i gruppi di sicurezza VPC per controllare il traffico di rete per Lustre clienti.

gruppi di sicurezza abilitati all'EFA

Se intendete creare un gruppo di sicurezza compatibile con EFA FSx per Lustre, dovete prima creare un gruppo di sicurezza compatibile con EFA e specificarlo come gruppo di sicurezza per il file system.

Un EFA richiede un gruppo di sicurezza che consenta tutto il traffico in entrata e in uscita da e verso il gruppo di sicurezza stesso e il gruppo di sicurezza dei client se i client risiedono in un gruppo di sicurezza diverso. Per ulteriori informazioni, consulta la Fase 1: Preparare un gruppo di sicurezza compatibile con EFA nella Amazon EC2 User Guide.

Controllo dell'accesso tramite regole in entrata e in uscita

Per utilizzare un gruppo di sicurezza per controllare l'accesso al tuo FSx file system Amazon e Lustre clienti, aggiungi le regole in entrata per controllare il traffico in entrata e le regole in uscita per controllare il traffico in uscita dal tuo file system e Lustre clienti. Assicurati di avere le regole del traffico di rete corrette nel tuo gruppo di sicurezza per mappare la condivisione di FSx file del tuo file system Amazon su una cartella sull'istanza di calcolo supportata.

Per ulteriori informazioni sulle regole dei gruppi di sicurezza, consulta le regole del gruppo di sicurezza nella Amazon EC2 User Guide.

Per creare un gruppo di sicurezza per il tuo FSx file system Amazon

1. Apri la EC2 console Amazon in https://console.aws.amazon.com/ec2.
2. Fare clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
3. Scegliere Create Security Group (Crea un gruppo di sicurezza).
4. Specificare un nome e una descrizione per il gruppo di sicurezza.
5. Per VPC, scegli il VPC associato al tuo FSx file system Amazon per creare il gruppo di sicurezza all'interno di quel VPC.
6. Per creare il gruppo di sicurezza, scegli Create (Crea).

Successivamente, aggiungi le regole in entrata al gruppo di sicurezza che hai appena creato per abilitare Lustre traffico tra i tuoi file FSx server for Lustre.

Per aggiungere regole in entrata al tuo gruppo di sicurezza

1. Seleziona il gruppo di sicurezza che hai appena creato se non è già selezionato. Nel menu Actions (Operazioni), selezionare Edit inbound rules (Modifica regole in entrata).
2. Aggiungi le seguenti regole in entrata.

Tipo	Protocollo	Intervallo porte	Origine	Descrizione
Regola TCP personalizzata	TCP	988	Scegli Personalizzato e inserisci l'ID del gruppo di sicurezza che hai appena creato	Allows Lustre traffico tra FSx i file server For Lustre
Regola TCP personalizzata	TCP	988	Scegli Personalizzato e inserisci il gruppo IDs di sicurezza dei gruppi di sicurezza associati al tuo Lustre clients	Allows Lustre traffico tra i file server FSx for Lustre e Lustre clients
Regola TCP personalizzata	TCP	1018-1023	Scegli Personalizzato e inserisci l'ID del gruppo di sicurezza che hai appena creato	Allows Lustre traffico tra FSx i file server For Lustre
Regola TCP personalizzata	TCP	1018-1023	Scegli Personalizzato e inserisci il gruppo di sicurezza dei gruppi IDs di sicurezza associati al tuo Lustre clients	Allows Lustre traffico tra i file server FSx for Lustre e Lustre clients

3. Scegli Salva per salvare e applicare le nuove regole in entrata.

Per impostazione predefinita, le regole dei gruppi di sicurezza consentono tutto il traffico in uscita (Tutto, 0.0.0.0/0). Se il tuo gruppo di sicurezza non consente tutto il traffico in uscita, aggiungi le seguenti regole in uscita al tuo gruppo di sicurezza. Queste regole consentono il traffico tra i file FSx server for Lustre e Lustre client e tra Lustre file server.

Per aggiungere regole in uscita al gruppo di sicurezza

1. Scegli lo stesso gruppo di sicurezza a cui hai appena aggiunto le regole in entrata. Per Azioni, scegli Modifica regole in uscita.
2. Aggiungi le seguenti regole in uscita.

Tipo	Protocollo	Intervallo porte	Origine	Descrizione
Regola TCP personalizzata	TCP	988	Scegli Personalizzato e inserisci l'ID del gruppo di sicurezza che hai appena creato	Consenso Lustre traffico tra FSx i file server For Lustre
Regola TCP personalizzata	TCP	988	Scegli Personalizzato e inserisci il gruppo IDs di sicurezza del gruppo di sicurezza associato al tuo Lustre clients	Consenso Lustre traffico tra i file server FSx for Lustre e Lustre clients
Regola TCP personalizzata	TCP	1018-1023	Scegli Personalizzato e inserisci l'ID del gruppo di sicurezza che hai appena creato	Allows Lustre traffico tra FSx i file server For Lustre
Regola TCP personalizzata	TCP	1018-1023	Scegli Personalizzato e inserisci	Allows Lustre traffico tra i file

Tipo	Protocollo	Intervallo porte	Origine	Descrizione
			il gruppo di sicurezza dei gruppi IDs di sicurezza associati al tuo Lustre clients	server FSx for Lustre e Lustre clients

3. Scegli Salva per salvare e applicare le nuove regole in uscita.

Per associare un gruppo di sicurezza al tuo FSx file system Amazon

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nella dashboard della console, scegli il tuo file system per visualizzarne i dettagli.
3. Nella scheda Rete e sicurezza, fai clic sul collegamento della EC2 console Amazon in Interfacce di rete per visualizzare tutte le interfacce di rete per il tuo file system.
4. Per ogni interfaccia di rete, scegli Azioni, quindi scegli Cambia gruppi di sicurezza.
5. Nella finestra di dialogo Modifica gruppi di sicurezza, scegli i gruppi di sicurezza che desideri associare all'interfaccia di rete.
6. Seleziona Salva.

Lustre regole del gruppo di sicurezza VPC client

Utilizzi i gruppi di sicurezza VPC per controllare l'accesso ai tuoi Lustre clienti aggiungendo regole in entrata per controllare il traffico in entrata e regole in uscita per controllare il traffico in uscita dal Lustre clienti. Assicurati di avere le giuste regole del traffico di rete nel tuo gruppo di sicurezza per garantire che Lustre il traffico può fluire tra i tuoi Lustre clienti e i tuoi FSx file system Amazon.

Aggiungi le seguenti regole in entrata ai gruppi di sicurezza applicati ai tuoi Lustre clienti.

Tipo	Protocollo	Intervallo porte	Origine	Descrizione
Regola TCP personalizzata	TCP	988	Scegli Personalizzato e inserisci il gruppo IDs	Allows Lustre traffico tra Lustre clients

Tipo	Protocollo	Intervallo porte	Origine	Descrizione
			di sicurezza dei gruppi di sicurezza applicati al Lustre clients	
Regola TCP personalizzata	TCP	988	Scegli Personalizzato e inserisci il gruppo IDs di sicurezza dei gruppi di sicurezza associati ai tuoi file FSx system for Lustre	Allows Lustre traffico tra i file FSx server for Lustre e Lustre clients
Regola TCP personalizzata	TCP	1018-1023	Scegli Personalizzato e inserisci il gruppo IDs di sicurezza dei gruppi di sicurezza applicati al Lustre clients	Allows Lustre traffico tra Lustre clients
Regola TCP personalizzata	TCP	1018-1023	Scegli Personalizzato e inserisci il gruppo IDs di sicurezza dei gruppi di sicurezza associati ai tuoi file system FSx for Lustre	Allows Lustre traffico tra i file FSx server for Lustre e Lustre clients

Aggiungi le seguenti regole in uscita ai gruppi di sicurezza applicati al tuo Lustre clienti.

Tipo	Protocollo	Intervallo porte	Origine	Descrizione
Regola TCP personalizzata	TCP	988	Scegli Personalizzato e inserisci il gruppo IDs di sicurezza dei gruppi di sicurezza applicati al Lustre clients	Allows Lustre traffico tra Lustre clients
Regola TCP personalizzata	TCP	988	Scegli Personalizzato e inserisci il gruppo IDs di sicurezza dei gruppi di sicurezza associati ai tuoi file FSx system for Lustre	Consenso Lustre traffico tra i file FSx server for Lustre e Lustre clients
Regola TCP personalizzata	TCP	1018-1023	Scegli Personalizzato e inserisci il gruppo IDs di sicurezza dei gruppi di sicurezza applicati al Lustre clients	Allows Lustre traffico tra Lustre clients
Regola TCP personalizzata	TCP	1018-1023	Scegli Personalizzato e inserisci il gruppo IDs di sicurezza dei gruppi di sicurezza	Allows Lustre traffico tra i file FSx server for Lustre e Lustre clients

Tipo	Protocollo	Intervallo porte	Origine	Descrizione
			associati ai tuoi file system FSx for Lustre	

Rete Amazon VPC ACLs

Un'altra opzione per proteggere l'accesso al file system all'interno del VPC è la creazione di elenchi di controllo degli accessi alla rete (ACLsrete). ACLs Le reti sono separate dai gruppi di sicurezza, ma hanno funzionalità simili per aggiungere un ulteriore livello di sicurezza alle risorse del tuo VPC. Per ulteriori informazioni sull'implementazione del controllo degli accessi tramite rete ACLs, consulta Controllare il traffico verso le sottoreti utilizzando la rete ACLs nella Amazon VPC User Guide.

