Guida per l'utente di ONTAP

FSx per ONTAP

FSx per ONTAP: Guida per l'utente di ONTAP

Table of Contents

Cos'è Amazon FSx for NetApp ONTAP?

Amazon FSx for NetApp ONTAP è un servizio completamente gestito che fornisce uno storage di file altamente affidabile, scalabile, ad alte prestazioni e ricco di funzionalità basato sul popolare file system ONTAP. NetApp FSx for ONTAP combina le caratteristiche, le prestazioni, le capacità e le operazioni API familiari dei NetApp file system con l'agilità, la scalabilità e la semplicità di un sistema completamente gestito. Servizio AWS

FSx for ONTAP offre uno storage di file condiviso ricco di funzionalità, veloce e flessibile, ampiamente accessibile dalle istanze di calcolo Linux, Windows e macOS in esecuzione in locale o in locale. AWS FSx for ONTAP offre storage su unità a stato solido (SSD) ad alte prestazioni con latenze inferiori al millisecondo. Con FSx for ONTAP, puoi raggiungere livelli di prestazioni SSD per il tuo carico di lavoro pagando lo storage SSD solo per una piccola parte dei tuoi dati.

La gestione dei dati con FSx for ONTAP è più semplice perché è possibile creare istantanee, clonare e replicare i file con un semplice clic. Inoltre, FSx for ONTAP suddivide automaticamente i dati su uno storage elastico a basso costo, riducendo la necessità di fornire o gestire la capacità.

FSx for ONTAP offre anche uno storage ad alta disponibilità e durevole con backup completamente gestiti e supporto per il disaster recovery tra regioni. Per semplificare la protezione e la protezione dei dati, FSx for ONTAP supporta le applicazioni antivirus e di sicurezza dei dati più diffuse.

Per i clienti che utilizzano NetApp ONTAP in locale, FSx for ONTAP è la soluzione ideale per migrare, eseguire il backup o eseguire il burst delle applicazioni basate su file da on-premise a AWS senza la necessità di modificare il codice dell'applicazione o il modo in cui gestisci i dati.

In quanto servizio completamente gestito, FSx for ONTAP semplifica l'avvio e la scalabilità di uno storage di file condiviso affidabile, ad alte prestazioni e sicuro nel cloud. Con FSx for ONTAP, non devi più preoccuparti di:

- Configurazione e provisioning di file server e volumi di storage
- Replica dei dati
- Installazione e applicazione di patch al software del file server
- Rilevamento e risoluzione dei guasti hardware
- Gestione del failover e del failback
- Esecuzione manuale dei backup

FSx for ONTAP offre anche una ricca integrazione con altri AWS servizi, come AWS Identity and Access Management (IAM), Amazon WorkSpaces, AWS Key Management Service (AWS KMS) e. AWS CloudTrail

Argomenti

Caratteristiche di FSx for ONTAP

Con FSx for ONTAP, ottieni una soluzione di storage di file completamente gestita con:

- Support per set di dati su scala petabyte in un unico namespace
- Fino a decine di gigabyte al secondo (GBps) di velocità effettiva per file system
- Accesso multiprotocollo ai dati tramite i protocolli Network File System (NFS), Server Message Block (SMB) e Internet Small Computer Systems Interface (iSCSI)
- Opzioni di implementazione Multi-AZ e Single-AZ ad alta disponibilità e durata
- Suddivisione automatica dei dati su più livelli che riduce i costi di storage trasferendo automaticamente i dati a cui si accede raramente a un livello di storage più economico in base ai modelli di accesso
- Compressione, deduplicazione e compattazione dei dati per ridurre il consumo di storage
- Support per la SnapMirror funzionalità NetApp di replica
- Support per le soluzioni NetApp di caching locali: NetApp Global File Cache e FlexCache
- Support per l'accesso e la gestione tramite operazioni native AWS o NetApp strumenti e API
  - AWS Management Console, AWS Command Line Interface (AWS CLI) e SDK
  - NetApp CLI ONTAP, API REST e BlueXP
- Support per le seguenti funzionalità di protezione e sicurezza dei dati:
  - Crittografia dei dati del file system e dei backup inattivi utilizzando AWS KMS keys
  - Crittografia dei dati in transito utilizzando le chiavi di sessione Kerberos SMB

- Scansione antivirus su richiesta
- Autenticazione e autorizzazione tramite Microsoft Active Directory
- Controllo dell'accesso ai file
- NetAppSnapLockFunzionalità WORM con supporto per volumi Compliance ed Enterprise

Sicurezza e protezione dei dati

Amazon FSx offre diversi livelli di sicurezza e conformità per facilitare la protezione dei dati. Crittografa automaticamente i dati inattivi nei file system e nei backup utilizzando le chiavi gestite in AWS Key Management Service ().AWS KMS Puoi anche crittografare i dati in transito utilizzando Kerberos per client NFS e SMB.

È stata valutata la conformità di Amazon FSx ai seguenti standard:

- Organizzazione internazionale per gli standard (ISO)
- Payment Card Industry Data Security Standard (PCI DSS)
- Certificazioni SOC (System and Organization Controls)
- L'Health Insurance Portability and Accountability Act del 1996 (HIPAA)

Per ulteriori informazioni, consulta Protezione dei dati in Amazon FSx for ONTAP NetApp .

Amazon FSx offre anche i seguenti livelli di controllo degli accessi:

- A livello di file system, Amazon FSx fornisce il controllo degli accessi utilizzando i gruppi di sicurezza Amazon Virtual Private Cloud (Amazon VPC).
- A livello di API, Amazon FSx fornisce il controllo degli accessi utilizzando policy di accesso AWS Identity and Access Management (IAM).
- Per fornire il controllo degli accessi a livello di file e cartelle, Amazon FSx supporta autorizzazioni Unix, elenchi di controllo di accesso (ACL) NFS e ACL NTFS. Quando si unisce Amazon FSx a un Active Directory, gli utenti che accedono ai file system possono autenticarsi utilizzando le proprie credenziali Active Directory.

Per consentirti di visualizzare le azioni intraprese dagli utenti sulle tue risorse Amazon FSx, Amazon FSx si integra per monitorare e AWS CloudTrail registrare le tue chiamate API Amazon FSx. Per ulteriori informazioni, consulta Registrazione di FSx per le chiamate API ONTAP conAWS CloudTrail.

Inoltre, Amazon FSx protegge i tuoi dati con backup di file system altamente durevoli. Amazon FSx esegue backup giornalieri automatici e puoi eseguire backup aggiuntivi in qualsiasi momento. Per ulteriori informazioni, consulta Proteggere i tuoi dati.

Prezzi di FSx for ONTAP

I file system vengono fatturati in base alle seguenti categorie:

- Capacità di archiviazione SSD (per gigabyte al mese o GB al mese)
- IOPS SSD forniti oltre tre IOPS/GB (per IOPS al mese)
- Capacità di throughput (per megabyte al secondo [MBps] al mese)
- Consumo di storage in pool di capacità (per GB al mese)
- Richieste di pool di capacità (per lettura e scrittura)
- Consumo di storage di backup (per GB al mese)

Per ulteriori informazioni sui prezzi e le commissioni associati al servizio, consulta i prezzi di Amazon FSx for NetApp ONTAP.

Forum FSx per ONTAP

Se riscontri problemi durante l'utilizzo di Amazon FSx, utilizza i forum di discussione di FSx for ONTAP per ottenere risposte.

Sei un utente Amazon FSx per la prima volta?

Se utilizzi Amazon FSx per la prima volta, ti consigliamo di leggere le seguenti sezioni nell'ordine:

1. Se sei nuovo AWS, consulta Configurazione di FSx per ONTAP per configurare un. Account AWS
2. Se sei pronto a creare il tuo primo file system Amazon FSx, segui le istruzioni riportate in. Guida introduttiva ad Amazon FSx for ONTAP NetApp
3. Per informazioni sulle prestazioni, consultare Amazon FSx per NetApp prestazioni ONTAP.
4. Per i dettagli sulla sicurezza di Amazon FSx, consulta. Sicurezza in Amazon FSx per ONTAP NetApp
5. Per informazioni sull'API Amazon FSx, consulta l'Amazon FSx API Reference.

Come funziona Amazon FSx for NetApp ONTAP

Questo argomento introduce le caratteristiche principali dei file system Amazon FSx NetApp for ONTAP e il loro funzionamento, con collegamenti a sezioni con descrizioni approfondite, importanti dettagli di implementazione e procedure di configurazione. step-by-step

Argomenti

File system FSx per ONTAP

Un file system è la risorsa FSx for ONTAP principale, analoga a un cluster ONTAP locale. NetApp Devi specificare la capacità di storage e la capacità di throughput delle unità a stato solido (SSD) per il tuo file system e scegli un Amazon Virtual Private Cloud (VPC) in cui creare il file system. Per ulteriori informazioni, consulta Gestione dei file system FSx for ONTAP.

Il file system può avere da una a 12 coppie ad alta disponibilità (HA) a seconda della configurazione. Una coppia HA è composta da due file server in una configurazione di standby attivo. I file system con una singola coppia HA sono chiamati file system scalabili. I file system con più coppie HA sono chiamati file system con scalabilità orizzontale. Per ulteriori informazioni, consulta Coppie ad alta disponibilità (HA).

Macchine virtuali di storage

Una macchina virtuale di archiviazione (SVM) è un file server isolato con propri endpoint amministrativi e di accesso ai dati per l'amministrazione e l'accesso ai dati. Quando accedete ai dati nel file system FSx for ONTAP, i client e le workstation si interfacciano con una SVM utilizzando l'indirizzo IP dell'endpoint SVM. Per ulteriori informazioni, consulta Gestione delle SVM.

È possibile aggiungere SVM a Microsoft Active Directory per l'autenticazione e l'autorizzazione dell'accesso ai file. Per ulteriori informazioni, consulta Utilizzo di Microsoft Active Directory in FSx for ONTAP.

Volumi

I volumi FSx for ONTAP sono risorse virtuali utilizzate per organizzare e raggruppare i dati. I volumi sono contenitori logici ospitati su SVM e i dati in essi archiviati consumano la capacità di archiviazione fisica del file system.

Quando si crea un volume, si imposta la dimensione, che determina la quantità di dati fisici che è possibile archiviare al suo interno, indipendentemente dal livello di storage su cui sono archiviati i dati. È inoltre possibile impostare il tipo di volume, RW (lettura-scrivibile) o DP (protezione dei dati). Un volume DP è di sola lettura e può essere utilizzato come destinazione in una relazione or. NetApp SnapMirror SnapVault

I volumi FSx for ONTAP sono dotati di thin provisioning, il che significa che consumano solo la capacità di storage per i dati in essi archiviati. Con i volumi con thin provisioning, la capacità di storage non viene prenotata in anticipo. Lo storage viene invece allocato dinamicamente, in base alle necessità. Lo spazio libero viene restituito al file system quando i dati nel volume o nella LUN vengono eliminati. Ad esempio, puoi creare tre volumi da 10 TiB su un file system configurato con 10 TiB di capacità di storage gratuita, purché la quantità totale di dati archiviati nei tre volumi non superi i 10 TiB in qualsiasi momento. La quantità di dati archiviati fisicamente su un volume viene conteggiata ai fini del consumo complessivo della capacità di storage. Per ulteriori informazioni, consulta Gestione dei volumi FSx for ONTAP.

Livelli di storage

Un file system FSx for ONTAP ha due livelli di storage: storage primario e storage con pool di capacità. Lo storage principale è uno storage SSD fornito, scalabile e ad alte prestazioni, creato appositamente per la parte attiva del set di dati. Lo storage con pool di capacità è un livello di storage completamente elastico che può scalare fino a petabyte ed è ottimizzato in termini di costi per i dati a cui si accede raramente. I dati scritti sui volumi consumano la capacità dei livelli di storage. Per ulteriori informazioni, consulta Livelli di storage FSx for ONTAP.

Tiering di dati

Il data tiering è il processo mediante il quale Amazon FSx NetApp for ONTAP sposta automaticamente i dati tra l'SSD e i livelli di storage del pool di capacità. Ogni volume ha una politica di suddivisione in più livelli che controlla se i dati vengono trasferiti al livello di capacità quando diventano inattivi (a freddo). Il periodo di raffreddamento della politica di tiering di un volume determina quando i dati diventano inattivi (a freddo). Per ulteriori informazioni, consulta Suddivisione dei dati su più livelli.

Efficienza dello storage

Amazon FSx for NetApp ONTAP supporta le funzionalità di efficienza dello storage a livello di blocco di ONTAP (compattazione, compressione e deduplicazione) per ridurre la capacità di storage consumata dai dati. Le funzionalità di efficienza dello storage possono ridurre l'ingombro dei dati nello storage SSD, nello storage in pool di capacità e nei backup. Il risparmio di capacità di archiviazione tipico per carichi di lavoro generici di condivisione di file senza sacrificare le prestazioni è pari al 65% grazie alla compressione, alla deduplicazione e alla compattazione, sia sui livelli di storage SSD che su quelli con pool di capacità. Per ulteriori informazioni, consulta FSx per l'efficienza dello storage ONTAP.

Accesso ai dati archiviati sui file system FSx for ONTAP

È possibile accedere ai dati sui volumi FSx for ONTAP da più client Linux, Windows o macOS contemporaneamente tramite i protocolli NFS (v3, v4, v4.1, v4.2) e SMB. È inoltre possibile accedere ai dati utilizzando il protocollo iSCSI (a blocchi). Per ulteriori informazioni, consulta Accesso ai dati .

Gestione delle risorse FSx for ONTAP

Esistono diversi modi per interagire con il file system FSx for ONTAP e gestirne le risorse. È possibile gestire le risorse FSx for ONTAP utilizzando entrambi gli strumenti di gestione AWS e NetApp ONTAP:

- AWS strumenti di gestione
  - La AWS Management Console
  - Il AWS Command Line Interface (AWS CLI)
  - L'API e gli SDK di Amazon FSx

    - AWS CloudFormation
- NetApp strumenti di gestione:
    - NetApp BlueXP
    - La CLI NetApp di ONTAP
    - L'API REST NetApp ONTAP

Per ulteriori informazioni, consulta Amministrazione delle risorse.

Configurazione di FSx per ONTAP

Prima di utilizzare Amazon FSx per la prima volta, completa le seguenti attività:

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

Argomenti

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 pagina all'indirizzo https://portal.aws.amazon.com/billing/signup.
2. Segui le istruzioni online.

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario 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 procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando 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, concedi 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 le impostazioni predefinite IAM Identity Center directory nella Guida per l'AWS IAM Identity Center utente.

Accedi come utente con accesso amministrativo

- 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 ad altri utenti

1. In IAM Identity Center, crea un set di autorizzazioni che segua la migliore pratica di applicazione delle autorizzazioni con privilegi minimi.

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center
2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

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

Approfondimenti

Per iniziare a usare FSx for ONTAP, consulta le istruzioni Guida introduttiva ad Amazon FSx for ONTAP NetApp per creare le tue risorse Amazon FSx.

Guida introduttiva ad Amazon FSx for ONTAP NetApp

Scopri come iniziare a usare Amazon FSx for NetApp ONTAP. Questo esercizio introduttivo include i seguenti passaggi.

Argomenti

Fase 1: creare un file system Amazon FSx for NetApp ONTAP

La console Amazon FSx offre due opzioni per creare un file system: un'opzione di creazione rapida e un'opzione di creazione standard. Per creare rapidamente e facilmente un file system Amazon FSx for NetApp ONTAP con la configurazione consigliata dal servizio, utilizza l'opzione Quick create.

L'opzione Quick create crea un file system con una singola coppia ad alta disponibilità (HA), una singola macchina virtuale di archiviazione (SVM) e un singolo volume. L'opzione Quick create configura questo file system per consentire l'accesso ai dati da istanze Linux tramite il protocollo Network File System (NFS). Dopo aver creato il file system, puoi creare SVM e volumi aggiuntivi secondo necessità, inclusa una SVM unita a un Active Directory per consentire l'accesso dai client Windows e macOS tramite il protocollo Server Message Block (SMB).

Per informazioni sull'utilizzo dell'opzione Standard create per creare un file system con una configurazione personalizzata e sull'utilizzo dell' AWS CLI API and, vedere. Creazione di FSx per i file system ONTAP

Per creare il file system

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di controllo, scegli Crea file system per avviare la procedura guidata di creazione del file system.
3. Nella pagina Seleziona il tipo di file system, scegli Amazon FSx for NetApp ONTAP, quindi scegli Avanti. Viene visualizzata la pagina Crea file system ONTAP.
4. Per Metodo di creazione, scegli Creazione rapida.

5. Nella sezione Configurazione rapida, per Nome del file system, facoltativo, inserisci un nome per il tuo file system. È più facile trovare e gestire i file system quando li si assegna un nome. È possibile utilizzare un massimo di 256 lettere Unicode, spazi bianchi e numeri, oltre ai seguenti caratteri speciali: + - (trattino) =. _ (trattino basso):/
6. Per il tipo di implementazione scegli Multi-AZ o Single-AZ.

   - I file system Multi-AZ replicano i dati e supportano il failover su più zone di disponibilità contemporaneamente. Regione AWS
   - I file system Single-AZ replicano i dati e offrono il failover automatico all'interno di un'unica zona di disponibilità.

   Per ulteriori informazioni, consulta Disponibilità e durabilità.
7. Per la capacità di archiviazione SSD, specifica la capacità di archiviazione del file system, in gibibyte (GiB). Immettete un numero intero compreso tra 1.024 e 196.608. Se hai bisogno di una maggiore capacità di archiviazione SSD, puoi utilizzare Standard create. Per ulteriori informazioni, consulta Per creare un file system (console).

   È possibile aumentare la capacità di archiviazione in base alle esigenze in qualsiasi momento dopo la creazione del file system. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione.
8. Per quanto riguarda la capacità di throughput, Amazon FSx fornisce automaticamente la capacità di throughput consigliata in base allo storage SSD. Puoi anche scegliere la velocità effettiva del tuo file system (fino a 4.096 MBps). Se hai bisogno di una maggiore capacità di trasmissione, puoi usare Standard create.
9. Per il Virtual Private Cloud (VPC), scegli l'Amazon VPC che desideri associare al tuo file system.
10. Per l'efficienza dello storage, scegli Abilitato per attivare le funzionalità di efficienza dello storage ONTAP (compressione, deduplicazione e compattazione) o Disabilitato per disattivarle.
11. (Solo Multi-AZ) L'intervallo di indirizzi IP dell'endpoint specifica l'intervallo di indirizzi IP in cui vengono creati gli endpoint per accedere al file system.

    Scegliete un'opzione di creazione rapida per l'intervallo di indirizzi IP dell'endpoint:

    - Intervallo di indirizzi IP non allocati dal tuo VPC: scegli questa opzione per fare in modo che Amazon FSx utilizzi gli ultimi 64 indirizzi IP dell'intervallo CIDR primario del VPC come intervallo di indirizzi IP dell'endpoint per il file system. Tieni presente che questo intervallo è condiviso tra più file system se scegli questa opzione più volte.

> **Note**
>
> - Ogni file system creato utilizza due indirizzi IP di questo intervallo, uno per il cluster e uno per la prima SVM. Anche il primo e l'ultimo indirizzo IP sono riservati. Per ogni SVM aggiuntiva, il file system utilizza un altro indirizzo IP. Ad esempio, un file system che ospita 10 SVM utilizza 11 indirizzi IP. I file system aggiuntivi funzionano allo stesso modo. Utilizzano i due indirizzi IP iniziali, più uno per ogni SVM aggiuntiva. Il numero massimo di file system che utilizzano lo stesso intervallo di indirizzi IP, ciascuno con una singola SVM, è 31.
> - Questa opzione è disattivata se uno degli ultimi 64 indirizzi IP nell'intervallo CIDR primario di un VPC è utilizzato da una sottorete.

- Intervallo di indirizzi IP flottante all'esterno del tuo VPC: scegli questa opzione per fare in modo che Amazon FSx utilizzi un intervallo di indirizzi 198.19.x.0/24 che non è già utilizzato da nessun altro file system con lo stesso VPC e le stesse tabelle di routing.

Puoi anche specificare il tuo intervallo di indirizzi IP nell'opzione Standard create.

12. Scegli Avanti e rivedi la configurazione del file system nella pagina Crea file system ONTAP. Nota quali impostazioni del file system puoi modificare dopo la creazione del file system.
13. Scegliere Create file system (Crea file system).

La creazione rapida crea un file system con un SVM (denominato`fsx`) e un volume (denominato`vol1`). Il volume ha un percorso di congiunzione `/vol1` e una politica di suddivisione in più livelli del pool di capacità di Auto (che suddividerà automaticamente tutti i dati a cui non si accede da 31 giorni in uno storage con pool di capacità a basso costo). La politica di snapshot predefinita viene assegnata al volume predefinito. I dati del file system vengono crittografati quando sono inattivi utilizzando la AWS KMS chiave gestita del servizio predefinita.

Fase 2: Montaggio del file system da un'istanza Amazon EC2 Linux

Puoi montare il tuo file system da un'istanza Amazon Elastic Compute Cloud (Amazon EC2). Questa procedura utilizza un'istanza che esegue Amazon Linux 2.