Convalida della conformità per Amazon FSx for Lustre

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa HIPAA.
- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e

mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).

- Evaluating Resources with Rules nella AWS Config Developer Guide: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Amazon FSx for Lustre e endpoint VPC di interfaccia ()AWS PrivateLink

Puoi migliorare il livello di sicurezza del tuo VPC configurando FSx Amazon per utilizzare un endpoint VPC di interfaccia. Gli endpoint VPC di interfaccia sono basati su una tecnologia che consente di AWS PrivateLinkaccedere ad FSx APIs Amazon in modo privato senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare con Amazon. FSx APIs Il traffico tra il tuo VPC e Amazon FSx non esce dalla AWS rete.

Ogni endpoint VPC di interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti. Un'interfaccia di rete fornisce un indirizzo IP privato che funge da punto di ingresso per il traffico verso l' FSx API Amazon.

Considerazioni sugli endpoint VPC con FSx interfaccia Amazon

Prima di configurare un endpoint VPC di interfaccia per Amazon FSx, assicurati di esaminare le proprietà e le limitazioni dell'endpoint VPC dell'interfaccia nella Amazon VPC User Guide.

Puoi chiamare qualsiasi operazione dell' FSx API Amazon dal tuo VPC. Ad esempio, puoi creare un file system FSx for Lustre chiamando l' CreateFileSystem API dall'interno del tuo VPC. Per l'elenco completo di Amazon FSx APIs, consulta Actions in the Amazon FSx API Reference.

Considerazioni sul peering VPC

Puoi connetterne altri VPCs al VPC con endpoint VPC di interfaccia utilizzando il peering VPC. Il peering VPC è una connessione di rete tra due. VPCs Puoi stabilire una connessione peering VPC tra i tuoi due VPCs o con un VPC in un altro. Account AWS VPCs Possono essere disponibili anche in due versioni diverse. Regioni AWS

Il traffico tra utenti VPCs peer rimane sulla AWS rete e non attraversa la rete Internet pubblica. Una volta VPCs eseguito il peering, risorse come le istanze Amazon Elastic Compute Cloud EC2 (Amazon) in entrambe VPCs possono accedere all' FSx API Amazon tramite endpoint VPC di interfaccia creati in uno dei. VPCs

Creazione di un endpoint VPC di interfaccia per Amazon API FSx

Puoi creare un endpoint VPC per l' FSx API Amazon utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta Creazione di un endpoint VPC di interfaccia nella Amazon VPC User Guide.

Per un elenco completo degli FSx endpoint Amazon, consulta la sezione FSx Endpoint e quote Amazon nel. Riferimenti generali di Amazon Web Services

Per creare un endpoint VPC di interfaccia per Amazon FSx, usa uno dei seguenti:

- **`com.amazonaws.`*`region`*`.fsx`**— Crea un endpoint per le operazioni delle FSx API Amazon.
- **`com.amazonaws.`*`region`*`.fsx-fips`**— Crea un endpoint per l' FSx API Amazon conforme al Federal Information Processing Standard (FIPS) 140-2.

Per utilizzare l'opzione DNS privato, devi impostare `enableDnsSupport` gli attributi `enableDnsHostnames` e del tuo VPC. Per ulteriori informazioni, consulta Visualizzazione e aggiornamento del supporto DNS per il tuo VPC nella Amazon VPC User Guide.

Ad eccezione Regioni AWS della Cina, se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API ad Amazon FSx con l'endpoint VPC utilizzando il suo nome DNS predefinito per, ad esempio. Regione AWS`fsx.us-east-1.amazonaws.com` Per la Cina (Pechino) e la Cina (Ningxia) Regioni AWS, puoi effettuare richieste API con l'endpoint VPC utilizzando e, rispettivamente. `fsx-api.cn-north-1.amazonaws.com.cn` `fsx-api.cn-northwest-1.amazonaws.com.cn`

Per ulteriori informazioni, consulta Accesso a un servizio tramite un endpoint VPC di interfaccia nella Amazon VPC User Guide.

Creazione di una policy sugli endpoint VPC per Amazon FSx

Per controllare ulteriormente l'accesso all' FSx API Amazon, puoi opzionalmente allegare una policy AWS Identity and Access Management (IAM) al tuo endpoint VPC. La policy specifica quanto segue:

- Il principale che può eseguire azioni.
- Le azioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire operazioni.

Per ulteriori informazioni, consulta Controllo degli accessi ai servizi con endpoint VPC in Guida per l'utente di Amazon VPC.

Quote di servizio per Amazon FSx for Lustre

Di seguito, puoi scoprire le quote quando lavori con Amazon FSx for Lustre.

Argomenti

Quote che è possibile incrementare

Di seguito sono riportate le quote di Amazon FSx for Lustre per AWS account e per AWS regione, che puoi aumentare.

Risorsa	Predefinito	Descrizione
LustreSistemi persistenti a 1 file	100	Il numero massimo di file system Amazon FSx for Lustre Persistent 1 che puoi creare in questo account.
LustreFile system persistenti a 2 file	100	Il numero massimo di file system Amazon FSx for Lustre Persistent 2 che puoi creare in questo account.
LustreCapacità di storage HDD persistente (per file system)	102000	La quantità massima di capacità di archiviazione dell'HDD (in GiB) che puoi configurare per un file system persistente FSx Amazon for Lustre.
LustreCapacità di storage persistente per 1 file	100800	La quantità massima di capacità di storage (in GiB) che puoi configurare per tutti

Risorsa	Predefinito	Descrizione
		i file system Amazon FSx for Lustre Persistent 1 in questo account.
LustreCapacità di storage persistente per 2 file	100800	La quantità massima di capacità di storage (in GiB) che puoi configurare per tutti i file system Amazon FSx for Lustre Persistent 2 in questo account.
LustreFile system Scratch	100	Il numero massimo di file system scratch di Amazon FSx for Lustre che puoi creare in questo account.
LustreCapacità di archiviaz ione Scratch	100800	La quantità massima di capacità di storage (in GiB) che puoi configurare per tutti i file system scratch di Amazon FSx for Lustre in questo account.
Lustrebackup	500	Il numero massimo di backup avviati dall'utente che puoi avere per tutti i file system Amazon FSx for Lustre in questo account.

Richiesta di un aumento delle quote

1. Apri la console Service Quotas.
2. Nel pannello di navigazione, scegli Servizi AWS (servizi AWS).
3. Scegli Lustre.
4. Scegli una quota.

5. Scegli Richiedi un aumento della quota e segui le istruzioni per richiedere un aumento della quota.
6. Per visualizzare lo stato della richiesta di quota, scegli Cronologia delle richieste di quota nel riquadro di navigazione della console.

Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente per Service Quotas.

Quote di risorse per ogni file system

Di seguito sono riportati i limiti delle risorse Amazon FSx for Lustre per ogni file system in una AWS regione.

Risorsa	Limite per file system
Numero massimo di tag	50
Periodo massimo di conservazione per i backup automatici	90 giorni
Numero massimo di richieste di copie di backup in corso verso una singola regione di destinazione per account.	5
Numero di aggiornamenti di file dal bucket S3 collegato per file system	10 milioni al mese
Capacità di archiviazione minima, file system SSD	1,2 TiB
Capacità di archiviazione minima, file system HDD	6 TiB
Throughput minimo per unità di storage, SSD	50 MBps
Throughput massimo per unità di storage, SSD	1000 MBps
Throughput minimo per unità di storage, HDD	12 MBps
Throughput massimo per unità di storage, HDD	40 MBps

Ulteriori considerazioni

In aggiunta, tieni presente quanto segue:

- Puoi utilizzare ogni chiave AWS Key Management Service (AWS KMS) su un massimo di 125 file system Amazon FSx for Lustre.
- Per un elenco delle AWS regioni in cui è possibile creare file system, consulta Amazon FSx Endpoints and Quotas nel. Riferimenti generali di AWS

Risoluzione dei problemi di Amazon FSx for Lustre

Questa sezione descrive vari scenari e soluzioni di risoluzione dei problemi per i file system Amazon FSx for Lustre.

Se riscontri problemi non elencati di seguito, prova a porre una domanda nel forum Amazon FSx for Lustre.

Argomenti

La creazione di un file system FSx for Lustre non riesce

L'esito negativo di una richiesta di creazione del file system può causare diverse cause, come descritto nei seguenti argomenti.

Impossibile creare un file system compatibile con EFA a causa di un gruppo di sicurezza non configurato correttamente

La creazione di un file system compatibile con EFA FSx for Lustre non riesce e viene visualizzato il seguente messaggio di errore:

```
Insufficient security group permissions to create an EFA-enabled file system.
Update security group to allow all internal inbound and outbound traffic.
```

Operazione da eseguire

Assicurati che il gruppo di sicurezza VPC che stai utilizzando per l'operazione di creazione sia configurato come descritto in. gruppi di sicurezza abilitati all'EFA Un EFA richiede un gruppo di sicurezza che consenta tutto il traffico in entrata e in uscita da e verso il gruppo di sicurezza stesso e il gruppo di sicurezza dei client se i client risiedono in un gruppo di sicurezza diverso.

Impossibile creare un file system a causa di un gruppo di sicurezza non configurato correttamente

La creazione di un file system FSx for Lustre non riesce e viene visualizzato il seguente messaggio di errore:

```
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
```

Operazione da eseguire

Assicurati che il gruppo di sicurezza VPC che stai utilizzando per l'operazione di creazione sia configurato come descritto in. Controllo degli accessi ai file system con Amazon VPC È necessario configurare il gruppo di sicurezza per consentire il traffico in entrata sulle porte 988 e 1018-1023 dal gruppo di sicurezza stesso o dall'intera sottorete CIDR, necessario per consentire agli host del file system di comunicare tra loro.

Impossibile creare un file system a causa di errori di capacità insufficiente

È possibile che venga visualizzato un errore di capacità insufficiente quando si tenta di creare un nuovo file system, aggiornare la capacità di archiviazione o modificare la capacità di throughput.

Causa

Questo errore si verifica quando FSx for Lustre non dispone attualmente di una capacità hardware disponibile sufficiente nella zona di disponibilità richiesta per soddisfare la richiesta.

Soluzione

Per risolvere il problema, prova a eseguire queste operazioni:

- Attendi qualche minuto e riprova la richiesta, poiché la disponibilità della capacità cambia frequentemente.

- Prova la tua richiesta in un'altra zona di disponibilità.
- Tenta l'operazione con una dimensione di storage inferiore o un livello di throughput inferiore

Impossibile creare un file system collegato a un bucket S3

Se la creazione di un nuovo file system collegato a un bucket S3 fallisce, viene visualizzato un messaggio di errore simile al seguente.

```
User: arn:aws:iam::012345678901:user/username is not authorized to perform:
 iam:PutRolePolicy on resource: resource ARN
```

Questo errore può verificarsi se tenti di creare un file system collegato a un bucket Amazon S3 senza le necessarie autorizzazioni IAM. Le autorizzazioni IAM richieste supportano il ruolo collegato al servizio Amazon FSx for Lustre utilizzato per accedere al bucket Amazon S3 specificato per tuo conto.

Operazione da eseguire

Assicurati che la tua entità IAM (utente, gruppo o ruolo) disponga delle autorizzazioni appropriate per creare file system. Ciò include l'aggiunta della politica di autorizzazioni che supporta il ruolo collegato al servizio Amazon FSx for Lustre. Per ulteriori informazioni, consulta Aggiungere le autorizzazioni per utilizzare gli archivi di dati in Amazon S3.

Per ulteriori informazioni sui ruoli collegati al servizio, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

Risoluzione dei problemi di montaggio del file system

L'errore di un comando di montaggio del file system può causare diverse cause, come descritto nei seguenti argomenti.

Il montaggio del file system fallisce immediatamente

Il comando di montaggio del file system fallisce immediatamente. Il codice seguente mostra un esempio.

```
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?
```

Questo errore può verificarsi se non si utilizza il `mountname` valore corretto durante il montaggio di un file system persistente o scratch 2 utilizzando il mount comando. È possibile ottenere il `mountname` valore dalla risposta del describe-file-systems AWS CLI comando o dall'operazione DescribeFileSystemsAPI.

Il montaggio di un file system rimane in attesa e quindi ha esito negativo con un errore di timeout

Il comando di montaggio del file system si blocca per uno o due minuti, e quindi ha esito negativo con un errore di timeout.

Il codice seguente mostra un esempio.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx

[2+ minute wait here]
Connection timed out
```

Questo errore può verificarsi perché i gruppi di sicurezza per l' EC2 istanza Amazon o il file system non sono configurati correttamente.

Operazione da eseguire

Assicurati che i tuoi gruppi di sicurezza per il file system abbiano le regole in entrata specificate inGruppi di sicurezza Amazon VPC.

Il montaggio automatico non funziona e l'istanza non risponde

In alcuni casi, il montaggio automatico potrebbe fallire per un file system e l' EC2istanza Amazon potrebbe smettere di rispondere.

Questo problema può verificarsi se l'`_netdev`opzione non è stata dichiarata. Se `_netdev` manca, l' EC2 istanza Amazon può smettere di rispondere. Questo risultato è dovuto al fatto che i file system di rete devono essere inizializzati dopo che l'istanza di calcolo ha avviato la sua interfaccia di rete.

Operazione da eseguire

Se si verifica questo problema, contatta Supporto AWS.

Il montaggio del file system non riesce durante l'avvio del sistema

Il montaggio del file system non riesce durante l'avvio del sistema. Il montaggio è automatizzato utilizzando`/etc/fstab`. Quando il file system non è montato, nel syslog viene visualizzato il seguente errore relativo al periodo di avvio dell'istanza.

```
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
```

Questo errore può verificarsi quando la porta 988 non è disponibile. Quando l'istanza è configurata per montare i file system NFS, è possibile che i montaggi NFS colleghino la porta client alla porta 988

Operazione da eseguire

È possibile ovviare a questo problema ottimizzando le opzioni di montaggio e di montaggio del client NFS, ove possibile. `noresvport` `noauto`

Il montaggio del file system utilizzando il nome DNS non riesce

I nomi DNS (Domain Name Service) configurati in modo errato possono causare errori di montaggio del file system, come illustrato negli scenari seguenti.

Scenario 1: Un montaggio del file system che utilizza un nome DNS (Domain Name Service) non riesce. Il codice seguente mostra un esempio.

```
sudo mount -t lustre file_system_dns_name@tcp:/mountname /mnt/fsx
mount.lustre: Can't parse NID
'file_system_dns_name@tcp:/mountname'
```

Operazione da eseguire

Controlla la configurazione del tuo cloud privato virtuale (VPC). Se si sta usando una VPC personalizzata, accertarsi che le impostazioni DNS siano abilitate. Per ulteriori informazioni, consultare Utilizzo del DNS con i VPC nella Guida per l'utente di Amazon VPC.

Per specificare un nome DNS nel `mount` comando, procedi come segue:

- Assicurati che l' EC2 istanza Amazon si trovi nello stesso VPC del file system Amazon FSx for Lustre.
- Collega la tua EC2 istanza Amazon all'interno di un VPC configurato per utilizzare il server DNS fornito da Amazon. Per ulteriori informazioni, consulta Set opzioni DHCP nella Guida per l'utente di Amazon VPC.
- Assicurati che l'Amazon VPC dell' EC2 istanza Amazon connessa abbia i nomi host DNS abilitati. Per ulteriori informazioni, consulta Updating DNS Support for Your VPC nella Amazon VPC User Guide.

Scenario 2: Un montaggio del file system che utilizza un nome DNS (Domain Name Service) non riesce. Il codice seguente mostra un esempio.

```
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?
```

Operazione da eseguire

Assicurati che ai gruppi di sicurezza VPC del client siano applicate le regole di traffico in uscita corrette. Questa raccomandazione è valida soprattutto se non si utilizza il gruppo di sicurezza predefinito o se è stato modificato il gruppo di sicurezza predefinito. Per ulteriori informazioni, consulta Gruppi di sicurezza Amazon VPC.

Non è possibile accedere al file system

Esistono diverse cause potenziali per cui non è possibile accedere al file system, ognuna con la propria risoluzione, come segue.

L'indirizzo IP elastico collegato all'interfaccia di rete elastica del file system è stato eliminato

Amazon FSx non supporta l'accesso ai file system dalla rete Internet pubblica. Amazon scollega FSx automaticamente qualsiasi indirizzo IP elastico, che è un indirizzo IP pubblico raggiungibile da Internet, che viene collegato all'interfaccia di rete elastica di un file system.

L'interfaccia elastic network interface del file system è stata modificata o eliminata

Non è necessario modificare o eliminare l'elastic network interface del file system. La modifica o l'eliminazione dell'interfaccia di rete può causare una perdita permanente della connessione tra il VPC e il file system. Crea un nuovo file system e non modificare o eliminare l' FSx elastic network interface. Per ulteriori informazioni, consulta Controllo degli accessi ai file system con Amazon VPC.

Impossibile convalidare l'accesso a un bucket S3 durante la creazione di un DRA

La creazione di un'associazione di repository di dati (DRA) dalla FSx console Amazon o l'utilizzo del comando `create-data-repository-association` CLI (CreateDataRepositoryAssociationè l'azione API equivalente) non riesce e viene visualizzato il seguente messaggio di errore.

```
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**
>
> Puoi anche ricevere l'errore precedente quando crei un file system Scratch 1, Scratch 2 o Persistent 1 collegato a un repository di dati (bucket o prefisso S3) utilizzando la console Amazon FSx o il comando `create-file-system` CLI (CreateFileSystemè l'azione API equivalente).

Operazione da eseguire

Se il file system FSx for Lustre si trova nello stesso account del bucket S3, questo errore indica che il ruolo IAM utilizzato per la richiesta di creazione non dispone delle autorizzazioni necessarie per accedere al bucket S3. Assicurati che il ruolo IAM disponga delle autorizzazioni elencate nel messaggio di errore. Queste autorizzazioni supportano il ruolo collegato al servizio Amazon FSx for Lustre utilizzato per accedere al bucket Amazon S3 specificato per tuo conto.