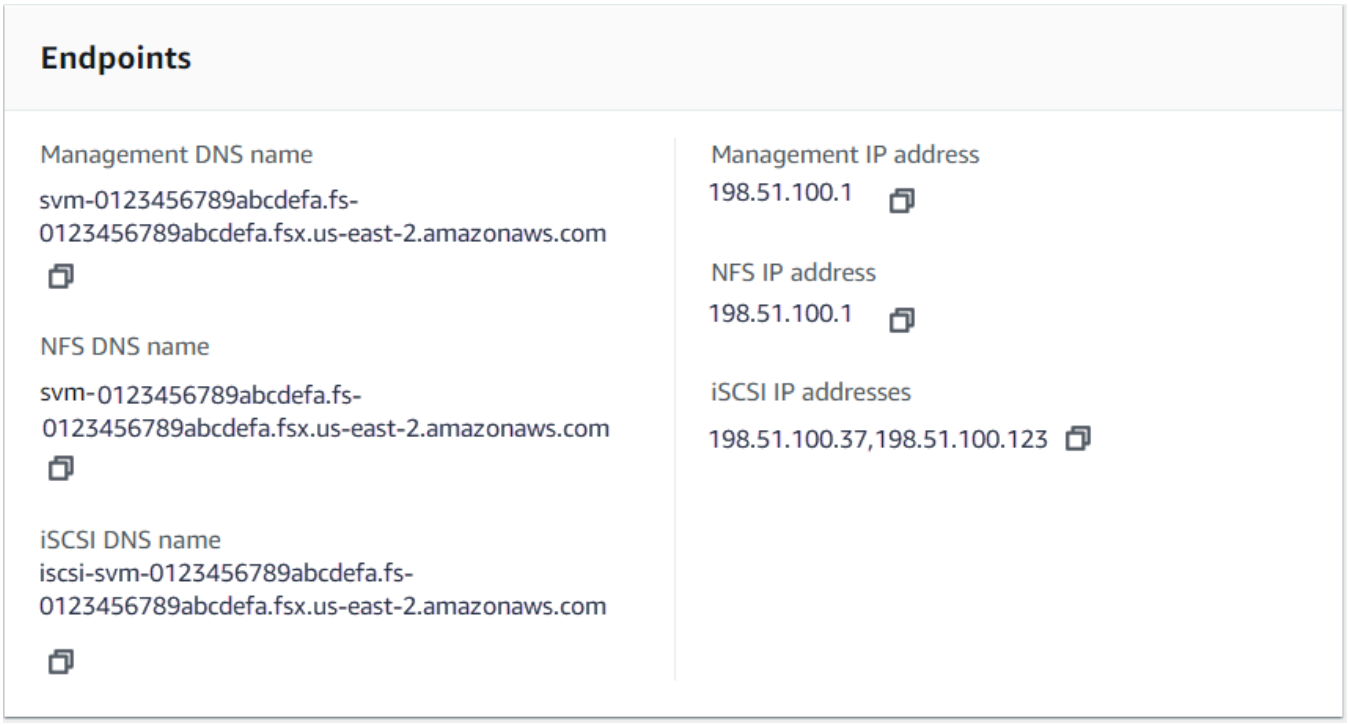
Per montare il file system da Amazon EC2

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Crea o seleziona un'istanza Amazon EC2 che esegue Amazon Linux 2 che si trova nello stesso cloud privato virtuale (VPC) del file system. Per ulteriori informazioni sul lancio di un'istanza, consulta la Fase 1: Avvio di un'istanza nella Amazon EC2 User Guide.
3. Connect alla tua istanza Amazon EC2 Linux. Per ulteriori informazioni, consulta Connect to your Linux istance nella Amazon EC2 User Guide.
4. Apri un terminale sulla tua istanza Amazon EC2 utilizzando Secure Shell (SSH) e accedi con le credenziali appropriate.
5. Crea una directory sulla tua istanza Amazon EC2 da utilizzare come punto di montaggio del volume con il seguente comando. Nell'esempio seguente, sostituisci *`mount-point`* con le tue informazioni.

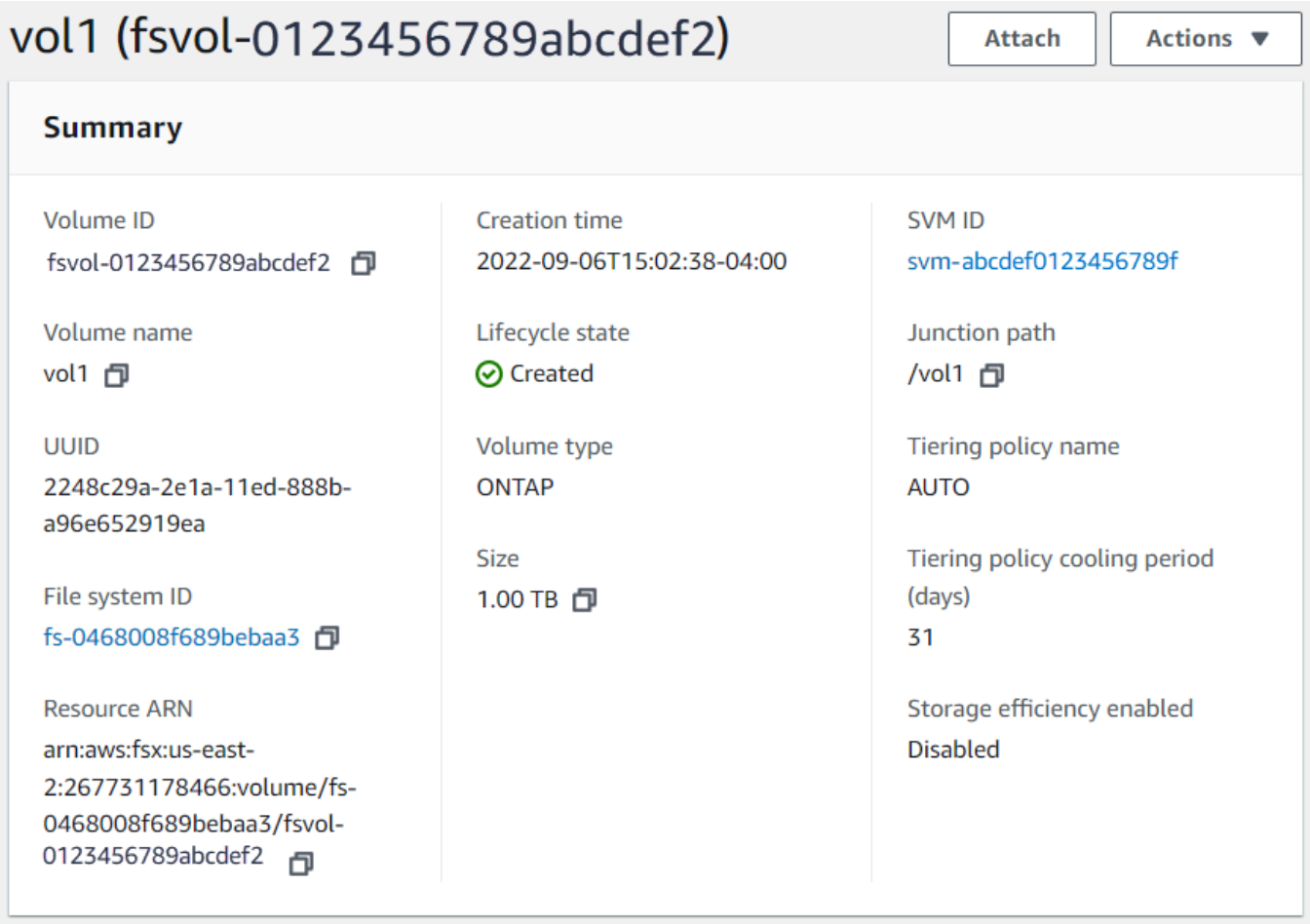
   ```
   $ sudo mkdir /mount-point
   ```

6. Installa il tuo file system Amazon FSx for NetApp ONTAP nella directory che hai creato. Usa un `mount` comando simile all'esempio che segue. Nell'esempio seguente, sostituite i seguenti valori segnaposto con le vostre informazioni.

   - *`nfs_version`*— La versione NFS in uso; FSx for ONTAP supporta le versioni 3, 4.0, 4.1 e 4.2.
   - *`nfs-dns-name`*— Il nome DNS NFS della macchina virtuale di archiviazione (SVM) in cui esiste il volume che si sta montando. Puoi trovare il nome DNS NFS nella console Amazon FSx scegliendo Storage virtual machines, quindi scegliendo la SVM su cui esiste il volume da montare. Il nome DNS NFS si trova nel pannello Endpoints, mostrato nell'immagine seguente.



- *`volume-junction-path`*— Il percorso di giunzione del volume che stai montando. Puoi trovare il percorso di giunzione di un volume nella console Amazon FSx nel pannello Riepilogo della pagina dei dettagli del volume, mostrato nell'immagine seguente.



- *mount-point*— Il nome della directory che hai creato sull'istanza EC2 per il punto di montaggio del volume.

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

Il comando seguente utilizza valori di esempio.

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

In caso di problemi con l'istanza Amazon EC2 (ad esempio il timeout delle connessioni), consulta Risoluzione dei problemi relativi alle istanze EC2 nella Amazon EC2 User Guide.

Fase 3: Eliminazione delle risorse

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

Per eliminare le risorse

1. Sulla console Amazon EC2, termina l'istanza. Per ulteriori informazioni, consulta Terminate Your Instance nella Amazon EC2 User Guide.
2. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
3. Sulla console Amazon FSx, elimina tutti i volumi FSx for ONTAP che non sono volumi root della SVM. Per ulteriori informazioni, consulta Eliminazione di un volume.
4. Elimina tutte le tue SVM FSx for ONTAP. Per ulteriori informazioni, consulta Eliminazione di una macchina virtuale di archiviazione (SVM).
5. Sulla console Amazon FSx, elimina il file system. Quando elimini un file system, tutti i backup automatici vengono eliminati automaticamente. Tuttavia, è comunque necessario eliminare tutti i backup creati manualmente. I passaggi seguenti descrivono questo processo.

    a. Dalla dashboard della console, scegliete il nome del file system creato per questo esercizio.

    b. In Azioni, seleziona Elimina file system.

    c. Nella finestra di dialogo Elimina il file system, inserite l'ID del file system che desiderate eliminare nella casella ID del file system.

    d. Scegliete Elimina file system.

    e. Sebbene Amazon FSx elimini il file system, il suo stato nella dashboard cambia in ELIMINAZIONE. Una volta eliminato, il file system non viene più visualizzato nella dashboard. Tutti i backup automatici vengono eliminati insieme al file system.

    f. Ora puoi eliminare qualsiasi backup creato manualmente per il tuo file system. Dalla barra di navigazione a sinistra, scegli Backup.

    g. Dalla dashboard, scegli tutti i backup con lo stesso ID di file system del file system che hai eliminato e scegli Elimina backup. Assicurati di conservare il backup finale, se ne hai creato uno.

    h. Viene visualizzata la finestra di dialogo Elimina backup. Mantieni selezionata la casella di controllo per gli ID dei backup che desideri eliminare, quindi scegli Elimina backup.

Il tuo file system Amazon FSx e tutti i relativi backup automatici vengono ora eliminati, insieme a tutti i backup manuali che hai scelto di eliminare.

Accesso ai dati

Puoi accedere ai tuoi file system Amazon FSx utilizzando una varietà di client e metodi supportati sia in ambiente locale che locale. Cloud AWS

Ogni SVM dispone di quattro endpoint utilizzati per accedere ai dati o per gestire l'SVM utilizzando l'ONTAP NetApp CLI o l'API REST:

- `Nfs`— Per la connessione tramite il protocollo Network File System (NFS)
- `Smb`— Per la connessione tramite il protocollo Service Message Block (SMB) (se la SVM fa parte di un Active Directory o utilizzi un gruppo di lavoro).
- `Iscsi`— Per la connessione tramite il protocollo Internet Small Computer Systems Interface (iSCSI) (solo per file system scalabili).
- `Management`— Per gestire le SVM utilizzando la NetApp CLI o l'API ONTAP o BlueXP NetApp

Argomenti

Client supportati

I file system FSx for ONTAP supportano l'accesso ai dati da un'ampia varietà di istanze di calcolo e sistemi operativi. A tale scopo supporta l'accesso tramite il protocollo Network File System (NFS) (v3, v4.0, v4.1 e v4.2), tutte le versioni del protocollo Server Message Block (SMB) (incluse 2.0, 3.0 e 3.1.1) e il protocollo Internet Small Computer Systems Interface (iSCSI).

> **Important**
>
> Amazon FSx non supporta l'accesso ai file system dalla rete Internet pubblica. Amazon FSx scollega 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.

Le seguenti istanze di AWS calcolo sono supportate per l'uso con FSx for ONTAP:

- Istanze Amazon Elastic Compute Cloud (Amazon EC2) che eseguono Linux con supporto NFS o SMB, Microsoft Windows e macOS. Per ulteriori informazioni, consulta Volumi di montaggio.
- Contenitori Docker Amazon Elastic Container Service (Amazon ECS) su istanze Amazon EC2 Windows e Linux. Per ulteriori informazioni, consulta Utilizzo di Amazon Elastic Container Service con FSx per ONTAP.
- Amazon Elastic Kubernetes Service — Per ulteriori informazioni, consulta il driver CSI Amazon FSx for NetApp ONTAP nella Guida per l'utente di Amazon EKS.
- Red Hat OpenShift Service on AWS (ROSA): per ulteriori informazioni, consulta What is Red Hat Service on? OpenShift AWS nella Red Hat OpenShift Service on AWS User Guide.
- WorkSpaces Istanze Amazon. Per ulteriori informazioni, consulta Utilizzo di Amazon WorkSpaces con FSx for ONTAP.
- Istanze Amazon AppStream 2.0.
- AWS Lambda — Per ulteriori informazioni, consulta il post del AWS blog Enabling SMB access for server-less workload with Amazon FSx.
- Macchine virtuali (VM) in esecuzione in VMware Cloud su ambienti. AWS Per ulteriori informazioni, consulta Configurare Amazon FSx for NetApp ONTAP come storage esterno e VMware Cloud on with AWS Amazon FSx for ONTAP Deployment Guide. NetApp

Una volta montati, i file system FSx for ONTAP vengono visualizzati come una directory locale o una lettera di unità su NFS e SMB, fornendo uno storage di file di rete condiviso e completamente gestito a cui possono accedere simultaneamente fino a migliaia di client. I LUN iSCSI sono accessibili come dispositivi a blocchi se montati su iSCSI.

Accesso ai dati dall'interno AWS

Ogni file system Amazon FSx è associato a un Virtual Private Cloud (VPC). È possibile accedere al file system FSx for ONTAP da qualsiasi punto del VPC del file system, indipendentemente dalla zona di disponibilità. È inoltre possibile accedere al file system da altri VPC che possono trovarsi in account diversi o. AWS Regioni AWS Oltre ai requisiti descritti nelle seguenti sezioni per l'accesso alle risorse FSx for ONTAP, è necessario assicurarsi che il gruppo di sicurezza VPC del file system sia configurato in modo che il traffico di dati e di gestione possa fluire tra il file system e i client. Per ulteriori informazioni sulla configurazione dei gruppi di sicurezza con le porte richieste, vedere. Gruppi di sicurezza Amazon VPC

Argomenti

Accesso ai dati dall'interno dello stesso VPC

Quando crei il tuo file system Amazon FSx for NetApp ONTAP, selezioni l'Amazon VPC in cui si trova. Tutte le SVM e i volumi associati al file system Amazon FSx NetApp for ONTAP si trovano anche nello stesso VPC. Quando si monta un volume, se il file system e il client che monta il volume si trovano nello stesso VPC e Account AWS, è possibile utilizzare il nome DNS e la giunzione di volume o la condivisione SMB di SVM, a seconda del client. Per ulteriori informazioni, consulta Volumi di montaggio.

È possibile ottenere prestazioni ottimali se il client e il volume si trovano nella stessa zona di disponibilità della sottorete del file system o nella sottorete preferita per i file system Multi-AZ. Per identificare la sottorete o la sottorete preferita di un file system, nella console Amazon FSx, scegli File system, quindi scegli il file system ONTAP di cui stai montando il volume e la sottorete o la sottorete preferita (Multi-AZ) viene visualizzata nel pannello Subnet o Preferred subnet.

Accesso ai dati dall'esterno del VPC di implementazione

Questa sezione descrive come accedere agli endpoint di un file system FSx for ONTAP da AWS posizioni esterne al VPC di implementazione del file system.

Accesso agli endpoint di gestione NFS, SMB e ONTAP su file system Multi-AZ

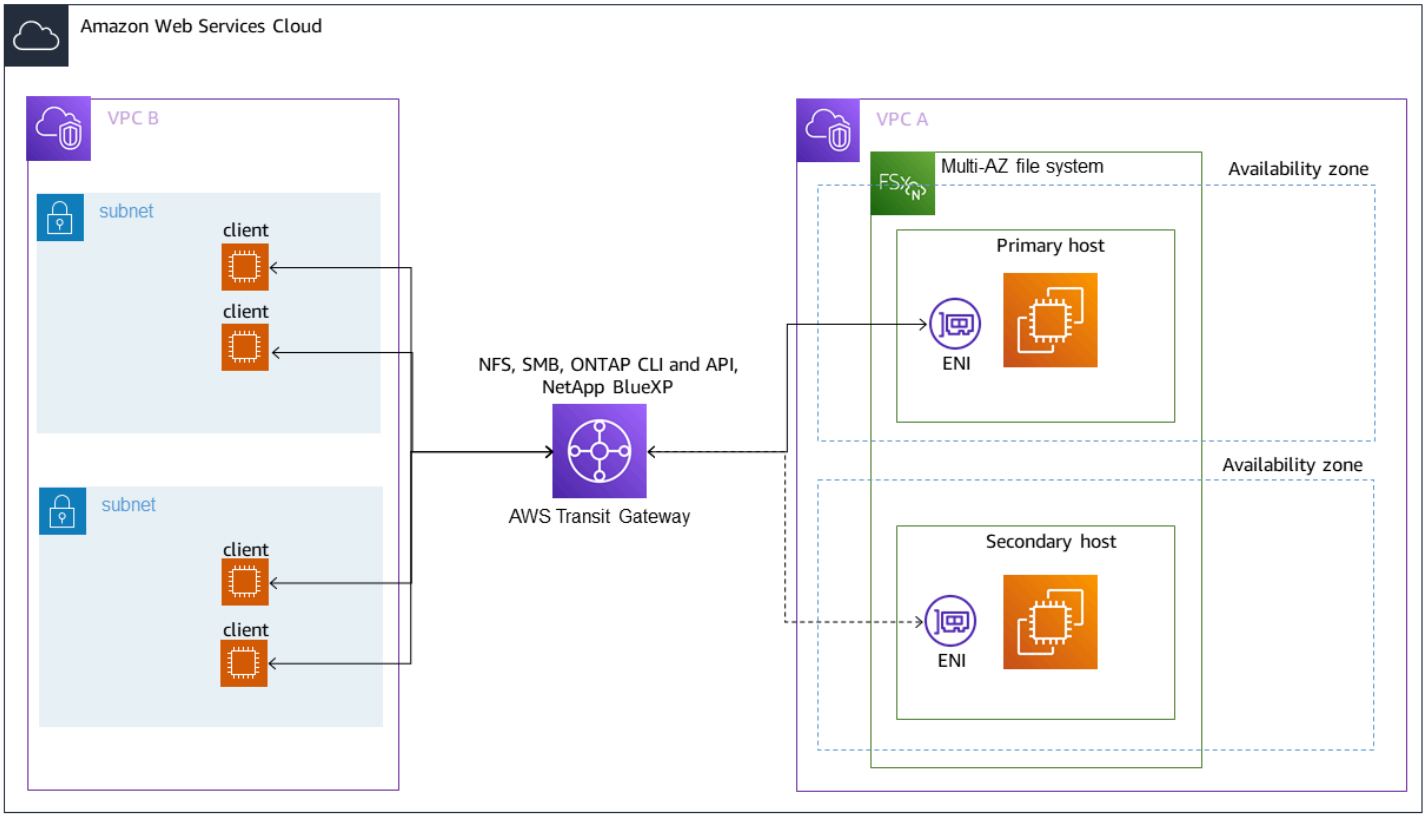
Gli endpoint di gestione NFS, SMB e ONTAP sui file system Amazon FSx NetApp for ONTAP Multi-AZ utilizzano indirizzi IP (Internet Protocol) mobili in modo che i client connessi passino senza problemi dal file server preferito a quello di standby durante un evento di failover. Per ulteriori informazioni sui failover, consulta Processo di failover per FSx for ONTAP.

Questi indirizzi IP mobili vengono creati nelle tabelle di routing VPC associate al file system e si trovano all'interno dei file system che `EndpointIpAddressRange` è possibile specificare durante la creazione. `EndpointIpAddressRange`Utilizza i seguenti intervalli di indirizzi, a seconda di come viene creato un file system:

- Per impostazione predefinita, i file system Multi-AZ creati utilizzando la console Amazon FSx utilizzano gli ultimi 64 indirizzi IP dell'intervallo CIDR primario del VPC per il file system. `EndpointIpAddressRange`
- Per impostazione predefinita, i file system Multi-AZ creati utilizzando l'API AWS CLI o Amazon FSx utilizzano un intervallo di indirizzi IP `198.19.0.0/16` all'interno del blocco di `EndpointIpAddressRange` indirizzi.

AWS Transit GatewaySupporta solo il routing verso indirizzi IP mobili, noto anche come peering transitivo. Peering VPC e AWS VPN non supportano AWS Direct Connect il peering transitivo. Pertanto, è necessario utilizzare Transit Gateway per accedere a queste interfacce da reti esterne al VPC del file system.

Il diagramma seguente illustra l'utilizzo di Transit Gateway for NFS, SMB o l'accesso di gestione a un file system Multi-AZ che si trova in un VPC diverso rispetto ai client che vi accedono.