Se il file system FSx for Lustre si trova in un account diverso da quello del bucket S3 (caso tra account diversi), oltre a verificare che il ruolo IAM utilizzato disponga delle autorizzazioni richieste,

è necessario configurare la policy del bucket S3 per consentire l'accesso dall'account in cui è stato creato for Lustre. FSx Di seguito è riportato un esempio di policy sui bucket,

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject",
                "s3:GetObject",
                "s3:GetBucketAcl",
                "s3:GetBucketNotification",
                "s3:ListBucket",
                "s3:PutBucketNotification"
            ],
            "Resource": [
                "arn:aws:s3:::bucket_name",
                "arn:aws:s3:::bucket_name/*"
            ],
            "Condition": {
                "StringLike": {
                    "aws:PrincipalArn": [
                        "arn:aws:iam::file_system_account_ID:role/aws-service-role/
s3.data-source.lustre.fsx.amazonaws.com/AWSServiceRoleForFSxS3Access_fs-*"
                }
            }
        }
    ]
}
```

Per ulteriori informazioni sulle autorizzazioni per i bucket tra account S3, consulta l'Esempio 2: Il proprietario del bucket concede le autorizzazioni per i bucket multiaccount nella Guida per l'utente di Amazon Simple Storage Service.

La ridenominazione delle directory richiede molto tempo

Domanda

Ho rinominato una directory su un file system collegato a un bucket Amazon S3 e ho abilitato l'esportazione automatica. Perché i file all'interno di questa directory impiegano molto tempo per essere rinominati nel bucket S3?

Risposta

Quando si rinomina una directory sul file system, FSx for Lustre crea nuovi oggetti S3 per tutti i file e le directory all'interno della directory che è stata rinominata. La quantità di tempo necessaria per propagare la ridenominazione della directory in S3 è direttamente correlata alla quantità di file e directory che discendono dalla directory da rinominare.

Risoluzione dei problemi relativi a un bucket S3 collegato non correttamente configurato

In alcuni casi, un bucket S3 collegato al file system FSx for Lustre potrebbe avere uno stato del ciclo di vita del repository di dati non configurato correttamente.

Possibile causa

Questo errore può verificarsi se Amazon FSx non dispone delle autorizzazioni AWS Identity and Access Management (IAM) necessarie per accedere al repository di dati collegato. Le autorizzazioni IAM richieste supportano il ruolo collegato al servizio Amazon FSx for Lustre utilizzato per accedere al bucket Amazon S3 specificato per tuo conto.

Operazione da eseguire

1. Assicurati che la tua entità IAM (utente, gruppo o ruolo) disponga delle autorizzazioni appropriate per creare file system. Ciò include l'aggiunta della politica di autorizzazioni che supporta il ruolo collegato al servizio Amazon FSx for Lustre. Per ulteriori informazioni, consulta Aggiungere le autorizzazioni per utilizzare gli archivi di dati in Amazon S3.
2. Utilizzando la FSx CLI o l'API di Amazon, aggiorna il file system con `AutoImportPolicy` il comando `update-file-system` CLI (UpdateFileSystemè l'azione API equivalente), come segue.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Per ulteriori informazioni sui ruoli collegati al servizio, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

Causa possibile

Questo errore può verificarsi se il repository di dati Amazon S3 collegato ha una configurazione di notifica degli eventi esistente con tipi di eventi che si sovrappongono alla configurazione di notifica degli FSx eventi di Amazon (,). `s3:ObjectCreated:*` `s3:ObjectRemoved:*`

Ciò può verificarsi anche se la configurazione di notifica FSx degli eventi di Amazon sul bucket S3 collegato è stata eliminata o modificata.

Operazione da eseguire

1. Rimuovi qualsiasi notifica di evento esistente sul bucket S3 collegato che utilizza uno o entrambi i tipi di eventi utilizzati dalla configurazione dell' FSx evento e. `s3:ObjectCreated:*` `s3:ObjectRemoved:*`
2. Assicurati che nel bucket S3 collegato sia presente una configurazione di notifica degli eventi S3 con il nome`FSx`, i tipi di evento `s3:ObjectCreated:*` e invia all'`s3:ObjectRemoved:*`argomento SNS con. ARN:*topic_arn_returned_in_API_response*
3. Riapplica la configurazione di notifica FSx degli eventi sul bucket S3 utilizzando la FSx CLI o l'API di Amazon per aggiornare il file system. `AutoImportPolicy` Fatelo con il comando `update-file-system` CLI (UpdateFileSystemè l'azione API equivalente), come segue.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--lustre-configuration AutoImportPolicy=the_existing_AutoImportPolicy
```

Risoluzione dei problemi di storage

In alcuni casi, potrebbero verificarsi problemi di archiviazione con il file system. È possibile risolvere questi problemi utilizzando `lfs` comandi, come il `lfs migrate` comando.

Errore di scrittura dovuto alla mancanza di spazio sulla destinazione di archiviazione

È possibile verificare l'utilizzo dello storage del file system utilizzando il `lfs df -h` comando, come descritto in[Layout di storage del file system](). Il `filesystem_summary` campo riporta l'utilizzo totale dello storage del file system.

Se l'utilizzo del disco del file system è del 100%, valuta la possibilità di aumentare la capacità di archiviazione del file system. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione.

Se l'utilizzo dello storage del file system non è al 100% e si verificano comunque errori di scrittura, è possibile che il file su cui si sta scrivendo sia archiviato su un OST completo.

Operazione da eseguire

- Se molti file OSTs sono pieni, aumentate la capacità di archiviazione del file system. Verificate la presenza di uno storage non bilanciato attivo OSTs seguendo le azioni della Archiviazione sbilanciata su OSTs sezione.
- Se non OSTs sei pieno, ottimizza la dimensione del buffer della pagina sporca del client applicando la seguente regolazione a tutte le istanze del client:

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

Archiviazione sbilanciata su OSTs

Amazon FSx for Lustre distribuisce nuove strisce di file in modo uniforme su tutto il territorio. OSTs Tuttavia, il file system potrebbe ancora diventare sbilanciato a causa dei modelli di I/O o del layout di archiviazione dei file. Di conseguenza, alcune destinazioni di storage possono diventare piene mentre altre rimangono relativamente vuote.

È possibile utilizzare il `lfs migrate` comando per spostare file o cartelle da una cartella più piena a una meno piena. OSTs È possibile utilizzare il `lfs migrate` comando in modalità a blocchi o non a blocchi.

- La modalità a blocchi è la modalità predefinita per il `lfs migrate` comando. Quando viene eseguito in modalità a blocchi, acquisisce `lfs migrate` innanzitutto un blocco di gruppo su file e directory prima della migrazione dei dati per impedire modifiche ai file, quindi rilascia il

blocco al termine della migrazione. Impedendo ad altri processi di modificare i file, la modalità a blocchi impedisce a questi processi di interrompere la migrazione. Lo svantaggio è che impedire a un'applicazione di modificare un file può causare ritardi o errori nell'applicazione.

- La modalità non a blocchi è abilitata per il `lfs migrate` comando con l'opzione. `-n` Quando vengono eseguiti `lfs migrate` in modalità non a blocchi, altri processi possono comunque modificare i file che vengono migrati. Se un processo modifica un file prima del `lfs migrate` completamento della migrazione, non `lfs migrate` riuscirà a migrare quel file, lasciando il file con il suo layout originale a strisce.

Ti consigliamo di utilizzare la modalità non a blocchi, poiché è meno probabile che interferisca con l'applicazione.

Operazione da eseguire

1. Avvia un'istanza client relativamente grande (come il tipo di EC2 `c5n.4xlarge` istanza Amazon) da montare sul file system.
2. Prima di eseguire lo script in modalità non blocco o lo script in modalità blocco, esegui i seguenti comandi su ogni istanza del client per accelerare il processo:

```
sudo lctl set_param 'mdc.*.max_rpcs_in_flight=60'
sudo lctl set_param 'mdc.*.max_mod_rpcs_in_flight=59'
```

3. Avvia una sessione sullo schermo ed esegui lo script in modalità non blocco o lo script in modalità blocco. Assicurati di modificare le variabili appropriate negli script:

   - Script in modalità non a blocchi:

```
#!/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
```

- Script in modalità blocco:
  - Sostituisci i valori 0STS con i valori del tuo OSTs.
  - Fornisci un valore intero `nproc` per impostare il numero di processi max-procs da eseguire in parallelo. Ad esempio, il tipo di EC2 `c5n.4xlarge` istanza Amazon ha 16 vCPUs, quindi puoi usare 16 (o un valore < 16) per`nproc`.
  - Fornisci il percorso della directory di montaggio in`mnt_dir_path`.

```
# find all OSTs with usage above a certain threshold; for example, greater than
 or equal to 85% full
for OST in $(lfs df -h |egrep '( 8[5-9]| 9[0-9]|100)%'|cut -d' ' -f1); do echo
 ${OST};done|tr '\012' ','

# customer can also just pass OST values directly to OSTS variable
OSTS='dzfevbmv-OST0000_UUID,dzfevbmv-OST0002_UUID,dzfevbmv-OST0004_UUID,dzfevbmv-
OST0005_UUID,dzfevbmv-OST0006_UUID,dzfevbmv-OST0008_UUID'

nproc=<Run up to max-procs processes if client is c5n.4xlarge with 16 vcpu, this
 value can be set to 16>

mnt_dir_path=<mount dir, e.g. '/my_mnt'>

lfs find ${mnt_dir_path} --ost ${OSTS}| xargs -P ${nproc} -n2 lfs migrate -E 100M
 -c 1 -E 10G -c 8 -E 100G -c 16 -E -1 -c 32
```

Note

- Se notate che c'è un impatto sulle prestazioni delle letture del file system, potete interrompere le migrazioni in qualsiasi momento utilizzando `ctrl-c` o k `ill -9` e ridurre il numero di thread (`nproc`valore) a un numero inferiore (ad esempio 8) e riprendere la migrazione dei file.
- Il `lfs migrate` comando avrà esito negativo su un file aperto anche dal carico di lavoro del client. Genererà un errore e passerà al file successivo; pertanto, se si accede a molti file, lo script non sarà in grado di migrare alcun file e ciò si rifletterà man mano che la migrazione procede molto lentamente.
- È possibile monitorare l'utilizzo di OST utilizzando uno dei seguenti metodi
  - Al momento del montaggio sul client, esegui il comando seguente per monitorare l'utilizzo di OST e trovare l'OST con un utilizzo superiore all'85%:

    ```
    lfs df -h |egrep '( 8[5-9]| 9[1-9]|100)%'
    ```

  - Controlla la CloudWatch metrica di Amazon`OST FreeDataStorageCapacity`, verifica`Minimum`. Se lo script rileva OSTs che è pieno per oltre l'85%, quando la metrica è vicina al 15%, usa `ctrl-c` o `kill -9` per interrompere la migrazione.