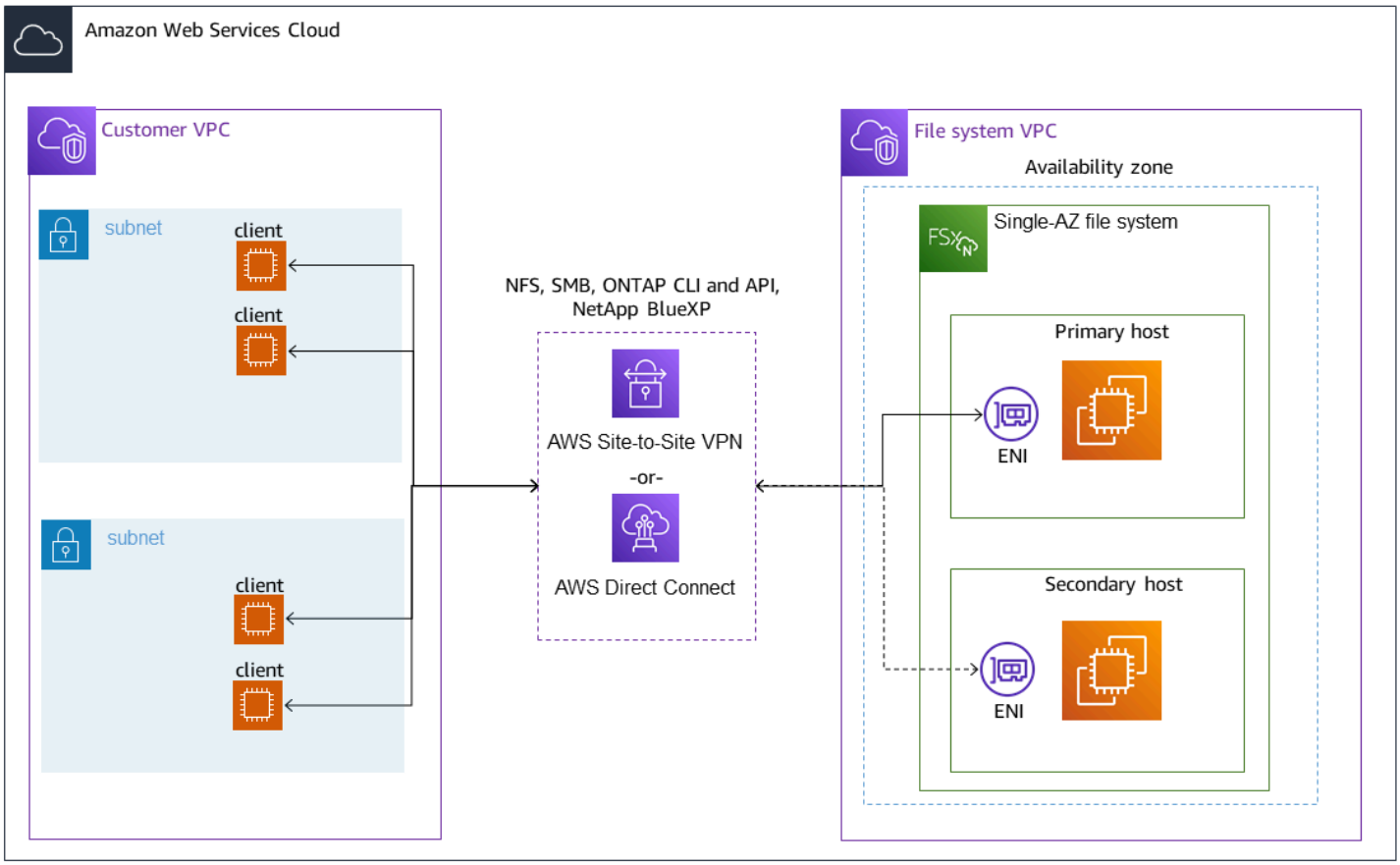
> **Note**
>
> Assicurati che tutte le tabelle di routing che stai utilizzando siano associate al tuo file system Multi-AZ. In questo modo è possibile prevenire l'indisponibilità durante un failover. Per informazioni sull'associazione delle tabelle di routing Amazon VPC al file system, consulta. Aggiornamento di un file system

Per informazioni su quando è necessario utilizzare Transit Gateway per accedere al file system FSx for ONTAP, vedere. Quando è richiesto il Transit Gateway?

Accesso a NFS, SMB o alla CLI e API ONTAP per file system Single-AZ

Gli endpoint utilizzati per accedere ai file system FSx for ONTAP Single-AZ tramite NFS o SMB e per amministrare i file system utilizzando l'ONTAP CLI o l'API REST sono indirizzi IP secondari sull'ENI del file server attivo. Gli indirizzi IP secondari rientrano nell'intervallo CIDR del VPC, quindi i client possono accedere ai dati e alle porte di gestione utilizzando il peering VPC o senza richiedere. AWS Direct Connect AWS VPN AWS Transit Gateway

Il diagramma seguente illustra l'utilizzo AWS VPN o AWS Direct Connect per l'accesso NFS, SMB o di gestione a un file system Single-AZ che si trova in un VPC diverso da quello dei client che vi accedono.



Quando è richiesto il Transit Gateway?

La necessità o meno del Transit Gateway per i file system Multi-AZ dipende dal metodo utilizzato per accedere ai dati del file system. I file system Single-AZ non richiedono Transit Gateway. La tabella seguente descrive quando sarà necessario utilizzare per accedere AWS Transit Gateway ai file system Multi-AZ.

Accesso ai dati	Richiede Transit Gateway?
Accesso a FSX tramite NFS, SMB o l'API NetApp REST ONTAP, CLI o BlueXP	Solo se: • Accesso da una rete peer-to-peer (ad esempio locale) e

Accesso ai dati	Richiede Transit Gateway?
	• Non si accede a FSx tramite un'istanza NetApp FlexCache o Global File Cache
Accesso ai dati tramite iSCSI	No
Unire un SVM a un Active Directory	No
SnapMirror	No
FlexCache Memorizzazione nella cache	No
Cache globale dei file	No

Configurazione del routing utilizzando AWS Transit Gateway

Se disponi di un file system Multi-AZ con un file system `EndpointIPAddressRange` che non rientra nell'intervallo CIDR del tuo VPC, devi configurare un routing aggiuntivo per accedere AWS Transit Gateway al file system da reti peer o locali.

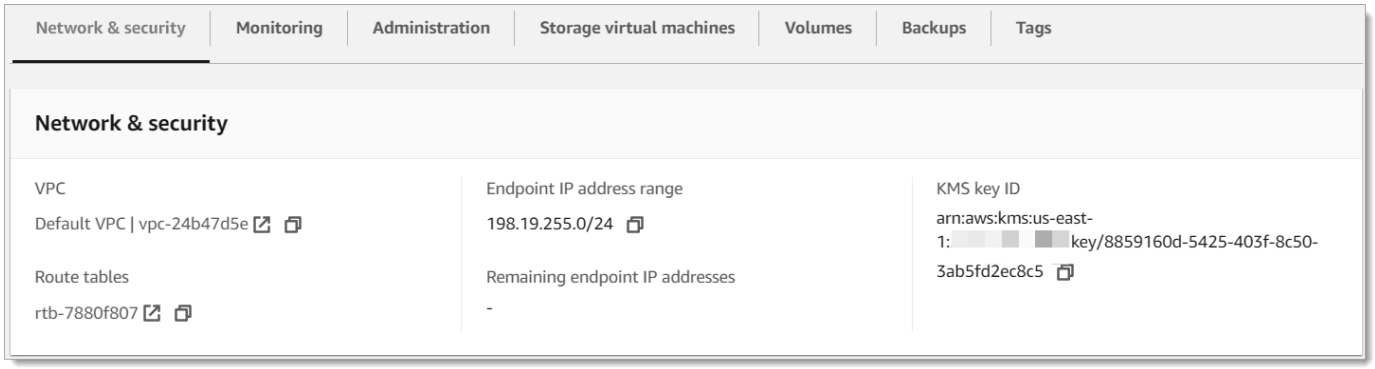
> **Important**
>
> Per accedere a un file system Multi-AZ utilizzando un Transit Gateway, ciascuno degli allegati del Transit Gateway deve essere creato in una sottorete la cui tabella di routing è associata al file system.

> **Note**
>
> Non è richiesta alcuna configurazione Transit Gateway aggiuntiva per i file system Single-AZ o Multi-AZ con un indirizzo `EndpointIPAddressRange` che rientri nell'intervallo di indirizzi IP del tuo VPC.

Per configurare il routing utilizzando AWS Transit Gateway

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegliete il file system FSx for ONTAP per il quale state configurando l'accesso da una rete peer.

3. In Rete e sicurezza, copiate l'intervallo di indirizzi IP dell'endpoint.



4. Aggiungi un percorso al Transit Gateway che indirizza il traffico destinato a questo intervallo di indirizzi IP al VPC del file system. Per ulteriori informazioni, consulta Lavorare con i gateway di transito nei gateway di transito Amazon VPC.
5. Conferma di poter accedere al file system FSx for ONTAP dalla rete peer.

Per aggiungere la tabella delle rotte al file system, vedere. Aggiornamento di un file system

> **Note**
>
> I record DNS per gli endpoint di gestione, NFS e SMB sono risolvibili solo all'interno dello stesso VPC del file system. Per montare un volume o connettersi a una porta di gestione da un'altra rete, è necessario utilizzare l'indirizzo IP dell'endpoint. Questi indirizzi IP non cambiano nel tempo.

Accesso agli endpoint iSCSI o intercluster all'esterno del VPC di installazione

È possibile utilizzare il peering VPC o accedere AWS Transit Gateway agli endpoint iSCSI o intercluster del file system dall'esterno del VPC di implementazione del file system. È possibile utilizzare VPC Peering per instradare il traffico iSCSI e intercluster tra VPC. Una connessione peering VPC è una connessione di rete tra due VPC e viene utilizzata per instradare il traffico tra di loro utilizzando indirizzi IPv4 privati. Puoi utilizzare il peering VPC per connettere VPC all'interno dello stesso Regione AWS o tra diversi. Regioni AWS Per ulteriori informazioni sul peering VPC, consulta Cos'è il peering VPC? nella Amazon VPC Peering Guide.

Accesso ai dati dall'ambiente locale

È possibile accedere ai file system FSx for ONTAP da locale utilizzando AWS VPNe AWS Direct Connect; linee guida più specifiche sui casi d'uso sono disponibili nelle sezioni seguenti. Oltre ai requisiti elencati di seguito per accedere a diverse risorse FSx for ONTAP dall'ambiente locale, devi anche assicurarti che il gruppo di sicurezza VPC del tuo file system consenta il flusso di dati tra il file system e i client; per un elenco delle porte richieste, consulta i gruppi di sicurezza Amazon VPC.

Accesso agli endpoint NFS, SMB o ONTAP CLI o REST API da locale

Questa sezione descrive come accedere alle porte di gestione NFS, SMB e ONTAP sui file system FSx for ONTAP dalle reti locali.

Accesso ai file system Multi-AZ

Amazon FSx richiede l'utilizzo AWS Transit Gateway o la configurazione di NetApp Global File Cache NetApp FlexCache remota o l'accesso ai file system Multi-AZ da una rete locale. Per supportare il failover tra AZ per file system Multi-AZ, Amazon FSx utilizza indirizzi IP mobili per le interfacce utilizzate per gli endpoint di gestione NFS, SMB e ONTAP. Poiché gli endpoint NFS, SMB e di gestione utilizzano IP mobili, è necessario utilizzarle insieme o per accedere a queste interfacce da una rete locale. AWS Transit Gateway AWS Direct Connect AWS VPN Gli indirizzi IP mobili utilizzati per queste interfacce rientrano nei limiti specificati durante la creazione del `EndpointIpAddressRange` file system Multi-AZ. Se crei il tuo file system dalla console Amazon FSx, per impostazione predefinita Amazon FSx sceglie gli ultimi 64 indirizzi IP dall'intervallo CIDR primario del VPC da utilizzare come intervallo di indirizzi IP dell'endpoint per il file system. Se crei il tuo file system da AWS CLI o dall'API Amazon FSx, per impostazione predefinita Amazon FSx sceglie un intervallo di indirizzi IP all'interno dell'intervallo di indirizzi IP. `198.19.0.0/16` Gli indirizzi IP mobili vengono utilizzati per consentire una transizione senza interruzioni dei client al file system di standby nel caso in cui sia necessario un failover. Per ulteriori informazioni, consulta Processo di failover per FSx for ONTAP.

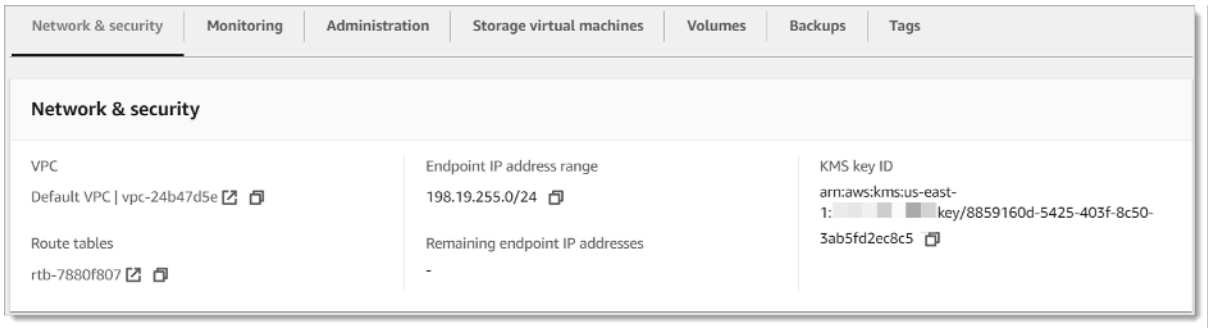
> **Important**
>
> Per accedere a un file system Multi-AZ utilizzando un Transit Gateway, ciascuno degli allegati del Transit Gateway deve essere creato in una sottorete la cui tabella di routing è associata al file system.

AWS Transit Gateway Per configurare l'accesso dall'esterno del tuo VPC

Se disponi di un file system Multi-AZ con un file system `EndpointIPAddressRange` che non rientra nell'intervallo CIDR del tuo VPC, devi configurare un routing aggiuntivo AWS Transit Gateway per accedere al file system da reti peer o locali.

> **Note**
>
> Non è richiesta alcuna configurazione Transit Gateway aggiuntiva per i file system Single-AZ o Multi-AZ con un indirizzo `EndpointIPAddressRange` che rientri nell'intervallo di indirizzi IP del tuo VPC.

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegliete il file system FSx for ONTAP per il quale state configurando l'accesso da una rete peer.
3. In Rete e sicurezza, copiate l'intervallo di indirizzi IP dell'endpoint.



4. Aggiungi un percorso al Transit Gateway che indirizza il traffico destinato a questo intervallo di indirizzi IP al VPC del file system. Per ulteriori informazioni, consulta Lavora con i gateway di transito nella Guida per l'utente di Amazon VPC Transit Gateway.
5. Conferma di poter accedere al file system FSx for ONTAP dalla rete peer.

> **Important**
>
> Per accedere a un file system Multi-AZ utilizzando un Transit Gateway, ciascuno degli allegati del Transit Gateway deve essere creato in una sottorete la cui tabella di routing è associata al file system.

Per aggiungere una tabella di routing al file system, vedere. Aggiornamento di un file system

Accesso ai file system Single-AZ

Il requisito da utilizzare AWS Transit Gateway per accedere ai dati da una rete locale non esiste per i file system Single-AZ. I file system Single-AZ vengono distribuiti in un'unica sottorete e non è necessario un indirizzo IP mobile per fornire il failover tra i nodi. Invece, gli indirizzi IP a cui accedi sui file system Single-AZ sono implementati come indirizzi IP secondari all'interno dell'intervallo VPC CIDR del file system, consentendoti di accedere ai tuoi dati da un'altra rete senza richiedere. AWS Transit Gateway

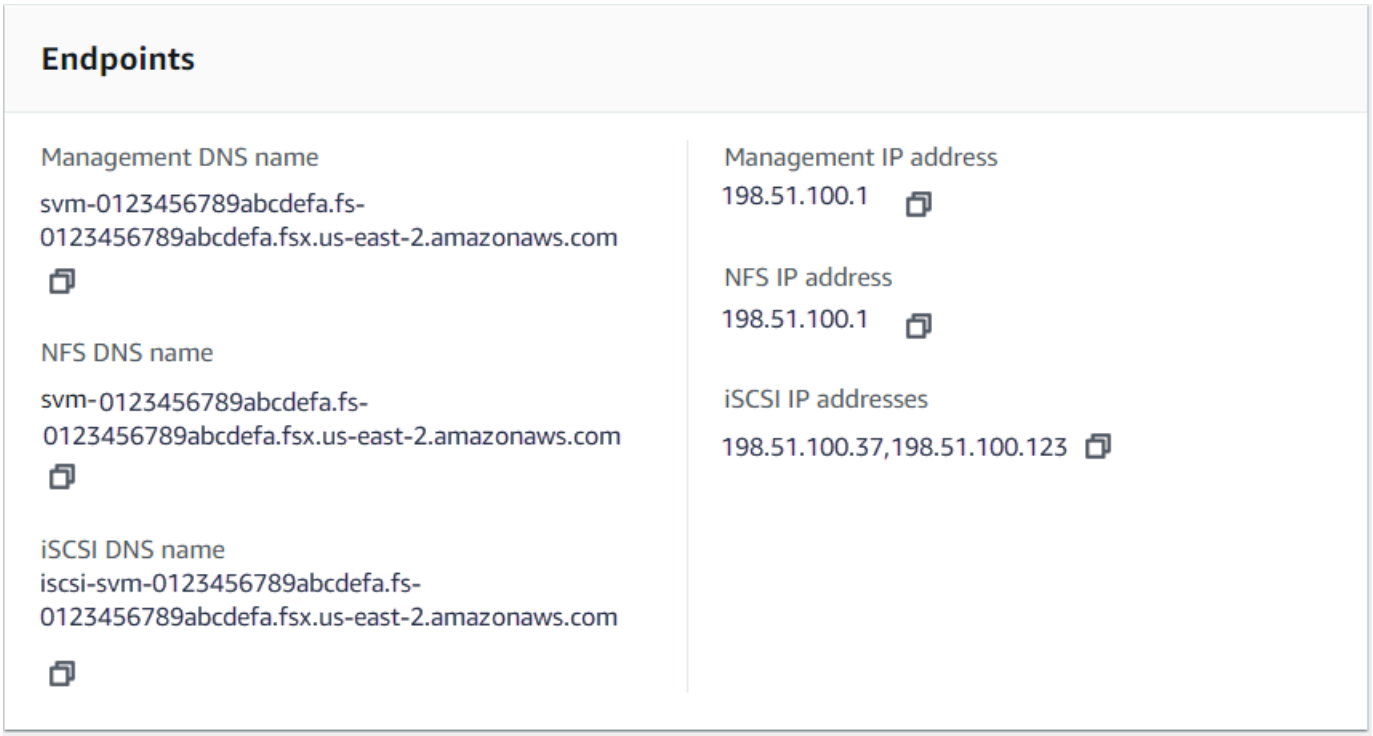
Accesso agli endpoint intercluster dall'ambiente locale

Gli endpoint intercluster di FSx for ONTAP sono dedicati al traffico di replica tra i file system ONTAP, incluse le implementazioni locali e FSx for NetApp ONTAP. NetApp Il traffico di replica include SnapMirror e FlexClone le relazioni tra le macchine virtuali di storage (SVM) e i volumi tra diversi file system e Global File Cache. FlexCache NetApp Gli endpoint intercluster vengono utilizzati anche per il traffico di Active Directory.

Poiché gli endpoint intercluster di un file system utilizzano indirizzi IP che rientrano nell'intervallo CIDR del VPC fornito quando crei il file system FSx for ONTAP, non è necessario utilizzare un Transit Gateway per il routing del traffico intercluster tra locali e. Cloud AWS Tuttavia, i client locali devono comunque utilizzare AWS VPN o AWS Direct Connect stabilire una connessione sicura al tuo VPC.

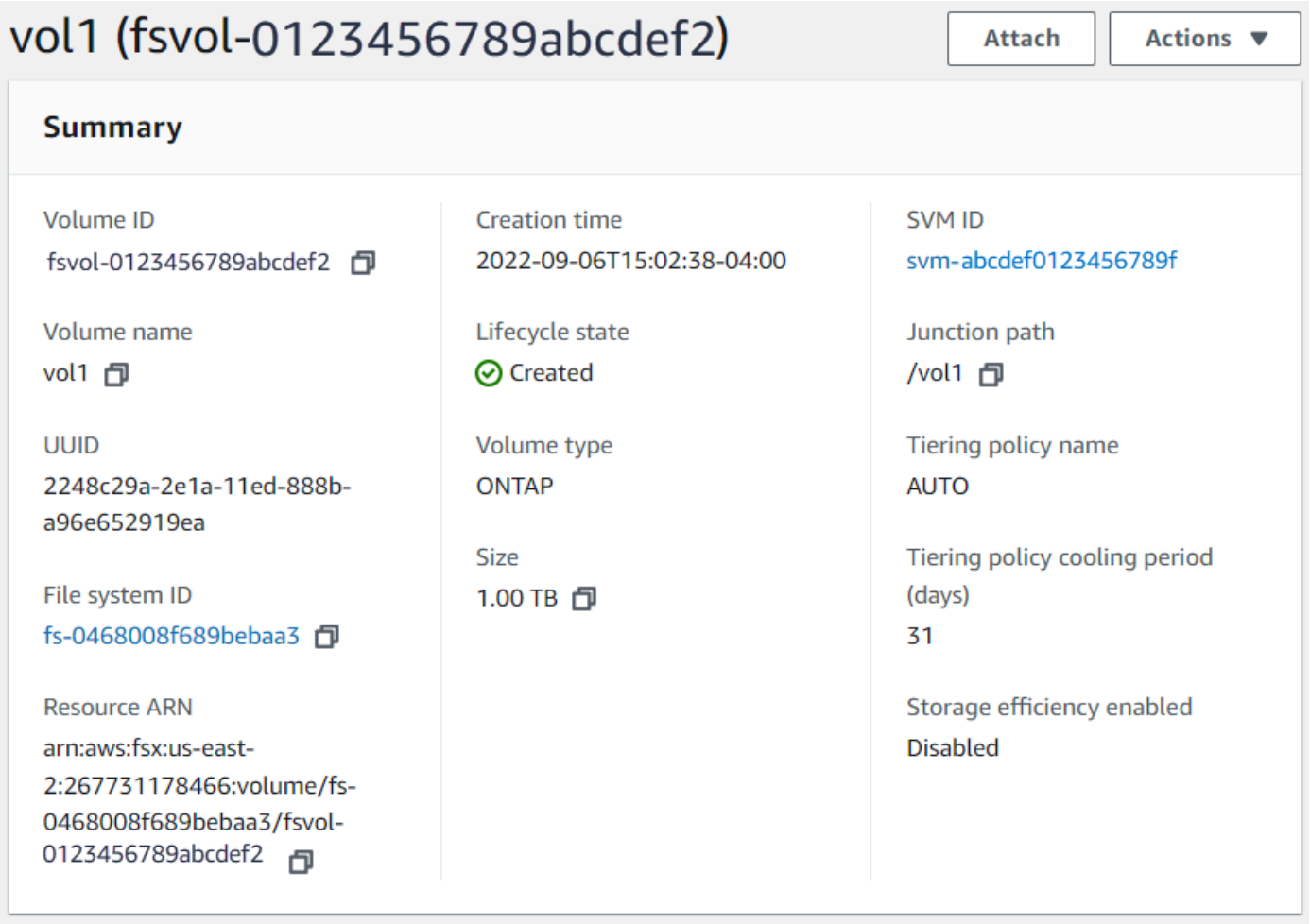
Volumi di montaggio

È possibile accedere ai dati in FSx for ONTAP montando un volume sul client. I comandi di questa sezione utilizzano il nome DNS o l'indirizzo IP dell'SVM in cui viene creato il volume per montare o collegare un volume. Puoi trovare il nome DNS e l'indirizzo IP di SVM nella console Amazon FSx scegliendo ONTAP **>** Storage virtual machines o nella scheda Storage virtual machine nella pagina dei dettagli del file system per il file system, mostrata nell'immagine seguente.