- Potresti anche prendere in considerazione la possibilità di modificare la configurazione dello stripe del tuo file system o di una directory, in modo che i nuovi file vengano distribuiti su più destinazioni di archiviazione. Per ulteriori informazioni, vedere in. Striping dei dati nel file system

Risoluzione dei problemi relativi FSx al driver Lustre CSI

Amazon FSx for Lustre supporta l'accesso dai container in esecuzione su Amazon EKS utilizzando il driver CSI open source FSx per Lustre. Per informazioni sulla distribuzione, consulta Use Amazon FSx for Lustre Storage nella Guida per l'utente di Amazon EKS.

Se riscontri problemi con il driver CSI FSx for Lustre per contenitori in esecuzione su Amazon EKS, consulta Risoluzione dei problemi del driver CSI (problemi comuni) disponibile su. GitHub

Informazioni aggiuntive

Questa sezione fornisce un riferimento alle funzionalità Amazon FSx supportate ma obsolete.

Argomenti

Configurazione di una pianificazione di backup personalizzata

Ti consigliamo di AWS Backup utilizzarlo per impostare una pianificazione di backup personalizzata per il tuo file system. Le informazioni fornite qui sono a scopo di riferimento se è necessario pianificare i backup più frequentemente di quanto sia possibile durante l'utilizzo AWS Backup.

Se abilitato, Amazon FSx esegue automaticamente un backup del file system una volta al giorno durante una finestra di backup giornaliera. Amazon FSx applica un periodo di conservazione specificato dall'utente per questi backup automatici. Supporta anche i backup avviati dall'utente, quindi puoi eseguire backup in qualsiasi momento.

Di seguito, puoi trovare le risorse e la configurazione per implementare una pianificazione dei backup personalizzata. La pianificazione dei backup personalizzata esegue backup avviati dall'utente su un file system Amazon FSx for Lustre secondo una pianificazione personalizzata definita dall'utente. Alcuni esempi potrebbero essere una volta ogni sei ore, una volta alla settimana e così via. Questo script configura anche l'eliminazione dei backup più vecchi del periodo di conservazione specificato.

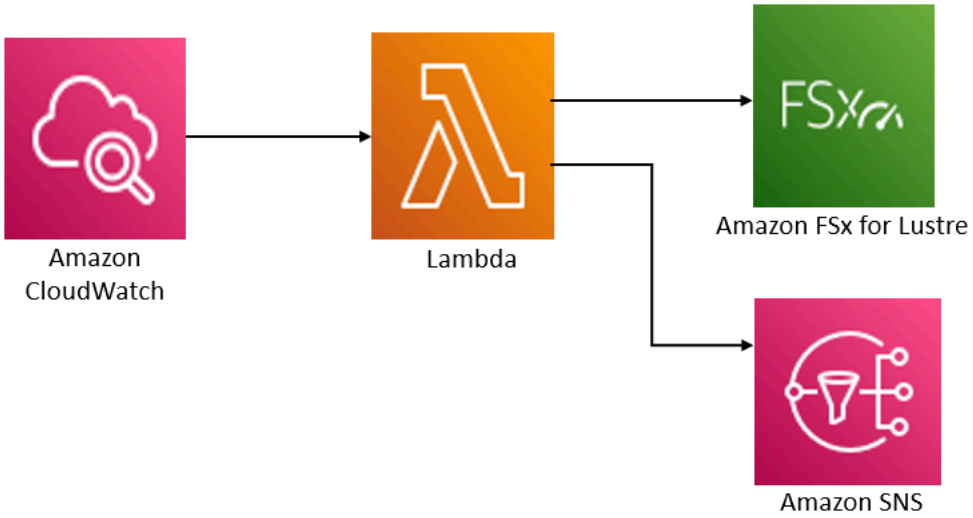
La soluzione distribuisce automaticamente tutti i componenti necessari e utilizza i seguenti parametri:

- Il file system
- Un modello di pianificazione CRON per l'esecuzione dei backup
- Il periodo di conservazione dei backup (in giorni)
- I tag con i nomi di backup

Per ulteriori informazioni sui modelli di pianificazione CRON, consulta Schedule Expressions for Rules nella Amazon CloudWatch User Guide.

Panoramica dell'architettura

L'implementazione di questa soluzione consente di creare le seguenti risorse in. Cloud AWS



Questa soluzione esegue le seguenti operazioni:

1. Il AWS CloudFormation modello implementa un CloudWatch evento, una funzione Lambda, una coda Amazon SNS e un ruolo IAM. Il ruolo IAM consente alla funzione Lambda di richiamare le operazioni dell'API Amazon FSx for Lustre.
2. L' CloudWatch evento viene eseguito secondo una pianificazione definita come pattern CRON, durante la distribuzione iniziale. Questo evento richiama la funzione Lambda del gestore di backup della soluzione che richiama l'operazione dell'API Amazon FSx for Lustre `CreateBackup` per avviare un backup.
3. Il backup manager recupera un elenco di backup esistenti avviati dall'utente per il file system specificato utilizzando. `DescribeBackups` Quindi elimina i backup precedenti al periodo di conservazione specificato durante la distribuzione iniziale.
4. Il backup manager invia un messaggio di notifica alla coda di Amazon SNS in caso di backup riuscito se scegli l'opzione per ricevere una notifica durante la distribuzione iniziale. Una notifica viene sempre inviata in caso di errore.

AWS CloudFormation modello

Questa soluzione consente AWS CloudFormation di automatizzare l'implementazione della soluzione di pianificazione del backup personalizzata Amazon FSx for Lustre. Per utilizzare questa soluzione, scarica il modello.template. fsx-scheduled-backup AWS CloudFormation

Distribuzione automatizzata

La procedura seguente configura e implementa questa soluzione di pianificazione dei backup personalizzata. L'implementazione richiede circa cinque minuti. Prima di iniziare, devi avere l'ID di un file system Amazon FSx for Lustre in esecuzione in un Amazon Virtual Private Cloud (Amazon VPC) nel AWS tuo account. Per ulteriori informazioni sulla creazione di queste risorse, consulta. Guida introduttiva ad Amazon FSx for Lustre

> **Note**
>
> L'implementazione di questa soluzione comporta la fatturazione dei servizi associati AWS . Per ulteriori informazioni, consulta le pagine dei dettagli sui prezzi di tali servizi.

Per avviare lo stack di soluzioni di backup personalizzate

1. Scarica il fsx-scheduled-backupmodello .template. AWS CloudFormation Per ulteriori informazioni sulla creazione di uno AWS CloudFormation stack, consulta Creazione di uno stack sulla AWS CloudFormation console nella Guida per l'AWS CloudFormation utente.

   > **Note**
   >
   > Per impostazione predefinita, questo modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). AWS Amazon FSx for Lustre è attualmente disponibile solo in alcuni casi specifici Regioni AWS. È necessario avviare questa soluzione in una AWS regione in cui è disponibile Amazon FSx for Lustre. Per ulteriori informazioni, consulta il Amazon FSx sezione Regioni AWS e Endpoints in. Riferimenti generali di AWS

2. Per Parametri, esaminate i parametri del modello e modificateli in base alle esigenze del file system. Questa soluzione utilizza i seguenti valori predefiniti.

Parametro	Predefinito	Descrizione
ID del file system Amazon FSx for Lustre	Nessun valore predefinito	L'ID del file system del file system di cui desideri eseguire il backup.

Parametro	Predefinito	Descrizione
Schema di pianificazione CRON per i backup.	0 0/4 * *? *	La pianificazione per l'esecuzione dell' CloudWatch evento, l'attivazione di un nuovo backup e l'eliminazione dei vecchi backup al di fuori del periodo di conservazione.
Conservazione del backup (giorni)	7	Il numero di giorni in cui conservare i backup avviati dall'utente. La funzione Lambda elimina i backup avviati dall'utente più vecchi di questo numero di giorni.
Nome per i backup	backup pianificato dall'utente	Il nome di questi backup, visualizzato nella colonna Backup Name della console di gestione Amazon FSx for Lustre.
Notifiche di backup	Sì	Scegli se ricevere una notifica quando i backup vengono avviati correttamente. Viene sempre inviata una notifica in caso di errore.
Indirizzo e-mail	Nessun valore predefinito	L'indirizzo e-mail per iscriversi alle notifiche SNS.

3. Scegli Next (Successivo).
4. Per Opzioni, scegli Avanti.
5. Per Revisione, rivedi e conferma le impostazioni. È necessario selezionare la casella di controllo per confermare che il modello crea risorse IAM.
6. Scegli Crea per distribuire lo stack.

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Status. Dovresti vedere lo stato di CREATE_COMPLETE tra circa cinque minuti.