Oppure, puoi trovarli nella risposta dell'operazione API. DescribeStorageVirtualMachines

Puoi trovare il percorso di giunzione di un volume nella console Amazon FSx nel pannello Riepilogo della pagina dei dettagli del volume, mostrato nell'immagine seguente.



Argomenti

- Montaggio su client Linux
- Montaggio su client Microsoft Windows
- Montaggio su client macOS

Montaggio su client Linux

Si consiglia che i volumi SVM a cui si collegano i client Linux abbiano un'impostazione di stile di `UNIX` sicurezza pari a o. `mixed` Per ulteriori informazioni, consulta Gestione dei volumi FSx for ONTAP.

> **Note**
>
> Per impostazione predefinita, i mount FSx for ONTAP NFS sono mount. `hard` Per garantire un failover regolare nel caso in cui si verifichi uno, si consiglia di utilizzare l'opzione di montaggio predefinita. `hard`

Per montare un volume ONTAP su un client Linux

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Crea o seleziona un'istanza Amazon EC2 che esegue Amazon Linux 2 che si trova nello stesso VPC del file system.

   Per ulteriori informazioni sul lancio di un'istanza EC2 Linux, consulta Step 1: Launch an instance nella Amazon EC2 User Guide.
3. Connect alla tua istanza Amazon EC2 Linux. Per ulteriori informazioni, consulta Connect to your Linux istance nella Amazon EC2 User Guide.
4. Apri un terminale sulla tua istanza EC2 utilizzando Secure Shell (SSH) e accedi con le credenziali appropriate.
5. Crea una directory sull'istanza EC2 per montare il volume SVM come segue:

   ```
   sudo mkdir /fsx
   ```
6. Monta il volume nella directory appena creata usando il seguente comando:

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   L'esempio seguente utilizza valori di esempio.

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   È inoltre possibile utilizzare l'indirizzo IP SVM della SVM anziché il relativo nome DNS. Consigliamo di utilizzare il nome DNS per montare i client su file system con scalabilità orizzontale, perché aiuta a garantire che i client siano bilanciati tra le coppie ad alta disponibilità (HA) del file system.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

> **Note**
>
> Per i file system scale-out, il protocollo parallel NFS (pNFS) è abilitato per impostazione predefinita e viene utilizzato per impostazione predefinita per tutti i client che montano volumi con NFS v4.1 o versione successiva.

Utilizzo di /etc/fstab per il montaggio automatico al riavvio dell'istanza

Per rimontare automaticamente il volume FSx for ONTAP al riavvio di un'istanza Amazon EC2 Linux, usa il file. `/etc/fstab` Il file `/etc/fstab` contiene informazioni sui file system. Il comando`mount -a`, che viene eseguito durante l'avvio dell'istanza, monta i file system elencati in. `/etc/fstab`

> **Note**
>
> I file system FSx for ONTAP non supportano il montaggio automatico su istanze Mac di Amazon `/etc/fstab` EC2.

> **Note**
>
> Prima di poter aggiornare il `/etc/fstab` file della tua istanza EC2, assicurati di aver già creato il file system FSx for ONTAP. Per ulteriori informazioni, consulta Creazione di FSx per i file system ONTAP.

Per aggiornare il file /etc/fstab nell'istanza EC2

1. Connettiti all'istanza EC2:
   - Per connettersi all'istanza da un computer che esegue macOS o Linux, specificare il file .pem per il comando SSH. Per fare ciò, utilizzare l'opzione `-i` e il percorso della chiave privata.
   - Per connetterti alla tua istanza da un computer che esegue Windows, puoi utilizzare MindTerm o PuTTY. Per utilizzare PuTTY, installarlo e convertire il file .pem in un file .ppk.

Per ulteriori informazioni, consulta i seguenti argomenti nella Guida per l'utente di Amazon EC2:

- Connessione all'istanza Linux tramite SSH
- Connessione all'istanza Linux da Windows tramite PuTTY

2. Crea una directory locale che verrà utilizzata per montare il volume SVM.

```
sudo mkdir /fsx
```

3. Apri il `/etc/fstab` file in un editor a tua scelta.
4. Aggiungere la seguente riga al file `/etc/fstab`. Inserite un carattere di tabulazione tra ogni parametro. Dovrebbe apparire come una riga senza interruzioni di riga.

```
svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
```

È inoltre possibile utilizzare l'indirizzo IP della SVM del volume. Gli ultimi tre parametri indicano le opzioni NFS (che abbiamo impostato come predefinite), il dumping del file system e il controllo del filesystem (in genere non vengono utilizzati, quindi li impostiamo su 0).

5. Salvare le modifiche apportate al file.
6. Ora monta la condivisione di file usando il seguente comando. Al successivo avvio del sistema, la cartella verrà montata automaticamente.

```
sudo mount /fsx
sudo mount svm-dns-name:volume-junction-path
```

L'istanza EC2 è ora configurata per montare il volume ONTAP ogni volta che viene riavviato.

Montaggio su client Microsoft Windows

Questa sezione descrive come accedere ai dati nel file system FSx for ONTAP con client che eseguono il sistema operativo Microsoft Windows. Esamina i seguenti requisiti, indipendentemente dal tipo di client che stai utilizzando.

Questa procedura presuppone che il client e il file system si trovino nello stesso Account AWS VPC e. Se il client si trova in locale o in un altro VPC, oppure Account AWS Regione AWS, questa procedura presuppone anche che sia stata configurata una connessione di rete dedicata AWS Transit

Gateway o che utilizzi AWS Direct Connect un tunnel privato e sicuro. AWS Virtual Private Network Per ulteriori informazioni, consulta Accesso ai dati dall'esterno del VPC di implementazione.

Ti consigliamo di collegare volumi ai tuoi client Windows utilizzando il protocollo SMB.

Prerequisiti

Per accedere a un volume di archiviazione ONTAP utilizzando un client Microsoft Windows, è necessario soddisfare i seguenti prerequisiti:

- L'SVM del volume da allegare deve essere aggiunto all'Active Directory dell'organizzazione oppure è necessario utilizzare un gruppo di lavoro. Per ulteriori informazioni su come aggiungere la SVM a un Active Directory, consulta. Gestione delle macchine virtuali di storage FSx for ONTAP Per ulteriori informazioni sull'uso dei gruppi di lavoro, consulta Configurare un server SMB in una panoramica dei gruppi di lavoro nel Documentation Center. NetApp
- Il volume che stai collegando ha un'impostazione di stile di sicurezza pari a o. `NTFS` `mixed` Per ulteriori informazioni, consulta Gestione dei volumi FSx for ONTAP.

Per collegare un volume ONTAP su un client Windows utilizzando SMB e Active Directory

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Crea o seleziona un'istanza Amazon EC2 che esegue Microsoft Windows che si trova nello stesso VPC del file system e unita alla stessa Microsoft Active Directory come SVM del volume.

   Per ulteriori informazioni sull'avvio di un'istanza, consulta la Fase 1: Avvio di un'istanza nella Amazon EC2 User Guide.

   Per ulteriori informazioni sull'aggiunta di una SVM a un'Active Directory, consulta. Gestione delle macchine virtuali di storage FSx for ONTAP
3. Connect alla tua istanza Amazon EC2 per Windows. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
4. Apri un prompt dei comandi.
5. Esegui il comando seguente. Sostituisci quanto segue:

   - `Z:` Sostituiscila con qualsiasi lettera di unità disponibile.
   - Sostituire `DNS_NAME` con il nome DNS o l'indirizzo IP dell'endpoint SMB per la SVM del volume.

- Sostituire `SHARE_NAME` con il nome di una condivisione SMB. `C$`è la condivisione SMB predefinita nella radice dello spazio dei nomi di SVM, ma non è consigliabile installarla in quanto espone lo storage al volume root e può causare interruzioni della sicurezza e del servizio. È necessario fornire un nome di condivisione SMB da montare anziché. `C$` Per ulteriori informazioni sulla creazione di condivisioni SMB, vedere. Gestione delle condivisioni SMB

```
net use Z: \\DNS_NAME\SHARE_NAME
```

L'esempio seguente utilizza valori di esempio.

```
net use Z: \\corp.example.com\group_share
```

È inoltre possibile utilizzare l'indirizzo IP della SVM anziché il relativo nome DNS. Consigliamo di utilizzare il nome DNS per montare i client su file system con scalabilità orizzontale, perché aiuta a garantire che i client siano bilanciati tra le coppie ad alta disponibilità (HA) del file system.

```
net use Z: \\198.51.100.5\group_share
```

Montaggio su client macOS

Questa sezione descrive come accedere ai dati nel file system FSx for ONTAP con client che eseguono il sistema operativo macOS. Esamina i seguenti requisiti, indipendentemente dal tipo di client che stai utilizzando.

Questa procedura presuppone che il client e il file system si trovino nello stesso Account AWS VPC e. Se il client si trova in sede o in un altro VPC Regione AWS, Account AWS oppure hai configurato una connessione di rete dedicata utilizzando AWS Transit Gateway AWS Direct Connect o utilizzando un tunnel privato e sicuro. AWS Virtual Private Network Per ulteriori informazioni, consulta Accesso ai dati dall'esterno del VPC di implementazione.

Ti consigliamo di collegare volumi ai tuoi client Mac utilizzando il protocollo SMB.

Per montare un volume ONTAP su un client macOS utilizzando SMB

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Crea o seleziona un'istanza Amazon EC2 per Mac che esegue macOS che si trova nello stesso VPC del file system.

   Per ulteriori informazioni sull'avvio di un'istanza, consulta la Fase 1: Avvio di un'istanza nella Amazon EC2 User Guide.

3. Connect alla tua istanza Amazon EC2 per Mac. Per ulteriori informazioni, consulta Connect to your Linux istance nella Amazon EC2 User Guide.

4. Apri un terminale sulla tua istanza EC2 utilizzando Secure Shell (SSH) e accedi con le credenziali appropriate.

5. Crea una directory sull'istanza EC2 per montare il volume come segue:

   ```
   sudo mkdir /fsx
   ```

6. Monta il volume usando il seguente comando.

   ```
   sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
   ```

   L'esempio seguente utilizza valori di esempio.

   ```
   sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-
   east-1.amazonaws.com:/C$ /fsx
   ```

   È inoltre possibile utilizzare l'indirizzo IP dell'SVM anziché il relativo nome DNS. Consigliamo di utilizzare il nome DNS per montare i client su file system con scalabilità orizzontale, perché aiuta a garantire che i client siano bilanciati tra le coppie ad alta disponibilità (HA) del file system.

   ```
   sudo mount -t smbfs 198.51.100.10:/C$ /fsx
   ```

   `C$`è la condivisione SMB predefinita che puoi montare per visualizzare la radice dello spazio dei nomi di SVM. Se hai creato delle condivisioni Server Message Block (SMB) nella tua SVM, fornisci i nomi delle condivisioni SMB anziché. `C$` Per ulteriori informazioni sulla creazione di condivisioni SMB, consulta. Gestione delle condivisioni SMB

Per montare un volume ONTAP su un client macOS utilizzando NFS

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.

2. Crea o seleziona un'istanza Amazon EC2 che esegue Amazon Linux 2 che si trova nello stesso VPC del file system.

   Per ulteriori informazioni sul lancio di un'istanza EC2 Linux, consulta Step 1: Launch an instance nella Amazon EC2 User Guide.

3. Connect alla tua istanza Amazon EC2 Linux. Per ulteriori informazioni, consulta Connect to your Linux istance nella Amazon EC2 User Guide.

4. Monta il volume FSx for ONTAP sull'istanza Linux EC2 utilizzando uno script di dati utente durante l'avvio dell'istanza o eseguendo i seguenti comandi:

   ```
   sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-point
   ```

   L'esempio seguente utilizza valori di esempio.

   ```
   sudo mount -t nfs -o nfsvers=4.1
    svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

   È inoltre possibile utilizzare l'indirizzo IP SVM della SVM anziché il relativo nome DNS. Consigliamo di utilizzare il nome DNS per montare i client su file system con scalabilità orizzontale perché aiuta a garantire che i client siano bilanciati tra le coppie HA del file system.

   ```
   sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
   ```

5. Monta il volume nella directory appena creata utilizzando il seguente comando.

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   L'esempio seguente utilizza valori di esempio.

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   È inoltre possibile utilizzare l'indirizzo IP SVM della SVM anziché il relativo nome DNS. Consigliamo di utilizzare il nome DNS per montare i client su file system con scalabilità orizzontale, perché aiuta a garantire che i client siano bilanciati tra le coppie ad alta disponibilità (HA) del file system.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

Montaggio di LUN iSCSI

Amazon FSx for NetApp ONTAP fornisce supporto per lo storage a blocchi condiviso tramite il protocollo iSCSI (Internet Small Computer Systems Interface). È possibile abilitare lo storage iSCSI effettuando il provisioning dei LUN (Logical Unit Number) e mappandoli ai gruppi di iniziatori (igroup), esponendo lo storage a blocchi agli host Linux e Windows.

> **Note**
>
> Il protocollo iSCSI non è supportato per i file system scalabili FSx for ONTAP, che sono file system con più di una coppia di file server ad alta disponibilità (HA).

Argomenti

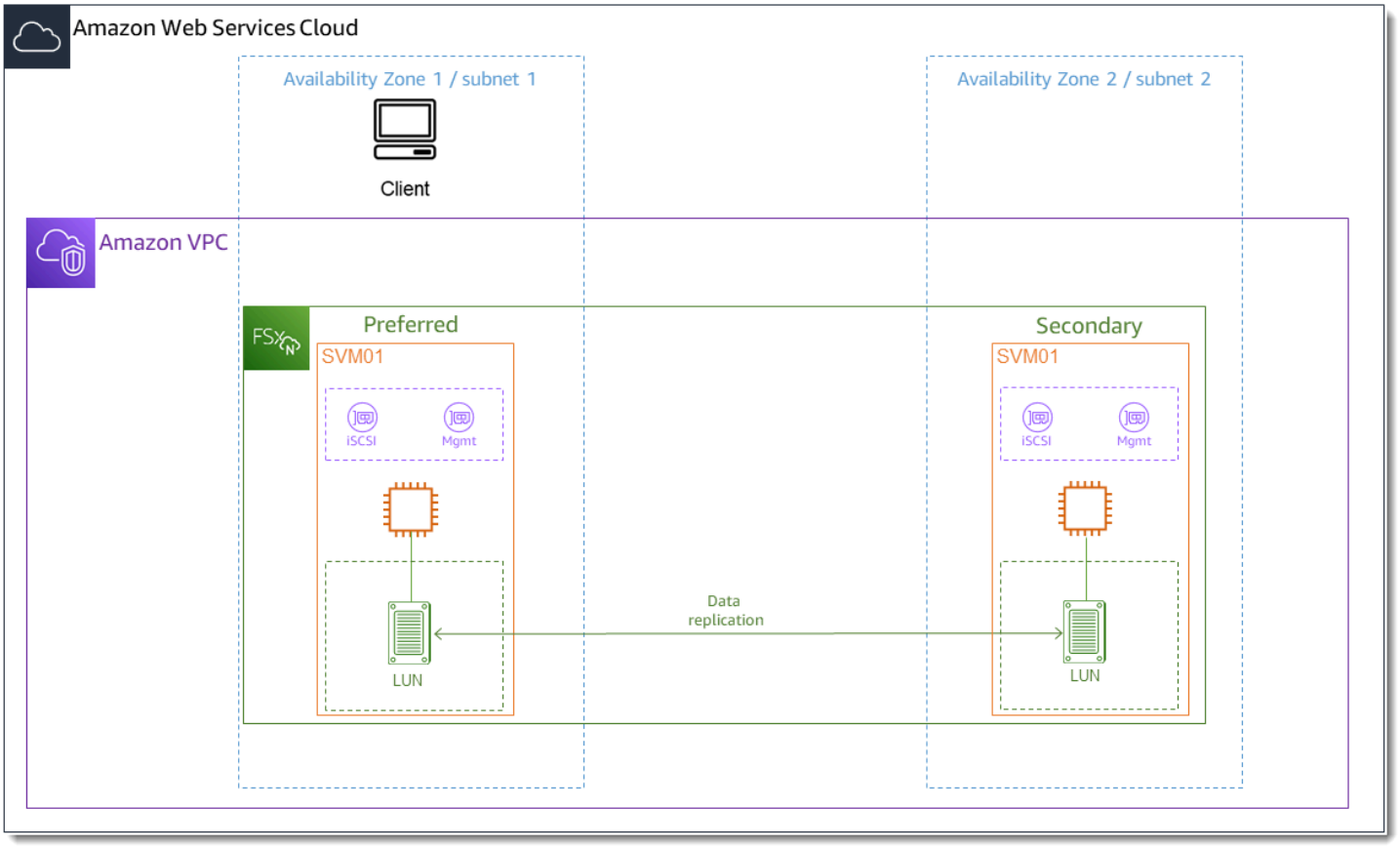
Montaggio di LUN iSCSI su un client Linux

Gli esempi presentati in queste procedure utilizzano la seguente configurazione:

- Il LUN iSCSI che viene montato sull'host Linux è già stato creato. Per ulteriori informazioni, consulta Creazione di un LUN iSCSI.
- L'host Linux che sta montando il LUN iSCSI è un'istanza Amazon EC2 che esegue Amazon Linux 2 Amazon Machine Image (AMI). Dispone di gruppi di sicurezza VPC configurati per consentire il traffico in entrata e in uscita come descritto in. Controllo degli accessi ai file system con Amazon VPC
- L'host Linux e il file system FSx for ONTAP si trovano nello stesso VPC e. Account AWS Se l'host si trova in un altro VPC, è possibile utilizzare il peering VPC o concedere AWS Transit Gateway ad altri VPC l'accesso agli endpoint iSCSI del volume. Per ulteriori informazioni, consulta Accesso ai dati dall'esterno del VPC di implementazione.

Se utilizzi un'istanza EC2 che esegue un'AMI Linux diversa, alcune delle utilità che vengono installate sull'host potrebbero essere preinstallate e potresti utilizzare comandi diversi per installare i pacchetti richiesti. Oltre all'installazione dei pacchetti, i comandi utilizzati in questa sezione sono validi per altre AMI Linux EC2.

Consigliamo che l'istanza EC2 si trovi nella stessa zona di disponibilità della sottorete preferita del file system, come mostrato nella figura seguente.



Argomenti

- Installare e configurare iSCSI sul client Linux
- Configurare iSCSI sul file system FSx for ONTAP
- Montare un LUN iSCSI sul client Linux

Installare e configurare iSCSI sul client Linux

Per installare il client iSCSI

1. Confermalo `iscsi-initiator-utils` e `device-mapper-multipath` sono installati sul tuo dispositivo Linux. Connect alla propria istanza Linux utilizzando un client SSH. Per ulteriori informazioni, vedi Connect alla tua istanza Linux usando SSH.
2. Installa `multipath` e installa il client iSCSI utilizzando il seguente comando. L'installazione `multipath` è necessaria se si desidera eseguire automaticamente il failover tra i file server.

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. Per facilitare una risposta più rapida in caso di failover automatico tra file server durante l'utilizzo`multipath`, impostate il valore di timeout sostitutivo nel `/etc/iscsi/iscsid.conf` file su un valore `5` anziché su quello predefinito di. `120`

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/
node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/
iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. Avviare il servizio iSCSI.

```
~$ sudo service iscsid start
```

Tieni presente che, a seconda della versione di Linux in uso, potrebbe essere necessario utilizzare invece questo comando:

```
~$ sudo systemctl start iscsid
```

5. Verificate che il servizio sia in esecuzione utilizzando il comando seguente.

```
~$ sudo systemctl status iscsid.service
```

Il sistema risponde con il seguente risultato:

```
iscsid.service - Open-iSCSI
    Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor
 preset: disabled)
    Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
```

```
    Docs: man:iscsid(8)
    man:iscsiadm(8)
    Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
    CGroup: /system.slice/iscsid.service
    ##14659 /usr/sbin/iscsid
    ##14660 /usr/sbin/iscsid
```

Per configurare iSCSI sul tuo client Linux

1. Per consentire ai client di eseguire automaticamente il failover tra i file server, è necessario configurare multipath. Utilizza il seguente comando:

   ```
   ~$ sudo mpathconf --enable --with_multipathd y
   ```

2. Determinate il nome dell'iniziatore del vostro host Linux utilizzando il comando seguente. La posizione del nome dell'iniziatore dipende dall'utilità iSCSI in uso. Se si utilizza`iscsi-initiator-utils`, il nome dell'iniziatore si trova nel file. `/etc/iscsi/initiatorname.iscsi`

   ```
   ~$ sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   Il sistema risponde con il nome dell'iniziatore.