Opzioni aggiuntive

Puoi utilizzare la funzione Lambda creata da questa soluzione per eseguire backup pianificati personalizzati di più di un file system Amazon FSx for Lustre. L'ID del file system viene passato alla funzione Amazon FSx for Lustre nell'input JSON dell' CloudWatch evento. Il JSON predefinito passato alla funzione Lambda è il seguente, in cui i valori `FileSystemId` per `SuccessNotification` e vengono passati dai parametri specificati all'avvio AWS CloudFormation dello stack.

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
}
```

Per pianificare i backup per un file system Amazon FSx for Lustre aggiuntivo, crea un'altra regola di CloudWatch evento. Lo fai utilizzando l'origine dell'evento Schedule, con la funzione Lambda creata da questa soluzione come destinazione. Scegliete Constant (testo JSON) in Configura input. Per l'input JSON, sostituisci semplicemente l'ID del file system Amazon FSx for Lustre di cui eseguire il backup al posto di. `${FileSystemId}` Inoltre, sostituiscilo con `Yes` o al posto del `No` codice JSON riportato sopra`${SuccessNotification}`.

Eventuali regole di CloudWatch evento aggiuntive create manualmente non fanno parte dello AWS CloudFormation stack di soluzioni di backup pianificato personalizzate Amazon FSx for Lustre. Pertanto, non vengono rimosse se elimini lo stack.

Cronologia dei documenti

- Versione API: 2018-03-01
- Ultimo aggiornamento della documentazione: 1 luglio 2025

La tabella seguente descrive importanti modifiche alla Amazon FSx for Lustre User Guide. Per ricevere notifiche sugli aggiornamenti della documentazione, è possibile sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Lustreè stato aggiunto il supporto client per Rocky Linux e Red Hat Enterprise Linux (RHEL) 9.6	Il client FSx for Lustre ora supporta EC2 le istanze Amazon che eseguono Rocky Linux e Red Hat Enterprise Linux (RHEL) 9.6. Per ulteriori informazioni, consulta Installazione del client. Lustre	1 luglio 2025
Support aggiunto per la classe di storage Intelligent-Tiering	Ora puoi creare file system FSx per Lustre con la classe di storage Intelligent-Tiering. Intelligent-Tiering offre uno storage completamente elastico con una cache SSD opzionale per l'accesso a bassa latenza ai dati a cui si accede di frequente. Per ulteriori informazioni, consulta Caratteristiche prestazionali della classe di storage Intelligent-Tiering.	29 maggio 2025
Amazon FSx ha aggiornato la politica FSx FullAccess AWS gestita da Amazon	La policy FSx FullAccess gestita da Amazon è stata aggiornata per aggiungere le `fsx:DetachAndDelet`	28 maggio 2025

	`eS3AccessPoint` autorizzazioni `fsx:Creat eAndAttachS3Access Point fsx:Descr ibeS3AccessPointAt tachments` , `fsx:Updat eS3AccessPointAtta chments`, e.	
Amazon FSx ha aggiornat o la politica FSx ConsoleFu llAccess AWS gestita da Amazon	La policy FSx ConsoleFu llAccess gestita da Amazon è stata aggiornata per aggiunger e le `fsx:DetachAndDelet eS3AccessPoint` autorizzazioni `fsx:Creat eAndAttachS3Access Point fsx:Descr ibeS3AccessPointAt tachments` , `fsx:Updat eS3AccessPointAtta chments`, e.	28 maggio 2025
Regione AWS Supporto aggiuntivo aggiunto	FSx i file system for Lustre sono ora disponibili in Asia Pacifico (Tailandia) e Messico (Centrale). Per ulteriori informazioni, consulta Disponibilità del tipo di distribuzione.	8 maggio 2025
Lustreè stato aggiunto il supporto client per Ubuntu 24	Il client FSx for Lustre ora supporta le EC2 istanze Amazon che eseguono Ubuntu 24.04. Per ulteriori informazi oni, consulta Installazione del client. Lustre	19 marzo 2025

Amazon FSx ha aggiornato la politica FSx ConsoleReadOnlyAccess AWS gestita da Amazon	Amazon FSx ha aggiornato la FSx ConsoleReadOnlyAccess politica di Amazon per aggiungere l'`ec2:DescribeNetworkInterfaces` autorizzazione. Per ulteriori informazioni, consulta la FSx ConsoleReadOnlyAccess politica di Amazon.	25 febbraio 2025
Support aggiunto per l'aggiornamento della versione Lustre	È ora possibile aggiornare la versione Lustre del file system FSx for Lustre a una versione più recente. Per ulteriori informazioni, vedere Managing Lustre version.	12 febbraio 2025
Amazon FSx ha aggiornato la politica FSx ConsoleFullAccess AWS gestita da Amazon	Amazon FSx ha aggiornato la FSx ConsoleFullAccess politica di Amazon per aggiungere l'`ec2:DescribeNetworkInterfaces` autorizzazione. Per ulteriori informazioni, consulta la FSx ConsoleFullAccess politica di Amazon.	7 febbraio 2025
Regione AWS Supporto aggiuntivo aggiunto per il tipo di distribuzione Persistent 2	Gli SSD Persistent 2 FSx per i file system Lustre sono ora disponibili nella regione Asia-Pacifico (Malesia). Regione AWS Per ulteriori informazioni, consulta Disponibilità del tipo di distribuzione.	2 gennaio 2025

Lustreè stato aggiunto il supporto client per Rocky Linux e Red Hat Enterprise Linux (RHEL) 9.5	Il client FSx for Lustre ora supporta EC2 le istanze Amazon che eseguono Rocky Linux e Red Hat Enterprise Linux (RHEL) 9.5. Per ulteriori informazioni, consulta Installazione del client. Lustre	26 dicembre 2024
Support aggiunto per EFA	È ora possibile creare un file system FSx for Lustre Persistent 2 con supporto per Elastic Fabric Adapter (EFA) che offre prestazioni di rete migliorate per le istanze client che supportano EFA. L'abilitazione di EFA fornisce anche il supporto per GPUDirect Storage (GDS) ed ENA Express. Per ulteriori informazioni, consulta Lavorare con i file system compatibili con EFA.	27 novembre 2024
Regione AWS Supporto aggiuntivo aggiunto per il tipo di distribuzione Persistent 2	Gli SSD Persistent 2 FSx per i file system Lustre sono ora disponibili negli Stati Uniti occidentali (California settentrionale). Regione AWS Per ulteriori informazioni, consulta Disponibilità del tipo di distribuzione.	27 novembre 2024

Lustresupporto client aggiunto per Ubuntu 22 Kernel 6.8.0	Il client FSx for Lustre ora supporta le EC2 istanze Amazon che eseguono Ubuntu 22.04 Kernel 6.8.0. Per ulteriori informazioni, consulta Installazione del client. Lustre	8 novembre 2024
Support aggiunto per ulteriori CloudWatch parametri Amazon e una dashboard di monitoraggio migliorata	FSx for Lustre offre ora parametri di rete, prestazioni e storage aggiuntivi e una dashboard di monitoraggio avanzata per una migliore visibilità dell'attività del file system. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.	25 settembre 2024
Regione AWS Supporto aggiuntivo aggiunto per il tipo di distribuzione Persistent 2	Gli SSD Persistent 2 FSx per i file system Lustre sono ora disponibili nella zona locale degli Stati Uniti orientali (Dallas). Per ulteriori informazioni, consulta Disponibilità del tipo di distribuzione.	20 settembre 2024
Lustresupporto client aggiunto per Ubuntu 22 Kernel 6.5.0	Il client FSx for Lustre ora supporta le EC2 istanze Amazon che eseguono Ubuntu 22.04 Kernel 6.5.0. Per ulteriori informazioni, consulta Installazione del client. Lustre	1° agosto 2024

Lustreè stato aggiunto il supporto client per CentOS, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.10	Il client FSx for Lustre ora supporta EC2 istanze Amazon che eseguono CentOS, Rocky Linux e Red Hat Enterpris e Linux (RHEL) 8.10. Per ulteriori informazioni, consulta Installazione del client. Lustre	18 giugno 2024
Support aggiunto per aumentare le prestazioni dei metadati	È ora possibile creare un file system FSx for Lustre Persistent 2 con una configura zione dei metadati che offre la possibilità di aumentare le prestazioni dei metadati. Per ulteriori informazioni, vedere Prestazioni dei metadati del file system e Gestione delle prestazioni dei metadati.	6 giugno 2024
Regione AWS Supporto aggiuntivo aggiunto per il tipo di distribuzione Persistent 2	Gli SSD Persistent 2 FSx per i file system Lustre sono ora disponibili nella zona locale degli Stati Uniti orientali (Atlanta). Per ulteriori informazioni, consulta Disponibilità del tipo di distribuzione.	29 maggio 2024
Lustreè stato aggiunto il supporto client per Rocky Linux e Red Hat Enterprise Linux (RHEL) 9.4	Il client FSx for Lustre ora supporta EC2 le istanze Amazon che eseguono Rocky Linux e Red Hat Enterprise Linux (RHEL) 9.4. Per ulteriori informazioni, consulta Installaz ione del client. Lustre	16 maggio 2024

Regione AWS Supporto aggiuntivo aggiunto per il tipo di distribuzione Persistent 2	Gli SSD Persistent 2 FSx per i file system Lustre sono ora disponibili nel Canada occidentale (Calgary). Regione AWS Per ulteriori informazioni, consulta Disponibilità del tipo di distribuzione.	3 maggio 2024
Lustreaggiunto il supporto client per Amazon Linux 2023	Il client FSx for Lustre ora supporta EC2 le istanze Amazon che eseguono Amazon Linux 2023. Per ulteriori informazioni, consulta Installazione del Lustre client.	25 marzo 2024
Lustreè stato aggiunto il supporto client per CentOS, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.9	Il client FSx for Lustre ora supporta EC2 istanze Amazon che eseguono CentOS, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.9. Per ulteriori informazioni, consulta Installazione del client. Lustre	9 gennaio 2024
Amazon FSx ha aggiornato le politiche FSx ServiceRolePolicy AWS gestite di Amazon FSx FullAccess FSx ConsoleFullAccess FSx ReadOnlyAccess FSxConsoleReadOnlyAccess, Amazon, Amazon e Amazon	Amazon FSx ha aggiornato le FSx ServiceRolePolicy politiche di Amazon FSx FullAccess FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon e Amazon per aggiungere l'`ec2:GetSecurityGroupsForVpc` autorizzazione. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	9 gennaio 2024

Lustreè stato aggiunto il supporto client per Rocky Linux e Red Hat Enterprise Linux (RHEL) 9.0 e 9.3	Il client FSx for Lustre ora supporta EC2 istanze Amazon che eseguono Rocky Linux e Red Hat Enterprise Linux (RHEL) 9.0 e 9.3. Per ulteriori informazioni, consulta Installazione del client. Lustre	20 dicembre 2023
Amazon FSx for Lustre ha aggiornato le politiche FSx ConsoleFullAccess AWS gestite da Amazon FSx FullAccess e Amazon	Amazon FSx ha aggiornato le FSx ConsoleFullAccess politiche di Amazon FSx FullAccess e Amazon per aggiungere l'`ManageCrossAccountDataReplication` azione. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	20 dicembre 2023
Amazon FSx ha aggiornato Amazon FSx FullAccess e le politiche FSx ConsoleFullAccess AWS gestite da Amazon	Amazon FSx ha aggiornato le FSx ConsoleFullAccess politiche di Amazon FSx FullAccess e Amazon per aggiungere l'`fsx:CopySnapshotAndUpdateVolume` autorizzazione. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	26 novembre 2023

Support aggiunto per la scalabilità della capacità di throughput	Ora puoi modificare la capacità di throughput esistente FSx per i file system persistenti basati su SSD Lustre man mano che i requisiti di throughput evolvono. Per ulteriori informazioni, vedere Gestione della capacità di trasmissione.	16 novembre 2023
Amazon FSx ha aggiornato Amazon FSx FullAccess e le politiche FSx ConsoleFullAccess AWS gestite da Amazon	Amazon FSx ha aggiornato le FSx ConsoleFullAccess politiche di Amazon FSx FullAccess e Amazon per aggiungere le `fsx:UpdateSharedVPCConfiguration` autorizzazioni `fsx:DescribeSharedVPCConfiguration` e. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	14 novembre 2023
Support aggiunto per le quote di progetto	Ora puoi creare quote di archiviazione per i progetti. Una quota di progetto si applica a tutti i file o le directory associati a un progetto. Per ulteriori informazioni, consulta Quote di archiviazione.	29 agosto 2023

Support aggiunto per la Lustre versione 2.15	I file system di All FSx for Lustre sono ora basati sulla Lustre versione 2.15 quando vengono creati utilizzando la console Amazon FSx . Per ulteriori informazioni, consulta Fase 1: creazione del file system Amazon FSx for Lustre.	29 agosto 2023
Regione AWS Supporto aggiuntivo aggiunto per il tipo di distribuzione Persistent 2	I file system Persistent 2 FSx for Lustre sono ora disponibili in Israele (Tel Aviv). Regione AWS Per ulteriori informazioni, consulta Opzioni di distribuzione FSx per i file system Lustre.	24 agosto 2023
Support aggiunto per le attività del repository dei dati di rilascio	FSx for Lustre ora fornisce attività di release data repository per rilasciare file archiviati da un file system collegato a un repository di dati S3. Il rilascio di un file mantiene l'elenco dei file e i metadati, ma rimuove la copia locale del contenuto di quel file. Per ulteriori informazioni, consulta Utilizzo delle attività del repository di dati per rilasciare file.	9 agosto 2023

Amazon FSx ha aggiornato la politica FSx ServiceRolePolicy AWS gestita da Amazon	Amazon FSx ha aggiornato l'`cloudwatch:PutMetricData` autorizzazione in Amazon FSxServiceRolePolicy. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	24 luglio 2023
Amazon FSx ha aggiornato la politica FSx FullAccess AWS gestita da Amazon	Amazon FSx ha aggiornato la FSx FullAccess politica di Amazon per rimuovere l'`fsx:*`autorizzazione e aggiungere `fsx` azioni specifiche. Per ulteriori informazioni, consulta la FSx FullAccess policy di Amazon.	13 luglio 2023
Amazon FSx ha aggiornato la politica FSx ConsoleFullAccess AWS gestita da Amazon	Amazon FSx ha aggiornato la FSx ConsoleFullAccess politica di Amazon per rimuovere l'`fsx:*`autorizzazione e aggiungere `fsx` azioni specifiche. Per ulteriori informazioni, consulta la FSx ConsoleFullAccess policy di Amazon.	13 luglio 2023
Lustreè stato aggiunto il supporto client per CentOS, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.8	Il client FSx for Lustre ora supporta EC2 istanze Amazon che eseguono CentOS, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.8. Per ulteriori informazioni, consulta Installazione del client. Lustre	25 maggio 2023

Support aggiunto per AutoImport e AutoExport metriche	FSx for Lustre ora fornisce CloudWatch parametri Amazon che monitorano gli aggiornamenti automatici di importazione ed esportazi one per i file system collegati agli archivi di dati. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.	31 marzo 2023
È stato aggiunto il supporto DRA per i tipi di distribuzione Persistent 1 e Scratch 2	È ora possibile creare associazioni di archivi di dati per collegare gli archivi di dati ai file system Lustre 2.12 con tipi di distribuzione Persisten t 1 o Scratch 2. Per ulteriori informazioni, consulta Usare gli archivi di dati con Amazon FSx for Lustre.	29 marzo 2023
Lustreè stato aggiunto il supporto client per CentOS, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.7	Il client FSx for Lustre ora supporta EC2 istanze Amazon che eseguono CentOS, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.7. Per ulteriori informazioni, consulta Installaz ione del client. Lustre	5 dicembre 2022

Regione AWS Supporto aggiuntivo aggiunto per il tipo di distribuzione Persistent 2	Gli SSD Persistent 2 di nuova generazione FSx per i file system Lustre sono ora disponibili in Europa (Stoccolma), Asia Pacifico (Hong Kong), Asia Pacifico (Mumbai) e Asia Pacifico (Seoul). Regioni AWS Per ulteriori informazioni, consulta Opzioni di distribuzione per i file system Lustre. FSx	10 novembre 2022
Lustreè stato aggiunto il supporto client per CentOS, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.6	Il client FSx for Lustre ora supporta EC2 istanze Amazon che eseguono CentOS, Rocky Linux e Red Hat Enterprise Linux (RHEL) 8.6. Per ulteriori informazioni, consulta Installazione del client. Lustre	8 settembre 2022
Lustreè stato aggiunto il supporto client per Ubuntu 22	Il client FSx for Lustre ora supporta le EC2 istanze Amazon che eseguono Ubuntu 22.04. Per ulteriori informazioni, consulta Installazione del client. Lustre	28 luglio 2022
Lustreè stato aggiunto il supporto client per Rocky Linux	Il client FSx for Lustre ora supporta le EC2 istanze Amazon che eseguono Rocky Linux. Per ulteriori informazioni, consulta Installazione del client. Lustre	8 luglio 2022

Support aggiunto per Lustre root squash	Ora puoi usare la funzionalità Lustre root squash per limitare l'accesso a livello root da parte dei client che tentano di accedere al file system FSx for Lustre come root. Per ulteriori informazioni, vedete Lustreroo t squash.	25 maggio 2022
Regione AWS Supporto aggiuntivo aggiunto per il tipo di distribuzione Persistent 2	Gli SSD Persistent 2 di nuova generazione FSx per i file system Lustre sono ora disponibili in Europa (Londra), Asia Pacifico (Singapore) e Asia Pacifico (Sydney). Regioni AWS Per ulteriori informazioni, consulta Opzioni di distribuzione FSx per i file system Lustre.	19 aprile 2022
Supporto aggiunto per l'utilizz o AWS DataSync per la migrazione dei file verso i file system Amazon FSx for Lustre.	Ora puoi utilizzarlo AWS DataSync per migrare i file dai file system esistenti ai file system FSx Lustre. Per ulteriori informazioni, consulta Come migrare i file esistenti su FSx for Lustre utilizzando. AWS DataSync	5 aprile 2022
Support aggiunto per gli AWS PrivateLink endpoint VPC di interfaccia	Ora puoi utilizzare gli endpoint VPC dell'interfaccia per accedere all' FSx API Amazon dal tuo VPC senza inviare traffico su Internet. Per ulteriori informazioni, consulta Amazon FSx e interfaccia gli endpoint VPC.	5 aprile 2022

Support aggiunto per l'Lustreaccodamento DRA	È ora possibile creare un'associazione DRA (data repository association) quando si crea un FSx file system for Lustre. La richiesta verrà messa in coda e il DRA verrà creato una volta che il file system sarà disponibile. Per ulteriori informazioni, consulta Collegamento del file system a un bucket S3.	28 febbraio 2022
Lustreaggiunto il supporto client per CentOS e Red Hat Enterprise Linux (RHEL) 8.5	Il client FSx for Lustre ora supporta EC2 istanze Amazon che eseguono CentOS e Red Hat Enterprise Linux (RHEL) 8.5. Per ulteriori informazioni, consulta Installazione del client. Lustre	20 dicembre 2021