   ```
   InitiatorName=iqn.1994-05.com.redhat:abcdef12345
   ```

Configurare iSCSI sul file system FSx for ONTAP

1. Connect alla CLI NetApp ONTAP sul file system FSx for ONTAP su cui è stato creato il LUN iSCSI utilizzando il comando seguente. Per ulteriori informazioni, consulta Utilizzo della CLI NetApp ONTAP.

   ```
   ~$ ssh fsxadmin@your_management_endpoint_ip
   ```

2. Crea il gruppo di iniziatori (`igroup`) utilizzando il comando NetApp ONTAP CLI. lun igroup create Un gruppo di iniziatori esegue il mapping sulle LUN iSCSI e controlla quali iniziatori (client) hanno accesso alle LUN. Sostituirlo `host_initiator_name` con il nome dell'iniziatore dell'host Linux recuperato nella procedura precedente.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype linux
```

Se si desidera rendere le LUN mappate su questo igroup disponibili a più host, è possibile specificare più nomi di iniziatori separati da una virgola. Per ulteriori informazioni, consulta lun igroup create nel Centro documentazione ONTAP. NetApp

3. Conferma che `igroup` esiste usando il comando: lun igroup show

```
::> lun igroup show
```

Il sistema risponde con il seguente risultato:

```
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
svm_name  igroup_name  iscsi    linux    iqn.1994-05.com.redhat:abcdef12345
```

4. Questo passaggio presuppone che sia già stato creato un LUN iSCSI. In caso contrario, consulta Creazione di un LUN iSCSI le step-by-step istruzioni in merito.

   Create una mappatura dal LUN creato all'igroup creato, utilizzando lun mapping create, specificando i seguenti attributi:

   - *svm_name*— Il nome della macchina virtuale di archiviazione che fornisce la destinazione iSCSI. L'host utilizza questo valore per raggiungere il LUN.
   - *vol_name*— Il nome del volume che ospita il LUN.
   - *lun_name*— Il nome assegnato al LUN.
   - *igroup_name*— Il nome del gruppo iniziatore.
   - *lun_id*— Il numero intero dell'ID LUN è specifico della mappatura, non del LUN stesso. Viene utilizzato dagli iniziatori dell'igroup poiché il numero di unità logica utilizza questo valore per l'iniziatore quando accede allo storage.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Utilizzate il `lun show -path`comando per confermare che il LUN è stato creato, online e mappato.

```
::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
```

Il sistema risponde con il seguente output:

```
 Vserver    Path                            serial-hex               state    mapped
 --------- ------------------------------- ------------------------ --------
 --------
 svm_name  /vol/vol_name/lun_name          6c5742314e5d52766e796150 online   mapped
```

Salva il `serial_hex` valore (in questo esempio lo è`6c5742314e5d52766e796150`), lo utilizzerai in un passaggio successivo per creare un nome descrittivo per il dispositivo a blocchi.

6. Utilizzate il `network interface show -vserver`comando per recuperare gli indirizzi `iscsi_1` e le `iscsi_2` interfacce per l'SVM in cui avete creato il LUN iSCSI.

```
::> network interface show -vserver svm_name
```

Il sistema risponde con il seguente output:

```
            Logical               Status     Network            Current
        Current Is
Vserver     Interface             Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------            ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.0.143/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.21.81/20
 FSxId0123456789abcdef8-02  e0e     true
            nfs_smb_management_1
                                  up/up      198.19.250.177/20
 FSxId0123456789abcdef8-01  e0e     true
3 entries were displayed.
```

In questo esempio, l'indirizzo IP di `iscsi_1` è `172.31.0.143` ed `iscsi_2` è`172.31.21.81`.

Montare un LUN iSCSI sul client Linux

1. *Sul client Linux, utilizzare il comando seguente per individuare i nodi iSCSI di destinazione utilizzando l'indirizzo IP iscsi_1 iSCSI_1_IP.*

```
~$ sudo iscsiadm --mode discovery --op update --type sendtargets --
portal iscsi_1_IP
```

```
172.31.0.143:3260,1029
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
172.31.21.81:3260,1028
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

   In questo esempio, `iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3` corrisponde al `target_initiator` LUN iSCSI nella zona di disponibilità preferita.

2. (Facoltativo) È possibile stabilire sessioni aggiuntive con. `target_initiator` Amazon EC2 ha un limite di larghezza di banda di 5 Gb/s (~625 MB/s) per il traffico a flusso singolo, ma puoi creare più sessioni per aumentare i livelli di throughput del tuo file system da un singolo client. Per ulteriori informazioni, consulta la larghezza di banda di rete delle istanze Amazon EC2 nella Guida per l'utente di Amazon Elastic Compute Cloud per istanze Linux.

   Il comando seguente stabilisce 8 sessioni per iniziatore per nodo ONTAP in ogni zona di disponibilità, consentendo al client di gestire fino a 40 GB/s (5.000 MB/s) di throughput aggregato verso il LUN iSCSI.

```
~$ sudo iscsiadm --mode node -T target_initiator --op update -n
 node.session.nr_sessions -v 8
```

3. Accedere agli iniziatori di destinazione. Le LUN iSCSI vengono presentate come dischi disponibili.

```
~$ sudo iscsiadm --mode node -T target_initiator --login
```

```
Logging in to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] (multiple)
```

```
Login to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] successful.
```

L'output precedente è troncato; dovrebbe essere visualizzata una `Logging in` `Login successful` risposta per ogni sessione su ciascun file server. Nel caso di 4 sessioni per nodo, ci saranno 8 `Logging in` e 8 risposte. `Login successful`

4. Utilizzare il comando seguente per verificare di aver `dm-multipath` identificato e unito le sessioni iSCSI mostrando un singolo LUN con più policy. Dovrebbe esserci un numero uguale di dispositivi elencati come `active` e quelli elencati come. `enabled`

```
~$ sudo multipath -ll
```

Nell'output, il nome del disco è formattato come`dm-xyz`, dove `xyz` è un numero intero. Se non sono presenti altri dischi multipath, questo valore è. `dm-0`

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
 hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda     8:0   active ready running
| |- 1:0:0:1 sdc     8:32  active ready running
| |- 3:0:0:1 sdg     8:96  active ready running
| `- 4:0:0:1 sdh     8:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb     8:16  active ready running
  |- 7:0:0:1 sdf     8:80  active ready running
  |- 6:0:0:1 sde     8:64  active ready running
  `- 5:0:0:1 sdd     8:48  active ready running
```

Il dispositivo a blocchi è ora connesso al client Linux. Si trova sotto il percorso`/dev/dm-xyz`. Non è consigliabile utilizzare questo percorso per scopi amministrativi, ma utilizzare il collegamento simbolico che si trova sotto il percorso`/dev/mapper/wwid`, dove si `wwid` trova un identificatore univoco per il LUN coerente tra i dispositivi. Nel passaggio successivo, fornirai un nome `wwid` descrittivo per distinguerlo dagli altri dischi a percorso multiplo.

Per assegnare al dispositivo a blocchi un nome descrittivo

1. Per assegnare al dispositivo un nome descrittivo, crea un alias nel `/etc/multipath.conf` file. A tale scopo, aggiungi la seguente voce al file utilizzando il tuo editor di testo preferito, sostituendo i seguenti segnaposto:

   - Sostituisci `serial_hex` con il valore salvato nella Configurare iSCSI sul file system FSx for ONTAP procedura.
   - Aggiungete il prefisso `3600a0980` al `serial_hex` valore come mostrato nell'esempio. Questo è un preambolo unico per la distribuzione NetApp ONTAP utilizzata da Amazon FSx for ONTAP. NetApp
   - `device_name`Sostituiscilo con il nome descrittivo che desideri utilizzare per il tuo dispositivo.

   ```
   multipaths {
       multipath {
           wwid 3600a0980serial_hex
           alias device_name
       }
   }
   ```

   In alternativa, puoi copiare e salvare il seguente script come file bash, ad esempio. `multipath_alias.sh` È possibile eseguire lo script con i privilegi sudo, sostituendolo *`serial_hex`* (senza il prefisso 3600a0980) e *`device_name`* con il rispettivo numero di serie e il nome descrittivo desiderato. Questo script cerca una sezione non commentata nel file. `multipaths` `/etc/multipath.conf` Se ne esiste una, aggiunge una `multipath` voce a quella sezione; in caso contrario, creerà una nuova `multipaths` sezione con una `multipath` voce per il dispositivo a blocchi.

   ```
   #!/bin/bash
   SN=serial_hex
   ALIAS=device_name
   CONF=/etc/multipath.conf
   grep -q '^multipaths {' $CONF
   UNCOMMENTED=$?
   if [ $UNCOMMENTED -eq 0 ]
   then
           sed -i '/^multipaths {/a\\tmultipath {\n\t\twwid 3600a0980'"${SN}"'\n\t
   \talias '"${ALIAS}"'\n\t}\n' $CONF
   else
   ```

```
        printf "multipaths {\n\tmultipath {\n\t\twwid 3600a0980$SN\n\t\talias
 $ALIAS\n\t}\n}" >> $CONF
fi
```

2. Riavvia il `multipathd` servizio per `/etc/multipathd.conf` rendere effettive le modifiche.

```
~$ systemctl restart multipathd.service
```

Per partizionare il LUN

Il passaggio successivo consiste nel formattare e partizionare il LUN utilizzando. `fdisk`

1. Utilizzate il seguente comando per verificare che il percorso del vostro `device_name` sia presente.

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. Partiziona il disco usando`fdisk`. Inserirai un prompt interattivo. Inserisci le opzioni nell'ordine mostrato. Si noti che il `Last sector` valore varia in base alla dimensione del LUN iSCSI (10 GB in questo esempio). È possibile creare più partizioni utilizzando un valore inferiore all'ultimo settore (`20971519`in questo esempio).

```
~$ sudo fdisk /dev/mapper/device_name
```

Viene avviato il prompt `fsdisk` interattivo.

```
Welcome to fdisk (util-linux 2.30.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
```

```
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
 20971519): 20971519

Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

Dopo l'accessow, la nuova partizione `/dev/mapper/`*`partition_name`* diventa disponibile. <device_name><partition_number>Il *`partition_name`* ha il formato. 1è stato utilizzato come numero di partizione utilizzato nel `fdisk` comando nel passaggio precedente.

3. Crea il tuo file system utilizzando `/dev/mapper/`*`partition_name`* come percorso.

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

Il sistema risponde con il seguente output:

```
mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Per montare il LUN sul client Linux

1. Create una directory *directory_path* come punto di montaggio per il file system.

```
~$ sudo mkdir /directory_path/mount_point
```

2. Monta il file system usando il seguente comando.

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. (Facoltativo) È possibile modificare la proprietà della directory di montaggio per l'utente. *username*Sostituiscila con il tuo nome utente.

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (Facoltativo) Verifica di poter leggere e scrivere dati sul file system.

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

È stato creato e montato correttamente un LUN iSCSI sul client Linux.

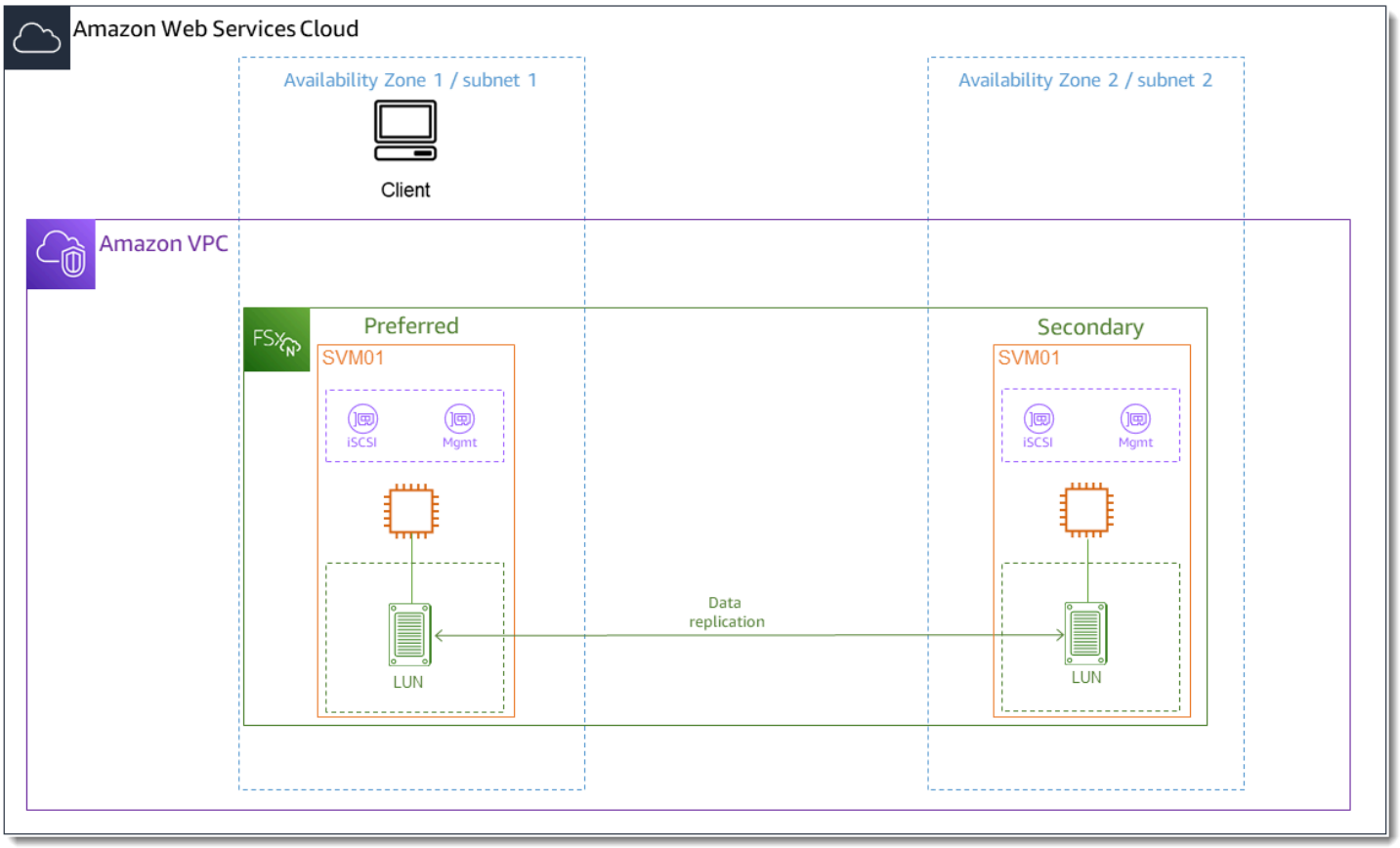
Montaggio di LUN iSCSI su un client Windows

Gli esempi presentati in queste procedure utilizzano la seguente configurazione:

- Il LUN iSCSI che viene montato su un host Windows è già stato creato. Per ulteriori informazioni, consulta Creazione di un LUN iSCSI.
- L'host Microsoft Windows che sta montando il LUN iSCSI è un'istanza Amazon EC2 che esegue un Microsoft Windows Server 2019 Amazon Machine Image (AMI). Dispone di gruppi di sicurezza VPC configurati per consentire il traffico in entrata e in uscita come descritto in. Controllo degli accessi ai file system con Amazon VPC

  È possibile che tu stia utilizzando un'AMI Microsoft Windows diversa nella configurazione.
- Il client e il file system si trovano nello stesso VPC e. Account AWS Se il client si trova in un altro VPC, è possibile utilizzare il peering VPC o concedere AWS Transit Gateway ad altri VPC l'accesso agli endpoint iSCSI. Per ulteriori informazioni, consulta Accesso ai dati dall'esterno del VPC di implementazione.

Consigliamo che l'istanza EC2 si trovi nella stessa zona di disponibilità della sottorete preferita del file system, come mostrato nel grafico seguente.



Argomenti

- Configurare iSCSI sul client Windows
- Configurare iSCSI sul file system FSx for ONTAP
- Montare un LUN iSCSI sul client Windows
- Convalida della configurazione iSCSI

Configurare iSCSI sul client Windows

1. Utilizzare Windows Remote Desktop per connettersi al client Windows su cui si desidera montare il LUN iSCSI. Per ulteriori informazioni, consulta Connect to your Windows using RDP nella Amazon Elastic Compute Cloud User Guide.

2. Apri un Windows PowerShell come amministratore. Utilizzare i seguenti comandi per abilitare iSCSI sull'istanza di Windows e configurare il servizio iSCSI per l'avvio automatico.

```
PS C:\> Start-Service MSiSCSI
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. Recuperate il nome dell'iniziatore dell'istanza di Windows. Questo valore verrà utilizzato per configurare iSCSI sul file system FSx for ONTAP utilizzando l'ONTAP CLI. NetApp

```
PS C:\> (Get-InitiatorPort).NodeAddress
```

Il sistema risponde con la porta dell'iniziatore:

```
iqn.1991-05.com.microsoft:ec2amaz-abc123d
```

4. Per consentire ai client di eseguire automaticamente il failover tra i file server, è necessario installare `Multipath-IO` (MPIO) sull'istanza di Windows. Utilizza il seguente comando:

```
PS C:\> Install-WindowsFeature Multipath-IO
```

5. Riavvia l'istanza di Windows al termine dell'`Multipath-IO`installazione. Tenere aperta l'istanza di Windows per eseguire i passaggi per il montaggio del LUN iSCSI in una sezione che segue.

Configurare iSCSI sul file system FSx for ONTAP

1. Connect alla CLI NetApp ONTAP sul file system FSx for ONTAP su cui è stato creato il LUN iSCSI utilizzando il comando seguente. Per ulteriori informazioni, consulta Utilizzo della CLI NetApp ONTAP.

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. Utilizzando la lun igroup createCLI NetApp ONTAP, create il gruppo di iniziatori oppure. `igroup` Un gruppo di iniziatori esegue il mapping sulle LUN iSCSI e controlla quali iniziatori (client) hanno accesso alle LUN. Sostituirlo `host_initiator_name` con il nome dell'iniziatore dall'host Windows recuperato nella procedura precedente.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype windows
```

Se si desidera rendere `igroup` disponibili a più host le LUN mappate su questo server, è possibile specificare più nomi di iniziatori separati da virgole. Per ulteriori informazioni, consulta *lun igroup create*il Centro di documentazione ONTAP. NetApp

3. Conferma che `igroup` è stato creato correttamente utilizzando il seguente comando:

```
::> lun igroup show
```

Il sistema risponde con il seguente risultato:

```
Vserver    Igroup        Protocol OS Type  Initiators
---------  ------------  -------- -------- ------------------------------------
svm_name   igroup_name   iscsi    windows  iqn.1994-05.com.windows:abcdef12345
```

Una volta `igroup` creato, sei pronto per creare LUN e mapparle su. `igroup`

4. Questo passaggio presuppone che sia già stato creato un LUN iSCSI. In caso contrario, consulta Creazione di un LUN iSCSI le step-by-step istruzioni in merito.

Crea una mappatura LUN dal LUN al tuo nuovo. `igroup`

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. Conferma che il LUN sia stato creato, online e mappato con il seguente comando:

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

Ora sei pronto per aggiungere il target iSCSI sulla tua istanza di Windows.

6. Recuperate gli indirizzi IP di `iscsi_1` e le `iscsi_2` interfacce per il vostro SVM utilizzando il seguente comando:

```
::> network interface show -vserver svm_name
```

```
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
```

```
----------- ---------- ---------- ------------------ ------------- ------- ----
svm_name
            iscsi_1    up/up      172.31.0.143/20    FSxId0123456789abcdef8-01
                                                                   e0e     true
            iscsi_2    up/up      172.31.21.81/20    FSxId0123456789abcdef8-02
                                                                   e0e     true
            nfs_smb_management_1
                       up/up      198.19.250.177/20  FSxId0123456789abcdef8-01
                                                                   e0e     true
3 entries were displayed.
```

In questo esempio, l'indirizzo IP di `iscsi_1` is e is`172.31.0.143`. `iscsi_2` `172.31.21.81`

Montare un LUN iSCSI sul client Windows

1. Sulla tua istanza Windows, apri un PowerShell terminale come amministratore.
2. Creerai uno `.ps1` script che esegue le seguenti operazioni:

   - Si connette a ciascuna delle interfacce iSCSI del file system.
   - Aggiunge e configura MPIO per iSCSI.
   - Stabilisce 8 sessioni per ogni connessione iSCSI, il che consente al client di indirizzare fino a 40 GB/s (5.000 MB/s) di throughput aggregato verso il LUN iSCSI. Le 8 sessioni garantiscono che un singolo client possa gestire l'intera capacità di throughput di 4.000 MB/s per la capacità di throughput FSx for ONTAP di massimo livello. Facoltativamente, è possibile modificare il numero di sessioni impostando un numero maggiore o minore di sessioni (ogni sessione fornisce fino a 625 MB/s di throughput) modificando il for-loop dello script nel passaggio da un altro limite superiore. `#Establish iSCSI connection` `1..8` Per ulteriori informazioni, consulta la larghezza di banda di rete delle istanze Amazon EC2 nella Guida per l'utente di Amazon Elastic Compute Cloud per istanze Windows.

   Copia il seguente set di comandi in un file per creare lo script. `.psl`

   - Sostituisci `iscsi_1` e `iscsi_2` con gli indirizzi IP recuperati nel passaggio precedente.
   - Sostituiscilo `ec2_ip` con l'indirizzo IP dell'istanza di Windows.