Support per l'esportazione delle modifiche da FSx for Lustre in un repository di dati collegato	Ora puoi configurare Lustre FSx per esportare automaticamente file nuovi, modificati ed eliminati dal tuo file system a un repository di dati Amazon S3 collegato. Puoi utilizzare le attività del repository di dati per esportare dati e modifiche ai metadati nel repository di dati. È inoltre possibile configurare collegamenti a più archivi di dati. Per ulteriori informazioni, vedere Esportazione delle modifiche all'archivio di dati.	30 novembre 2021

Support aggiunto per la Lustre registrazione	Ora puoi configurare Lustre FSx per registrare su Amazon CloudWatch Logs gli eventi di errore e avviso per gli archivi di dati associati al tuo file system. Per ulteriori informazioni, consulta Logging with Amazon CloudWatch Logs.	30 novembre 2021
I file system SSD persistenti supportano un throughput più elevato e una capacità di archiviazione inferiore	Gli SSD persistenti di nuova generazione FSx per i file system Lustre offrono opzioni di throughput più elevate e una capacità di archiviazione minima inferiore. Per ulteriori informazioni, consulta Opzioni di distribuzione per FSx i file system Lustre.	30 novembre 2021
Support aggiunto per la Lustre versione 2.12	Ora puoi scegliere la Lustre versione 2.12 quando crei un file system FSx for Lustre. Per ulteriori informazioni, consulta Fase 1: creazione del file system Amazon FSx for Lustre.	5 ottobre 2021
Lustreaggiunto il supporto client per CentOS e Red Hat Enterprise Linux (RHEL) 8.4	Il client FSx for Lustre ora supporta EC2 istanze Amazon che eseguono CentOS e Red Hat Enterprise Linux (RHEL) 8.4. Per ulteriori informazioni, consulta Installazione del client. Lustre	9 giugno 2021

Support aggiunto per la compressione dei dati	Ora puoi abilitare la compressione dei dati quando crei un file system FSx for Lustre. È inoltre possibile abilitare o disabilitare la compressione dei dati su un file system FSx for Lustre esistente. Per ulteriori informazioni, vedete compressione Lustre dei dati.	27 maggio 2021
Support aggiunto per la copia dei backup	Ora puoi usare Amazon FSx per copiare i backup all'interno dello stesso Account AWS su un altro Regione AWS (copie tra regioni) o all'interno della stessa Regione AWS (copie all'interno della stessa regione). Per ulteriori informazioni, consulta Copiare i backup.	12 Aprile 2021
Lustresupporto client per set di file Lustre	Il client FSx for Lustre ora supporta l'uso di set di file per montare solo un sottoinsieme dello spazio dei nomi del file system. Per ulteriori informazioni, vedere Montaggio di set di file specifici.	18 marzo 2021
Support aggiunto per l'accesso dei client tramite indirizzi IP non privati	È possibile accedere FSx ai file system Lustre da un client locale utilizzando indirizzi IP non privati. Per ulteriori informazioni, consulta Montaggio di Amazon FSx file system da un ambiente locale o da un Amazon VPC peering.	17 dicembre 2020

Lustreaggiunto il supporto client per CentOS 7.9 basato su ARM	Il client FSx for Lustre ora supporta le EC2 istanze Amazon che eseguono CentOS 7.9 basato su ARM. Per ulteriori informazioni, consulta Installazione del client. Lustre	17 dicembre 2020
Lustreaggiunto il supporto client per CentOS e Red Hat Enterprise Linux (RHEL) 8.3	Il client FSx for Lustre ora supporta EC2 istanze Amazon che eseguono CentOS e Red Hat Enterprise Linux (RHEL) 8.3. Per ulteriori informazioni, consulta Installazione del client. Lustre	16 dicembre 2020
Support aggiunto per la scalabilità della capacità di storage e throughput	Ora è possibile aumentare la capacità di storage e di throughput dei file system esistenti FSx per Lustre man mano che i requisiti di storage e throughput si evolvono. Per ulteriori informazioni, vedere Gestione della capacità di storage e throughput.	24 novembre 2020
Support aggiunto per le quote di archiviazione	Ora puoi creare quote di archiviazione per utenti e gruppi. Le quote di archiviazione limitano la quantità di spazio su disco e il numero di file che un utente o un gruppo può consumare sul file system FSx for Lustre. Per ulteriori informazioni, vedere Quote di archiviazione.	9 novembre 2020

Amazon FSx è ora integrato con AWS Backup	Ora puoi utilizzarli AWS Backup per eseguire il backup e il ripristino dei FSx file system oltre a utilizzare i FSx backup nativi di Amazon. Per ulteriori informazioni, consulta Using AWS Backup with Amazon FSx.	9 novembre 2020
Support aggiunto per le opzioni di archiviazione HDD (unità disco rigido)	Oltre all'opzione di archiviazione SSD (unità a stato solido), FSx for Lustre ora supporta l'opzione di archiviazione HDD (unità disco rigido). È possibile configurare il file system in modo che utilizzi l'HDD per carichi di lavoro ad alta velocità di trasmissione, che in genere prevedono operazioni sequenziali su file di grandi dimensioni. Per ulteriori informazioni, consulta Opzioni di archiviazione multiple.	12 agosto 2020
Support per l'importazione di modifiche al repository di dati collegati in FSx for Lustre	È ora possibile configurare il file system FSx for Lustre per importare automaticamente i nuovi file aggiunti e i file modificati in un repository di dati collegato dopo la creazione del file system. Per ulteriori informazioni, consulta Importazione automatica degli aggiornamenti dal data repository.	23 luglio 2020

Lustresupporto client per SUSE Linux e aggiunto SP4 SP5	Il client FSx for Lustre ora supporta EC2 le istanze Amazon che eseguono SUSE Linux e. SP4 SP5 Per ulteriori informazioni, consulta Installazione del client. Lustre	20 luglio 2020
Lustreaggiunto il supporto client per CentOS e Red Hat Enterprise Linux (RHEL) 8.2	Il client FSx for Lustre ora supporta EC2 istanze Amazon che eseguono CentOS e Red Hat Enterprise Linux (RHEL) 8.2. Per ulteriori informazioni, consulta Installazione del client. Lustre	20 luglio 2020
Support per backup automatici e manuali del file system aggiunto	Ora puoi eseguire backup giornalieri automatici e backup manuali di file system non collegati a un repository di dati durevole di Amazon S3. Per ulteriori informazioni, consulta Utilizzo dei backup.	23 giugno 2020
Sono stati rilasciati due nuovi tipi di distribuzione dei file system	I file system Scratch sono progettati per l'archiviazione temporanea e l'elaborazione a breve termine dei dati. I file system persistenti sono progettati per l'archiviazione e i carichi di lavoro a lungo termine. Per ulteriori informazioni, consulta le opzioni di distribuzione di FSx Lustre.	12 febbraio 2020

Support per i metadati POSIX aggiunto	FSx for Lustre conserva i metadati POSIX associati durante l'importazione e l'esportazione di file in un repository di dati durevole collegato su Amazon S3. Per ulteriori informazioni, consulta il supporto dei metadati POSIX per gli archivi di dati.	23 dicembre 2019
È stata rilasciata una nuova funzionalità per le attività di archiviazione dei dati	Ora puoi esportare i dati modificati e i metadati POSIX associati in un repository di dati durevole collegato su Amazon S3 utilizzando le attività del repository di dati. Per ulteriori informazioni, consulta Attività nell'archivio dati.	23 dicembre 2019
Regione AWS Supporto aggiuntivo aggiunto	FSx for Lustre è ora disponibi le nella regione Regione AWS Europa (Londra). FSx Per i limiti specifici della regione Lustre, vedi Limiti.	9 luglio 2019
Supporto aggiuntivo aggiunto Regione AWS	FSx for Lustre è ora disponibi le nella regione Asia-Pacifico (Singapore). Regione AWS FSx Per i limiti specifici della regione Lustre, vedi Limiti.	26 giugno 2019

Lustresupporto clienti per e aggiunto Amazon LinuxAmazon Linux 2	Il client FSx for Lustre ora supporta EC2 le istanze Amazon in esecuzione Amazon Linux e. Amazon Linux 2 Per ulteriori informazioni, consulta Installazione del Lustre client.	11 marzo 2019
È stato aggiunto il supporto per il percorso di esportazione dei dati definito dall'utente	Gli utenti ora hanno la possibilità di sovrascrivere gli oggetti originali nel bucket Amazon S3 o di scrivere i file nuovi o modificati in un prefisso da te specificato. Con questa opzione, hai una maggiore flessibilità da incorporare Lustre nei tuoi flussi di FSx lavoro di elaborazione dei dati. Per ulteriori informazioni, consulta Esportazione dei dati nel bucket Amazon S3.	6 febbraio 2019
Il limite di storage totale predefinito è aumentato	Lo spazio di archiviazione totale predefinito FSx per tutti i file system Lustre è aumentato a 100.800 GiB. Per ulteriori informazioni, consulta Limiti.	11 gennaio 2019
Amazon FSx for Lustre è ora disponibile a tutti	Amazon FSx for Lustre è un file system completamente gestito ottimizzato per carichi di lavoro ad alta intensità di calcolo, come l'elaborazione ad alte prestazioni, l'apprendimento automatico e i flussi di lavoro di elaborazione multimediale.	28 novembre 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.