```
#iSCSI IP addresses for Preferred and Standby subnets
$TargetPortalAddresses = @("iscsi_1","iscsi_2")
```

```
#iSCSI Initator IP Address (Local node IP address)
$LocaliSCSIAddress = "ec2_ip"

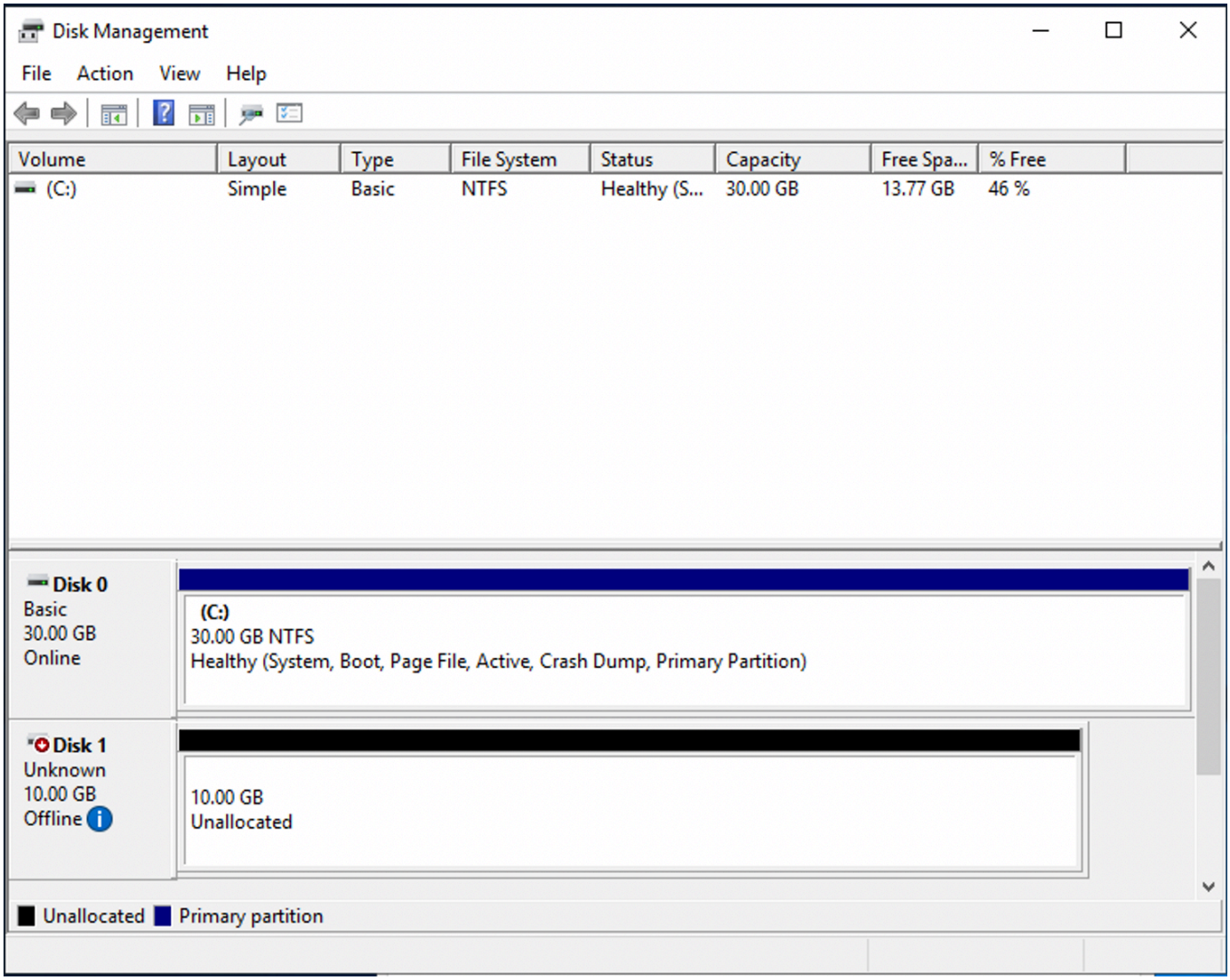
#Connect to FSx for NetApp ONTAP file system
Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
}

#Add MPIO support for iSCSI
New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

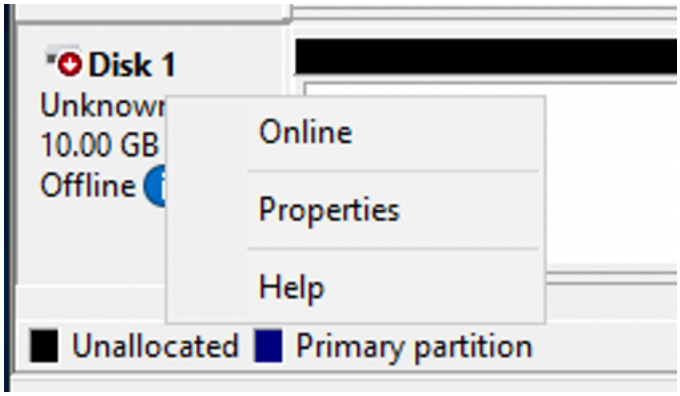
#Establish iSCSI connection
1..8 | %{Foreach($TargetPortalAddress in $TargetPortalAddresses)
{Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true}}

#Set the MPIO Policy to Round Robin
Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

3. Avvia l'applicazione Windows Disk Management. Apri la finestra di dialogo Esegui di Windows, quindi inserisci `diskmgmt.msc` e premi Invio. Si apre l'applicazione Gestione disco.



4. Individua il disco non allocato Questo è il LUN iSCSI. Nell'esempio, il disco 1 è il disco iSCSI. È offline.



Porta il volume online posizionando il cursore sul Disco 1, fai clic con il pulsante destro del mouse, quindi scegli Online.

> **Note**
>
> È possibile modificare la politica della rete SAN (Storage Area Network) in modo che i nuovi volumi vengano automaticamente portati online. Per ulteriori informazioni, vedere le politiche SAN nel Microsoft Windows Server Command Reference.

5. Per inizializzare il disco, posiziona il cursore sul Disco 1 con il pulsante destro del mouse e scegli Inizializza. Viene visualizzata la finestra di dialogo di inizializzazione. Scegliete OK per inizializzare il disco.
6. Formattate il disco come fareste normalmente. Al termine della formattazione, l'unità iSCSI viene visualizzata come unità utilizzabile sul client Windows.

Convalida della configurazione iSCSI

Abbiamo fornito uno script per verificare che la configurazione iSCSI sia configurata correttamente. Lo script esamina parametri quali il conteggio delle sessioni, la distribuzione dei nodi e lo stato di Multipath I/O (MPIO). La seguente attività spiega come installare e utilizzare lo script.

Per convalidare la configurazione iSCSI

1. Aprire una finestra di Windows PowerShell .
2. Scaricate lo script utilizzando il seguente comando.

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/
samples/CheckiSCSI.zip" -OutFile "CheckiSCSI.zip"
```

3. Espandi il file zip usando il seguente comando.

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

4. Esegui lo script utilizzando il seguente comando.

```
PS C:\> ./CheckiSCSI.ps1
```

5. Esamina l'output per comprendere lo stato attuale della configurazione. L'esempio seguente dimostra una configurazione iSCSI corretta.

```
PS C:\> ./CheckiSCSI.ps1
```

```
This script checks the iSCSI configuration on the local instance.
It will provide information about the number of connected sessions, connected file
 servers, and MPIO status.

MPIO is installed on this server.

Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'
has 16 total sessions (16 active, 0 non-active)
spread across 2 node(s).
MPIO: Yes
```

Utilizzo di FSx for ONTAP con altri servizi AWS

Oltre ad Amazon EC2, puoi utilizzare altri AWS servizi con i tuoi volumi per accedere ai tuoi dati.

Argomenti

- Utilizzo di Amazon WorkSpaces con FSx for ONTAP
- Utilizzo di Amazon Elastic Container Service con FSx per ONTAP
- Utilizzo di VMware Cloud con FSx for ONTAP

Utilizzo di Amazon WorkSpaces con FSx for ONTAP

FSx for ONTAP può essere utilizzato con Amazon per WorkSpaces fornire storage NAS (Network-Attached Storage) condiviso o per archiviare profili di roaming per account Amazon. WorkSpaces Dopo essersi connesso a una condivisione di file SMB con un' WorkSpaces istanza, l'utente può creare e modificare file sulla condivisione di file.

Le seguenti procedure mostrano come utilizzare Amazon FSx con Amazon WorkSpaces per fornire un profilo di roaming e accesso alla cartella principale un'esperienza coerente e per fornire una cartella di team condivisa per gli utenti Windows e Linux. WorkSpaces Se non conosci Amazon WorkSpaces, puoi creare il tuo primo WorkSpaces ambiente Amazon seguendo le istruzioni riportate nella Guida all' WorkSpaces amministrazione di Amazon Get started with WorkSpaces Quick Setup.

Argomenti

Fornisci supporto per i profili di roaming

Puoi usare Amazon FSx per fornire supporto per i profili di roaming agli utenti della tua organizzazione. Un utente avrà le autorizzazioni per accedere solo al proprio profilo di roaming. La cartella verrà connessa automaticamente utilizzando i criteri di gruppo di Active Directory. Con un profilo di roaming, i dati e le impostazioni del desktop degli utenti vengono salvati quando si disconnettono da una condivisione di file Amazon FSx, che consente la condivisione di documenti e impostazioni tra diverse WorkSpaces istanze e il backup automatico tramite i backup automatici giornalieri di Amazon FSx.

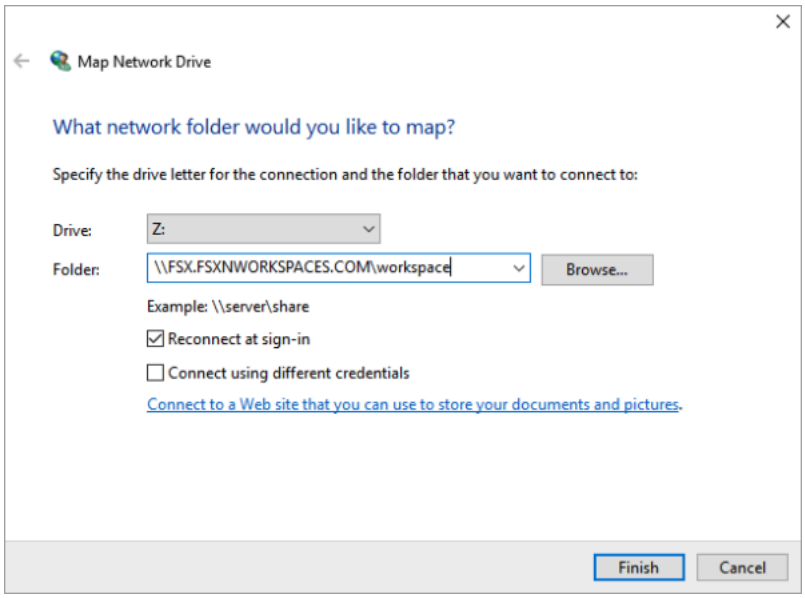
Fase 1: creare una posizione per la cartella del profilo per gli utenti del dominio utilizzando Amazon FSx

1. Crea un file system FSx for ONTAP utilizzando la console Amazon FSx. Per ulteriori informazioni, consulta Per creare un file system (console).

   > **Important**
   >
   > Ogni file system FSx for ONTAP ha un intervallo di indirizzi IP dell'endpoint da cui vengono creati gli endpoint associati al file system. Per i file system Multi-AZ, FSx for ONTAP sceglie un intervallo di indirizzi IP inutilizzato predefinito compreso tra 198.19.0.0/16 come intervallo di indirizzi IP dell'endpoint. Questo intervallo di indirizzi IP viene utilizzato anche WorkSpaces per la gestione dell'intervallo di traffico, come descritto nella sezione Requisiti dell'indirizzo IP e della porta WorkSpaces nella Amazon WorkSpaces Administration Guide. Di conseguenza, per accedere al file system Multi-AZ FSx for ONTAP WorkSpaces da, è necessario selezionare un intervallo di indirizzi IP dell'endpoint che non si sovrapponga a 198.19.0.0/16.

2. Se non disponi di una macchina virtuale di archiviazione (SVM) unita a un Active Directory, creane una ora. Ad esempio, è possibile effettuare il provisioning di una SVM denominata `fsx` e impostare lo stile di sicurezza su. `NTFS` Per ulteriori informazioni, consulta Per creare una macchina virtuale di archiviazione (console).

3. Crea un volume per il tuo SVM. Ad esempio, potete creare un volume denominato `fsx-vol` che erediti lo stile di sicurezza del volume root della SVM. Per ulteriori informazioni, consulta Per creare un volume (console) FlexVol.
4. Crea una condivisione SMB sul tuo volume. Ad esempio, puoi creare una condivisione chiamata `workspace` sul tuo volume denominato`fsx-vol`, in cui crei una cartella denominata`profiles`. Per ulteriori informazioni, consulta Gestione delle condivisioni SMB.
5. Accedi al tuo Amazon FSx SVM da un'istanza Amazon EC2 che esegue Windows Server o da un. WorkSpace Per ulteriori informazioni, consulta Accesso ai dati .
6. Puoi mappare la tua condivisione `Z:\` su un'istanza Windows: WorkSpaces



Passaggio 2: collegare la condivisione di file FSx for ONTAP agli account utente

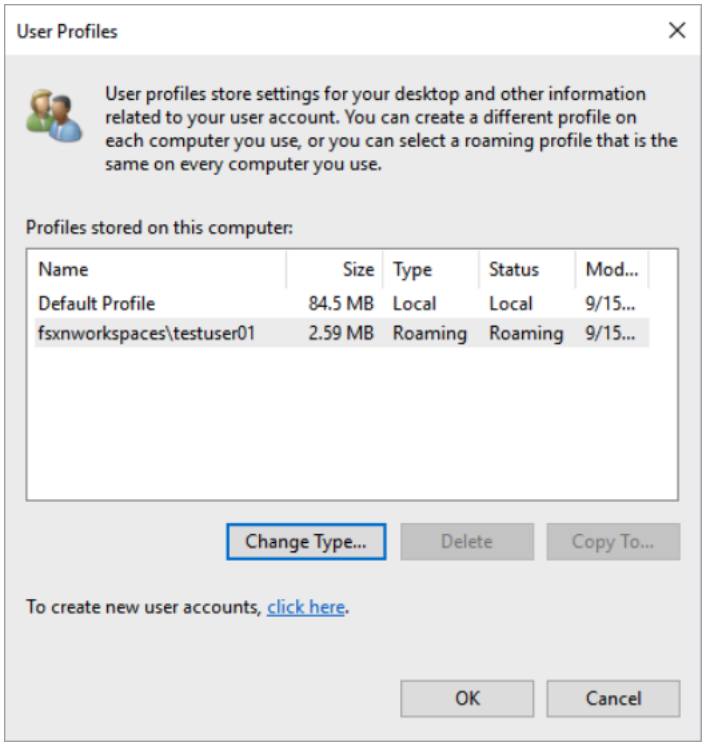
1. Su quello dell'utente di prova WorkSpace, scegli Windows > Sistema > Impostazioni di sistema avanzate.
2. In Proprietà del sistema, seleziona la scheda Avanzate e premi il pulsante Impostazioni nella sezione Profili utente. L'utente che ha effettuato l'accesso avrà un tipo di profilo di. `Local`
3. Disconnettere l'utente di prova da. WorkSpace
4. Imposta l'utente di test in modo che disponga di un profilo di roaming sul tuo file system Amazon FSx. Nel tuo amministratore WorkSpaces, apri una PowerShell console e usa un comando simile al seguente esempio (che utilizza la `profiles` cartella che hai creato in precedenza nel passaggio 1):

```
Set-ADUser username -ProfilePath \\filesystem-dns-
name\sharename\foldername\username
```

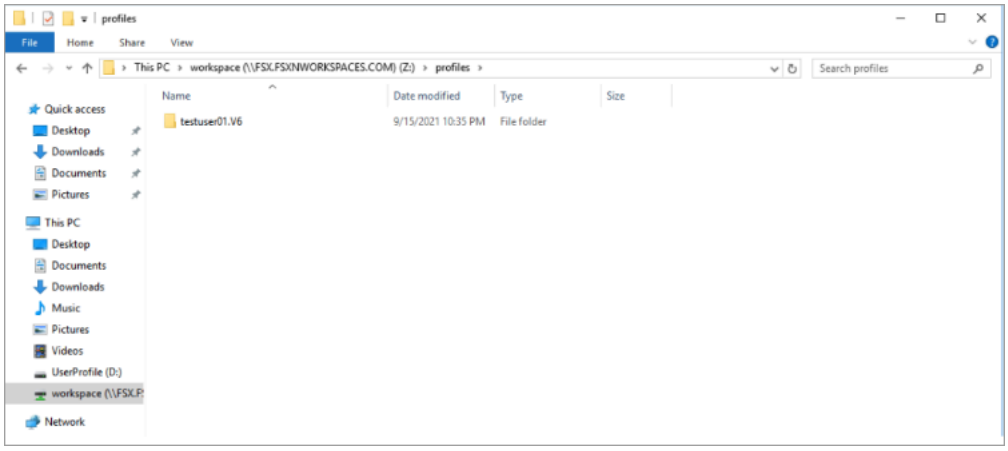
Per esempio:

```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxnworkspaces.com\workspace\profiles
\testuser01
```

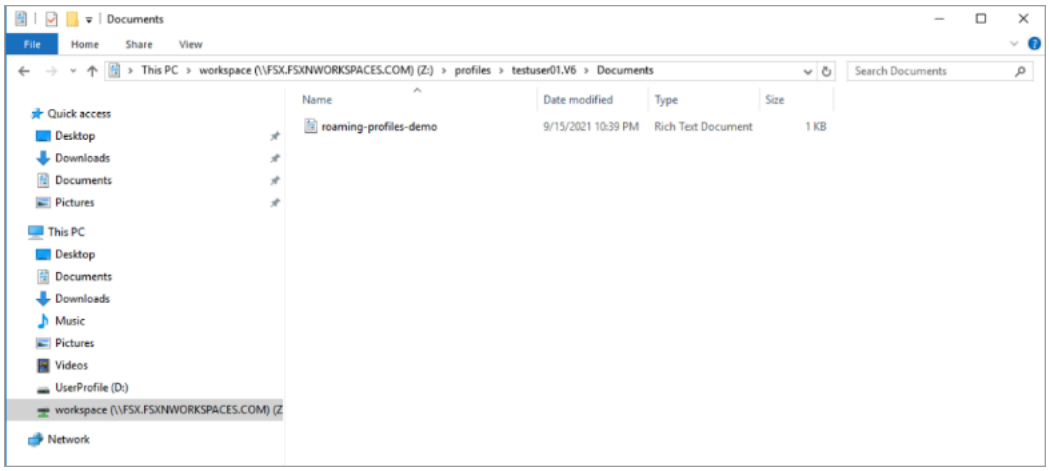
5. Accedere all'utente di prova WorkSpace.
6. In Proprietà del sistema, seleziona la scheda Avanzate e premi il pulsante Impostazioni nella sezione Profili utente. L'utente che ha effettuato l'accesso avrà un tipo di profilo di. `Roaming`



7. Sfoglia la cartella condivisa di FSx for ONTAP. Nella `profiles` cartella, vedrai una cartella per l'utente.



8. Crea un documento nella `Documents` cartella dell'utente di test
9. Disconnetti l'utente di test dal suo WorkSpace.
10. Se accedi nuovamente come utente di prova e accedi al suo archivio di profili, vedrai il documento che hai creato.



Fornisci una cartella condivisa per accedere ai file comuni

Puoi usare Amazon FSx per fornire una cartella condivisa agli utenti della tua organizzazione. Una cartella condivisa può essere utilizzata per archiviare i file utilizzati dalla tua comunità di utenti, come file demo, esempi di codice e manuali di istruzioni necessari a tutti gli utenti. In genere, le unità sono mappate per cartelle condivise; tuttavia, poiché le unità mappate utilizzano lettere, esiste un limite al numero di condivisioni che è possibile avere. Questa procedura crea una cartella condivisa Amazon FSx disponibile senza una lettera drive, offrendoti una maggiore flessibilità nell'assegnazione delle condivisioni ai team.

Per montare una cartella condivisa per l'accesso multipiattaforma da Linux e Windows WorkSpaces

1. Dalla barra delle applicazioni, scegli Places > Connect to Server.

   a. Per Server, inserisci. *`file-system-dns-name`*

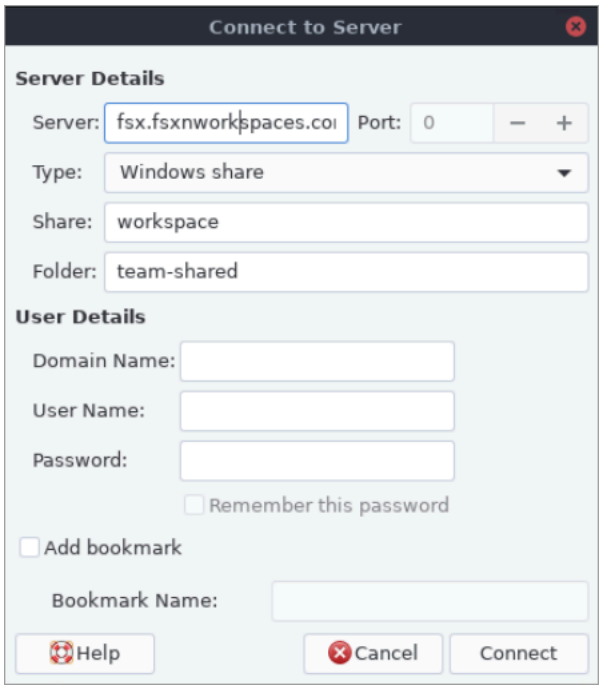
   b. Imposta Tipo su`Windows share`.

   c. Imposta Share sul nome della condivisione SMB, ad esempio`workspace`.

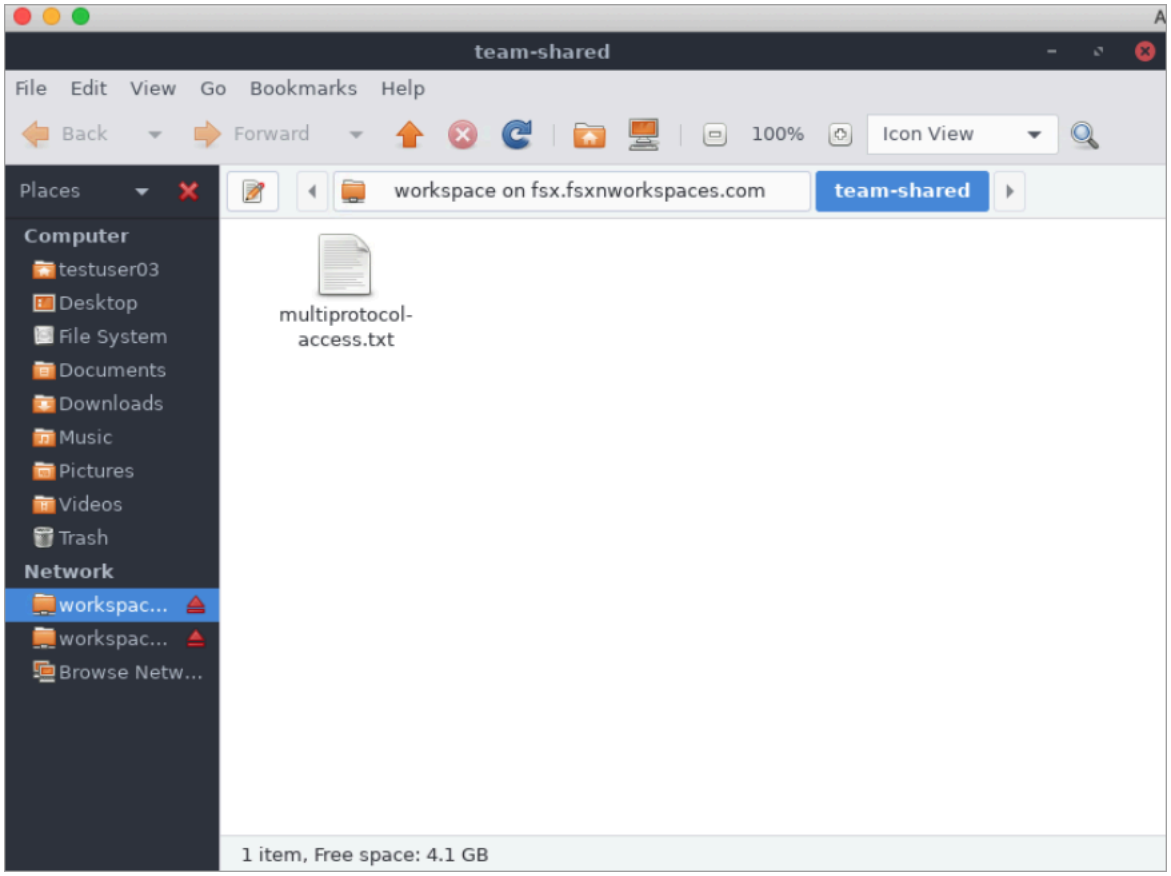
   d. È possibile lasciare la cartella invariata `/` o impostarla su una cartella, ad esempio una cartella denominata`team-shared`.

   e. Per un Linux WorkSpace, non è necessario inserire i dati utente se Linux si WorkSpace trova nello stesso dominio della condivisione Amazon FSx.

   f. Scegli Connetti.



2. Dopo aver effettuato la connessione, è possibile visualizzare la cartella condivisa (denominata `team-shared` in questo esempio) nella condivisione SMB denominata. `workspace`



Utilizzo di Amazon Elastic Container Service con FSx per ONTAP

Puoi accedere ai tuoi file system Amazon FSx for NetApp ONTAP da un contenitore Docker Amazon Elastic Container Service (Amazon ECS) su un'istanza Amazon EC2 Linux o Windows.

Montaggio su un container Amazon ECS Linux

1. Crea un cluster ECS utilizzando il modello di cluster EC2 Linux + Networking per i tuoi contenitori Linux. Per ulteriori informazioni, consulta Creating a cluster nella Amazon Elastic Container Service Developer Guide.
2. Crea una directory sull'istanza EC2 per montare il volume SVM come segue:

```
sudo mkdir /fsxontap
```

3. Monta il volume FSx for ONTAP sull'istanza Linux EC2 utilizzando uno script di dati utente durante l'avvio dell'istanza o eseguendo i seguenti comandi:

```
sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
```

4. Monta il volume utilizzando il seguente comando:

```
sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /
fsxontap
```

L'esempio seguente utilizza valori di esempio.

```
sudo mount -t nfs -o nfsvers=4.1
 svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
fsxontap
```

È inoltre possibile utilizzare l'indirizzo IP SVM dell'SVM anziché il nome DNS.

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. Quando crei le definizioni delle attività Amazon ECS, aggiungi quanto segue `volumes` e le proprietà del `mountPoints` contenitore nella definizione del contenitore JSON. Sostituite il `sourcePath` con il punto di montaggio e la directory nel file system FSx for ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Montaggio su un contenitore Amazon ECS Windows

1. Crea un cluster ECS utilizzando il modello di cluster EC2 Windows+ Networking per i tuoi contenitori Windows. Per ulteriori informazioni, consulta Creating a cluster nella Amazon Elastic Container Service Developer Guide.
2. Aggiungi un'istanza Windows EC2 aggiunta a un dominio al cluster ECS Windows e mappa una condivisione SMB.

   Avvia un'istanza Windows EC2 ottimizzata per ECS aggiunta al tuo dominio Active Directory e inizializza l'agente ECS eseguendo il comando seguente.

   ```
   PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
   EnableTaskIAMRole
   ```

   Puoi anche passare le informazioni contenute in uno script al campo di testo user-data come segue.

   ```
   <powershell>
   Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
   </powershell>
   ```
3. Crea una mappatura globale SMB sull'istanza EC2 in modo da poter mappare la tua condivisione SMB su un'unità. Sostituisci i valori sotto netbios o nome DNS per il file system FSx e il nome della condivisione. Il volume NFS vol1 che è stato montato sull'istanza Linux EC2 è configurato come una condivisione CIFS fsxontap sul file system FSx.

   ```
   vserver cifs share show -vserver svm08 -share-name fsxontap


                                   Vserver: svm08
                                     Share: fsxontap
                   CIFS Server NetBIOS Name: FSX0NTAPDEMO
                                     Path: /vol1
                           Share Properties: oplocks
                                             browsable
                                             changenotify
                                             show-previous-versions
                                Symlink Properties: symlinks
                         File Mode Creation Mask: -
                    Directory Mode Creation Mask: -
   ```

```
                                Share Comment: -
                                    Share ACL: Everyone / Full Control
                File Attribute Cache Lifetime: -
                                  Volume Name: vol1
                                Offline Files: manual
                    Vscan File-Operations Profile: standard
              Maximum Tree Connections on Share: 4294967295
                     UNIX Group for File Create: -
```

4. Crea la mappatura globale SMB sull'istanza EC2 utilizzando il seguente comando:

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. Quando crei le definizioni delle attività Amazon ECS, aggiungi quanto segue `volumes` e le proprietà del `mountPoints` contenitore nella definizione del contenitore JSON. Sostituite il `sourcePath` con il punto di montaggio e la directory nel file system FSx for ONTAP.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Utilizzo di VMware Cloud con FSx for ONTAP

È possibile utilizzare FSx for ONTAP come datastore esterno per VMware Cloud on AWS Software-Defined Data Center (SDDC). Per ulteriori informazioni, consulta Configurare Amazon FSx for

NetApp ONTAP come storage esterno e VMware Cloud on with AWS Amazon FSx for ONTAP Deployment Guide. NetApp

Disponibilità e durabilità

Amazon FSx for NetApp ONTAP utilizza due tipi di implementazione, Single-AZ e Multi-AZ, che offrono diversi livelli di disponibilità e durabilità. Questo argomento descrive le caratteristiche di disponibilità e durabilità di ogni tipo di implementazione per aiutarti a scegliere quella più adatta ai tuoi carichi di lavoro. Per informazioni sullo SLA (Service Level Agreement) di disponibilità del servizio, consulta Amazon FSx Service Level Agreement.

Argomenti

Scelta del tipo di distribuzione del file system

Le caratteristiche di disponibilità e durabilità dei tipi di implementazione dei file system Single-AZ e Multi-AZ sono descritte nelle sezioni seguenti.

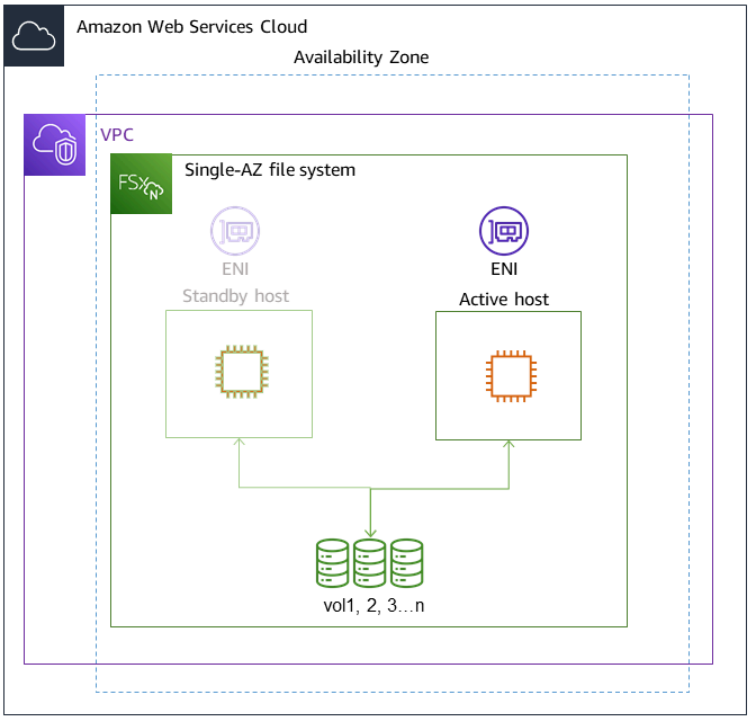
Tipo di implementazione Single-AZ

Quando crei un file system Single-AZ, Amazon FSx effettua automaticamente il provisioning da una a dodici coppie di file server in una configurazione di standby attivo, con i file server attivi e in standby di ciascuna coppia situati in domini di errore separati all'interno di una singola zona di disponibilità nel. Regione AWS Durante la manutenzione pianificata del file system o un'interruzione non pianificata del servizio di qualsiasi file server attivo, Amazon FSx esegue automaticamente e indipendentemente il failover di quella coppia ad alta disponibilità (HA) sul file server di standby, in genere entro pochi secondi. Durante un failover, continui ad avere accesso ai tuoi dati senza intervento manuale.

Per garantire un'elevata disponibilità, Amazon FSx monitora continuamente i guasti hardware e sostituisce automaticamente i componenti dell'infrastruttura in caso di guasto. Per ottenere una durabilità elevata, Amazon FSx replica automaticamente i dati all'interno di una zona di disponibilità per proteggerli dai guasti dei componenti. Inoltre, hai la possibilità di configurare backup giornalieri automatici dei dati del file system. Questi backup vengono archiviati in più zone di disponibilità per fornire resilienza Multi-AZ per tutti i dati di backup.

I file system Single-AZ sono progettati per casi d'uso che non richiedono il modello di resilienza dei dati di un file system Multi-AZ. Forniscono una soluzione ottimizzata in termini di costi per casi d'uso come ambienti di sviluppo e test o per l'archiviazione di copie secondarie di dati già archiviati in locale o in altro modo Regioni AWS, replicando i dati solo all'interno di una singola zona di disponibilità.

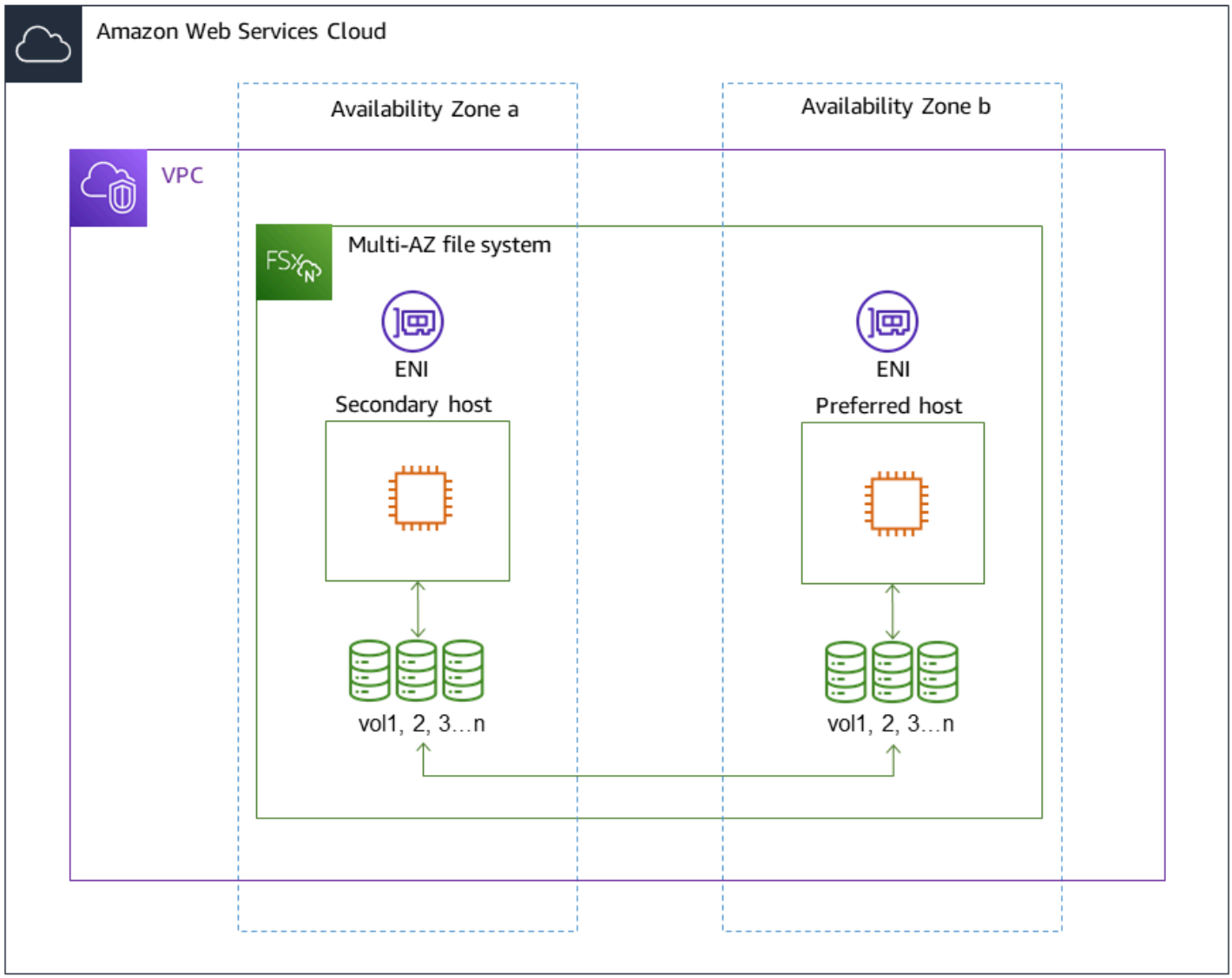
Il diagramma seguente illustra l'architettura di un file system FSx for ONTAP Single-AZ.



Tipo di implementazione Multi-AZ

I file system Multi-AZ supportano tutte le caratteristiche di disponibilità e durabilità dei file system Single-AZ. Inoltre, sono progettati per fornire una disponibilità continua dei dati anche quando non è disponibile una zona di disponibilità. Le implementazioni Multi-AZ prevedono un'unica coppia di file server HA, il file server di standby viene distribuito in una zona di disponibilità diversa dal file server attivo nella stessa. Regione AWS Tutte le modifiche scritte nel file system vengono replicate in modo sincrono tra le zone di disponibilità fino allo standby.

I file system Multi-AZ sono progettati per casi d'uso come carichi di lavoro di produzione aziendali critici che richiedono un'elevata disponibilità dei dati dei file ONTAP condivisi e richiedono uno storage con replica integrata tra le zone di disponibilità. Il diagramma seguente illustra l'architettura di un file system FSx for ONTAP Multi-AZ.



Processo di failover per FSx for ONTAP

I file system Single-AZ e Multi-AZ eseguono automaticamente il failover di una determinata coppia HA dal file server preferito o attivo al file server di standby se si verifica una delle seguenti condizioni:

- Il file server preferito o attivo non è più disponibile
- La capacità di throughput del file system viene modificata
- Il file server preferito o attivo viene sottoposto a manutenzione pianificata
- Si verifica un'interruzione della zona di disponibilità (solo file system Multi-AZ)

> **Note**
>
> Per i file system con scalabilità orizzontale, il comportamento di failover di ogni coppia HA è indipendente. Se il file server preferito per una coppia HA non è disponibile, solo quella coppia HA eseguirà il failover sul relativo file server di standby.

Quando si esegue il failover da un file server a un altro, il nuovo file server attivo inizia automaticamente a inviare tutte le richieste di lettura e scrittura del file system a quella coppia HA. Per i file system Multi-AZ, quando il file server preferito viene completamente ripristinato e diventa disponibile, Amazon FSx esegue automaticamente il failback su di esso, con il failback che di solito viene completato in meno di 60 secondi. Per i file system Single-AZ e Multi-AZ, il failover viene generalmente completato in meno di 60 secondi, dal rilevamento dell'errore sul file server attivo alla promozione del file server di standby allo stato attivo. Poiché l'indirizzo IP dell'endpoint utilizzato dai client per accedere ai dati tramite NFS o SMB rimane lo stesso, i failover sono trasparenti per le applicazioni Linux, Windows e macOS, che riprendono le operazioni del file system senza intervento manuale.

Per garantire che i failover siano trasparenti per i client collegati al file system FSx for ONTAP Single-AZ e Multi-AZ, vedere. Accesso ai dati dall'interno AWS

Test del failover su un file system

È possibile testare il failover su un file system con scalabilità verticale modificandone la capacità di throughput. Quando modifichi la capacità di throughput del file system, Amazon FSx disattiva i file server del file system in modo seriale. I file system eseguono automaticamente il failover sul server secondario, mentre Amazon FSx sostituisce prima il file server preferito. Una volta aggiornato, il file system esegue automaticamente il failback sul nuovo server primario e Amazon FSx sostituisce il file server secondario.

Puoi monitorare l'avanzamento della richiesta di aggiornamento della capacità di throughput nella console Amazon FSx, nella CLI e nell'API. Per ulteriori informazioni sulla modifica della capacità di throughput del file system e sul monitoraggio dell'avanzamento della richiesta, consulta. Gestione della capacità di throughput

Risorse di rete

Questa sezione descrive le risorse di rete utilizzate dai file system Single-AZ e Multi-AZ.

Sottoreti

Quando si crea un file system Single-AZ, si specifica una singola sottorete per il file system. La sottorete scelta definisce la zona di disponibilità in cui viene creato il file system. Quando si crea un file system Multi-AZ, si specificano due sottoreti, una per il file server preferito e una per il file server di standby. Le due sottoreti scelte devono trovarsi in zone di disponibilità diverse all'interno della stessa. Regione AWS Per ulteriori informazioni su Amazon VPC, consulta Cos'è Amazon VPC? nella Guida per l'utente di Amazon Virtual Private Cloud.

> **Note**
>
> Indipendentemente dalla sottorete specificata, è possibile accedere al file system da qualsiasi sottorete all'interno del VPC del file system.

Interfacce di rete elastiche del file system

Per i file system Single-AZ, Amazon FSx fornisce due interfacce di rete elastiche (ENI) nella sottorete associata al file system. Per i file system Multi-AZ, Amazon FSx fornisce anche due ENI, una in ciascuna delle sottoreti associate al file system. I client comunicano con il file system Amazon FSx utilizzando l'interfaccia elastic network. Le interfacce di rete sono considerate rientranti nell'ambito del servizio di Amazon FSx, nonostante facciano parte del VPC del tuo account. I file system Multi-AZ utilizzano indirizzi IP (Internet Protocol) mobili in modo che i client connessi passino senza problemi dal file server preferito a quello di standby durante un evento di failover.

> **Warning**
>
> - Non è necessario modificare o eliminare le interfacce di rete elastiche associate al 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.
> - Le interfacce di rete elastiche associate al file system avranno percorsi creati e aggiunti automaticamente alle tabelle di routing VPC e subnet predefinite. La modifica o l'eliminazione di queste route può causare la perdita temporanea o permanente della connettività per i client del file system.

La tabella seguente riassume le risorse di sottorete, elastic network interface e indirizzo IP per ciascuno dei tipi di implementazione del file system FSx for ONTAP:

	Single-AZ (scalabilità verticale)	Single-AZ (scalabilità orizzontale)	Multi-AZ (scalabilità verticale)
Numero di sottoreti	1	1	2
Numero di interfacce di rete elastiche	2	2 per coppia HA	2
Numero di indirizzi IP per ENI	1 + il numero di SVM nel file system	Numero di coppie HA + Numero di coppie HA moltiplicato per il numero di SVM nel file system	1 + il numero di SVM nel file system
Numero di percorsi della tabella di routing VPC	N/D	N/D	1 + il numero di SVM nel file system

Una volta creato un file system o SVM, i relativi indirizzi IP non cambiano finché il file system non viene eliminato.

> **Important**
>
> Amazon FSx non supporta l'accesso ai file system da o l'esposizione dei file system alla rete Internet pubblica. Amazon FSx scollega 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.

Gestione della capacità di archiviazione

Amazon FSx for NetApp ONTAP offre una serie di funzionalità relative allo storage che puoi utilizzare per gestire la capacità di storage sul tuo file system.

Argomenti

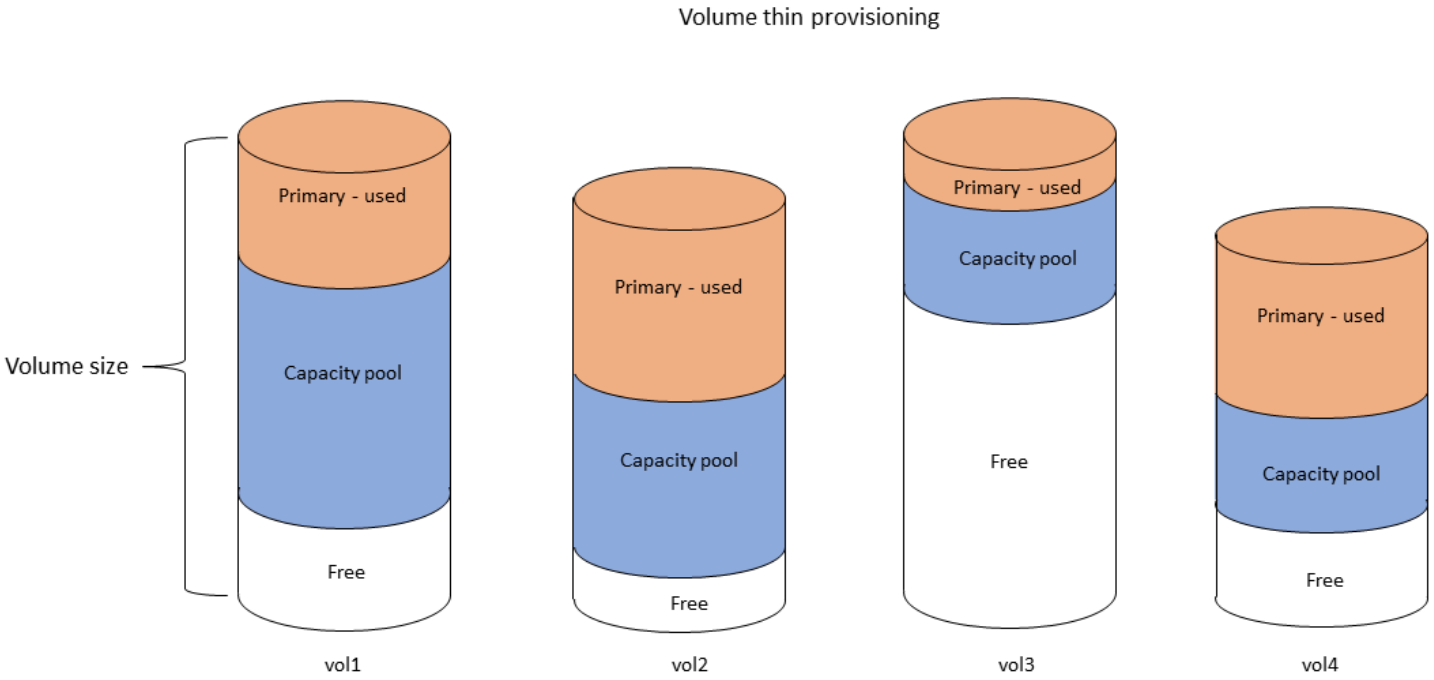
Livelli di storage FSx for ONTAP

I livelli di storage sono i supporti di storage fisici per un file system Amazon FSx NetApp for ONTAP. FSx for ONTAP offre i seguenti livelli di storage:

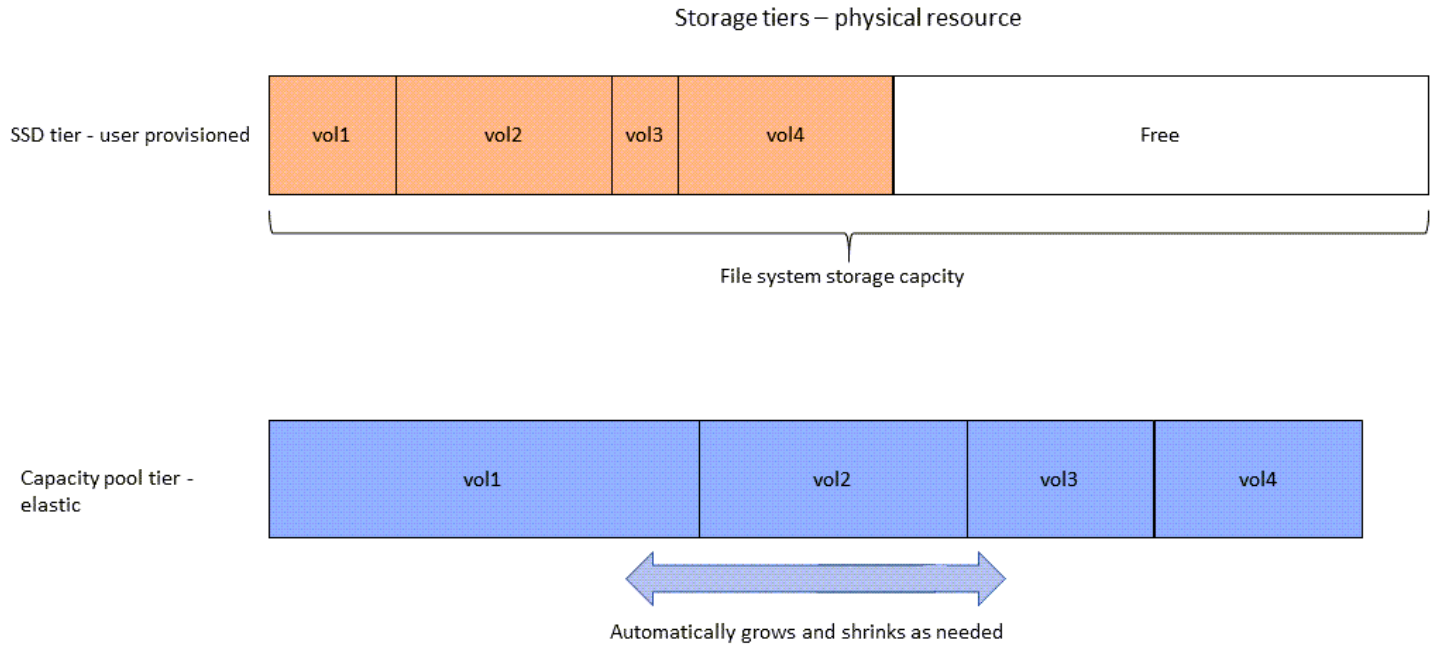
- Livello SSD: lo storage su unità a stato solido (SSD) ad alte prestazioni fornito dall'utente e progettato appositamente per la parte attiva del set di dati.
- Livello di pool di capacità: storage completamente elastico con scalabilità automatica fino a petabyte e ottimizzato in termini di costi per i dati a cui si accede raramente.

Un volume FSx for ONTAP è una risorsa virtuale che, analogamente alle cartelle, non consuma capacità di storage. I dati archiviati, e che utilizzano lo storage fisico, risiedono all'interno di volumi. Quando crei un volume, ne specifichi la dimensione, che puoi modificare dopo la creazione. I volumi FSx for ONTAP sono dotati di thin provisioning e lo storage del file system non è riservato in anticipo. Invece, lo storage su SSD e pool di capacità viene allocato dinamicamente, in base alle esigenze. Una politica di tiering, configurata a livello di volume, determina se e quando i dati archiviati nel livello SSD passano al livello del pool di capacità.

Il diagramma seguente illustra un esempio di dati disposti su più volumi FSx for ONTAP in un file system.



Il diagramma seguente illustra come la capacità di archiviazione fisica del file system viene consumata dai dati nei quattro volumi del diagramma precedente.



È possibile ridurre i costi di storage scegliendo la politica di suddivisione in più livelli che meglio soddisfa i requisiti per ogni volume del file system. Per ulteriori informazioni, consulta Suddivisione dei dati su più livelli.

Scelta della giusta quantità di storage SSD per file system

Quando si sceglie la quantità di capacità di archiviazione SSD per il file system FSx for ONTAP, è necessario tenere presente i seguenti elementi che influiscono sulla quantità di storage SSD disponibile per l'archiviazione dei dati:

- Capacità di archiviazione riservata al sovraccarico del NetApp software ONTAP.
- Metadati dei file
- Dati scritti di recente
- File che intendi archiviare su un dispositivo di archiviazione SSD, che si tratti di dati che non hanno raggiunto il periodo di raffreddamento o di dati che hai letto di recente e che sono stati recuperati su SSD.

Come viene utilizzata l'archiviazione SSD

L'archiviazione SSD del file system viene utilizzata per una combinazione di software NetApp ONTAP (overhead), metadati dei file e dati.

NetApp Sovraccarico del software ONTAP

Come altri file system NetApp ONTAP, fino al 16% della capacità di archiviazione SSD di un file system è riservata al sovraccarico di ONTAP, il che significa che non è disponibile per l'archiviazione dei file. L'overhead ONTAP viene allocato come segue:

- L'11% è riservato al software ONTAP NetApp . Per i file system con oltre 30 tebibyte (TiB) di capacità di archiviazione SSD, il 6% è riservato.
- Il 5% è riservato alle istantanee aggregate, necessarie per sincronizzare i dati tra entrambi i file server di un file system.

Metadati dei file

I metadati dei file in genere occupano il 3-7% della capacità di archiviazione utilizzata dai file. Questa percentuale dipende dalla dimensione media dei file (una dimensione media di file inferiore richiede più metadati) e dalla quantità di risparmio in termini di efficienza di archiviazione ottenuto sui file. Tieni presente che i metadati dei file non traggono vantaggio dai risparmi in termini di efficienza dello

storage. Puoi utilizzare le seguenti linee guida per stimare la quantità di storage SSD utilizzata per i metadati sul tuo file system.

Dimensione media del file	Dimensione dei metadati come percentuale dei dati del file
4 KB	7%
8 KB	3,5%
32 KB o superiore	1-3%

Quando si ridimensiona la quantità di capacità di archiviazione SSD necessaria per i metadati dei file che si intende archiviare sul livello del pool di capacità, si consiglia di utilizzare un rapporto conservativo di 1 GiB di storage SSD per ogni 10 GiB di dati che si prevede di archiviare sul livello del pool di capacità.

Dati di file archiviati sul livello SSD

Oltre al set di dati attivo e a tutti i metadati dei file, tutti i dati scritti sul file system vengono inizialmente scritti sul livello SSD prima di essere suddivisi in livelli di storage con pool di capacità. Ciò vale indipendentemente dalla politica di suddivisione in più livelli del volume, ad eccezione del trasferimento dei dati tramite un volume configurato con una politica di suddivisione SnapMirror in più livelli dei dati.

Le letture casuali dal livello del pool di capacità vengono memorizzate nella cache del livello SSD, a condizione che il livello SSD sia utilizzato al di sotto del 90%. Per ulteriori informazioni, consulta Suddivisione dei dati su più livelli.

Utilizzo della capacità SSD consigliato

Si consiglia di non superare l'80% di utilizzo del livello di storage SSD su base continuativa. Per i file system con scalabilità orizzontale, consigliamo inoltre di non superare l'80% di utilizzo degli aggregati del file system su base continuativa. Questi consigli sono coerenti con quelli consigliati per NetApp ONTAP. Poiché il livello SSD del file system viene utilizzato anche per lo staging delle scritture e per le letture casuali dal livello del pool di capacità, eventuali cambiamenti improvvisi nei modelli di accesso possono causare un rapido aumento dell'utilizzo del livello SSD.

Al 90% di utilizzo dell'unità SSD, i dati letti dal livello del pool di capacità non vengono più memorizzati nella cache sul livello SSD, in modo che la capacità SSD residua venga preservata per eventuali nuovi dati scritti sul file system. Ciò fa sì che le letture ripetute degli stessi dati dal livello del pool di capacità vengano lette dallo storage del pool di capacità anziché essere memorizzate nella cache e lette dal livello SSD, il che può influire sulla capacità di throughput del file system.

Tutte le funzionalità di suddivisione in più livelli si interrompono quando il livello SSD raggiunge o supera il 98% di utilizzo. Per ulteriori informazioni, consulta Soglie di suddivisione in più livelli.

FSx per l'efficienza dello storage ONTAP

NetApp ONTAP offre funzionalità di efficienza dello storage a livello di blocco, tra cui compressione, compattazione e deduplicazione, che consentono di risparmiare fino al 65% della capacità di storage per le condivisioni di file generiche, senza sacrificare le prestazioni.

Amazon FSx for NetApp ONTAP supporta anche altre funzionalità ONTAP che consentono di risparmiare spazio, tra cui istantanee, thin provisioning e volumi. FlexClone

Le funzionalità di efficienza dello storage non sono abilitate per impostazione predefinita. È possibile abilitarle come segue:

- Sul volume root di una SVM quando si crea un file system.
- Quando crei un nuovo volume.
- Quando modifichi un volume esistente.

Per visualizzare la quantità di risparmio di storage su un file system con l'efficienza dello storage abilitata, vedereVisualizzazione dei risparmi sull'efficienza dello storage.

Calcolo dei risparmi in termini di efficienza dello storage

È possibile utilizzare le metriche del CloudWatch file `StorageUsed` system `LogicalDataStored` and FSx for ONTAP per calcolare i risparmi di storage derivanti da compressione, deduplicazione, compattazione, istantanee e. FlexClones Queste metriche hanno un'unica dimensione,. `FileSystemId` Per ulteriori informazioni, consulta Metriche del file system.

- Per calcolare i risparmi in termini di efficienza dello storage in byte, prendi la media di `StorageUsed` un determinato periodo e la sottrai dalla media dello stesso periodo. `LogicalDataStored`

- Per calcolare i risparmi in termini di efficienza dello storage come percentuale della dimensione totale dei dati logici, prendete il valore di in un determinato periodo e `Average StorageUsed` sottraetelo dal risultato ottenuto nello stesso periodo. `Average LogicalDataStored` Quindi dividi la differenza per il o nello stesso periodo`Average. LogicalDataStored`

Esempio di dimensionamento di un SSD

Si supponga di voler archiviare 100 TiB di dati per un'applicazione in cui l'80% dei dati viene utilizzato raramente. In questo scenario, l'80% (80 TB) dei dati viene automaticamente trasferito su più livelli al livello del pool di capacità e il restante 20% (20 TB) rimane nello storage SSD. In base al tipico risparmio di efficienza dello storage del 65% per carichi di lavoro di condivisione di file generici, ciò equivale a 7 TiB di dati. Per mantenere un tasso di utilizzo dell'SSD dell'80%, sono necessari 8,75 TiB di capacità di storage SSD per i 20 TiB di dati a cui si accede attivamente. La quantità di storage SSD fornita deve inoltre tenere conto del sovraccarico di archiviazione del software ONTAP del 16%, come illustrato nel calcolo seguente.

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

Quindi, in questo esempio, è necessario effettuare il provisioning di almeno 10,42 TiB di storage SSD. Utilizzerai anche 28 TiB di storage con pool di capacità per i restanti 80 TiB di dati a cui si accede raramente.

Capacità di storage del file system e IOPS

Quando si crea un file system FSx for ONTAP, si specifica la capacità di storage del livello SSD. Per i file system con scalabilità orizzontale, la capacità di storage specificata viene distribuita in modo uniforme tra i pool di storage di ciascuna coppia ad alta disponibilità (HA); questi pool di storage sono chiamati aggregati.

Per ogni GiB di storage SSD fornito, Amazon FSx effettua automaticamente il provisioning di 3 operazioni di input/output SSD al secondo (IOPS) per il file system, fino a un massimo di 160.000 IOPS SSD per file system. Per i file system con scalabilità orizzontale, gli IOPS SSD sono distribuiti in modo uniforme su ciascuno degli aggregati del file system. È possibile specificare un livello di IOPS SSD assegnato superiore ai 3 IOPS SSD automatici per GiB. Per ulteriori informazioni sul numero massimo di IOPS SSD che è possibile fornire per il file system FSx for ONTAP, vedere. Impatto della capacità di throughput sulle prestazioni

Argomenti

Aggiornamento dello storage SSD e degli IOPS del file system

Quando hai bisogno di storage aggiuntivo per la parte attiva del tuo set di dati, puoi aumentare la capacità di storage SSD del tuo file system Amazon FSx NetApp for ONTAP. Usa la console Amazon FSx, l'API Amazon FSx o AWS Command Line Interface (AWS CLI) per aumentare la capacità di storage SSD. Per ulteriori informazioni, consulta Modifica della capacità di archiviazione SSD e degli IOPS assegnati.

Quando aumenti la capacità di storage SSD del tuo file system Amazon FSx, la nuova capacità è in genere disponibile per l'uso in pochi minuti. Ti verrà addebitata la nuova capacità di storage SSD non appena sarà disponibile. Per ulteriori informazioni sui prezzi, consulta la pagina dei prezzi di Amazon FSx for NetApp ONTAP.

Dopo aver aumentato la capacità di storage, Amazon FSx esegue un processo di ottimizzazione dello storage in background per riequilibrare i dati. Per la maggior parte dei file system, l'ottimizzazione dello storage richiede alcune ore, con un impatto minimo evidente sulle prestazioni del carico di lavoro.

Puoi monitorare l'avanzamento del processo di ottimizzazione dello storage in qualsiasi momento utilizzando la console Amazon FSx, la CLI e l'API. Per ulteriori informazioni, consulta Monitoraggio della capacità di storage e degli aggiornamenti IOPS.

Considerazioni

Ecco alcuni elementi importanti da considerare quando si modifica la capacità di storage SSD di un file system e gli IOPS assegnati:

- Solo aumento della capacità di archiviazione: puoi solo aumentare la quantità di capacità di archiviazione SSD per un file system, non puoi diminuire la capacità di archiviazione.
- Aumento minimo della capacità di archiviazione: ogni aumento della capacità di archiviazione SSD deve essere pari almeno al 10 percento dell'attuale capacità di archiviazione SSD del file system, fino alla capacità di archiviazione SSD massima per la configurazione del file system.
- (Solo scalabilità orizzontale) Diffusione della capacità di archiviazione: la nuova capacità di archiviazione o IOPS SSD selezionata per il file system viene distribuita in modo uniforme su tutti gli aggregati del file system.
- Tempo tra un aumento e l'altro: dopo aver modificato la capacità di archiviazione SSD, gli IOPS assegnati o la capacità di throughput su un file system, è necessario attendere almeno sei ore prima di modificare nuovamente una di queste configurazioni sullo stesso file system. Talvolta viene definito tempo di raffreddamento.
- Modalità IOPS assegnate: per una modifica IOPS assegnata, è necessario specificare una delle due modalità IOPS:
  - Modalità automatica: Amazon FSx ridimensiona automaticamente gli IOPS SSD per mantenere 3 IOPS SSD assegnati per GiB di capacità di storage SSD, fino al massimo di IOPS SSD per la configurazione del file system.

    > **Note**
    >
    > Per ulteriori informazioni sul numero massimo di IOPS SSD che è possibile fornire per il file system FSx for ONTAP, vedere. Impatto della capacità di throughput sulle prestazioni

  - Modalità con provisioning utente: si specifica il numero di IOPS SSD, che deve essere maggiore o uguale a 3 IOPS per GiB di capacità di archiviazione SSD. Se scegli di fornire un livello più elevato di IOPS, pagherai per gli IOPS medi forniti al di sopra della tariffa inclusa per il mese, misurata in mesi IOPS.

Per ulteriori informazioni sui prezzi, consulta la pagina dei prezzi di Amazon FSx for NetApp ONTAP.

Quando aumentare la capacità di archiviazione SSD

Se stai esaurendo lo storage disponibile di livello SSD, ti consigliamo di aumentare la capacità di archiviazione del tuo file system. L'esaurimento dello spazio di archiviazione indica che il livello SSD è sottodimensionato rispetto alla parte attiva del set di dati.

Per monitorare la quantità di spazio di archiviazione gratuito disponibile sul file system, utilizza i parametri a livello di file system e `StorageCapacity` `StorageUsed` Amazon CloudWatch . Puoi creare un CloudWatch allarme in base a una metrica e ricevere una notifica quando scende al di sotto di una soglia specifica. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.

> **Note**
>
> Ti consigliamo di non utilizzare più dell'80% della capacità di archiviazione SSD per garantire che la suddivisione dei dati su più livelli, la scalabilità del throughput e altre attività di manutenzione funzionino correttamente e che sia disponibile capacità per dati aggiuntivi. Per i file system con scalabilità orizzontale, questo consiglio si applica sia all'utilizzo medio di tutti gli aggregati del file system sia a ogni singolo aggregato.

Per ulteriori informazioni su come viene utilizzata l'archiviazione SSD di un file system e sulla quantità di storage SSD riservata ai metadati dei file e al software operativo, consulta. Scelta della giusta quantità di storage SSD per file system

Monitoraggio dell'utilizzo dello storage SSD

È possibile monitorare l'utilizzo della capacità di archiviazione SSD del file system utilizzando una varietà di strumenti. AWS NetApp Con Amazon CloudWatch puoi monitorare l'utilizzo della capacità di storage e impostare allarmi per avvisarti quando l'utilizzo della capacità di storage raggiunge una soglia personalizzabile.

> **Note**
>
> Ti consigliamo di non superare l'80% di utilizzo della capacità di archiviazione del livello di archiviazione SSD. Ciò garantisce il corretto funzionamento del tiering su più livelli e comporta un sovraccarico per i nuovi dati. Se il livello di archiviazione SSD è costantemente superiore all'80% di utilizzo della capacità di archiviazione, è possibile aumentare la capacità del livello di archiviazione SSD. Per ulteriori informazioni, consulta Aggiornamento dello storage SSD e degli IOPS del file system.

Puoi visualizzare lo storage SSD disponibile di un file system e la distribuzione complessiva dello storage nella console Amazon FSx. Il grafico della capacità di storage SSD disponibile mostra la

quantità di capacità di storage SSD disponibile su un file system nel tempo. Il grafico di distribuzione dello storage mostra come la capacità di archiviazione complessiva di un file system sia attualmente distribuita in 3 categorie:

- Livello del pool di capacità
- Livello SSD: disponibile
- Livello SSD: usato

È possibile monitorare l'utilizzo della capacità di archiviazione SSD del file system in AWS Management Console, utilizzando la procedura seguente.

Per monitorare la capacità di storage disponibile a livello SSD (console) del file system

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli File system nella colonna di navigazione a sinistra, quindi scegli il ONTAP file system per cui desideri visualizzare le informazioni sulla capacità di storage. Viene visualizzata la pagina dei dettagli del file system.
3. Nel secondo pannello, scegli la scheda Monitoraggio e prestazioni, quindi scegli Archiviazione. Vengono visualizzati i grafici della capacità di archiviazione principale disponibile e dell'utilizzo della capacità di archiviazione per aggregato.

Creazione di un allarme sull'utilizzo della capacità di archiviazione del file system

Si consiglia di non superare un utilizzo medio della capacità di archiviazione SSD dell'80% su base continuativa. Sono accettabili picchi occasionali di utilizzo dello storage SSD superiori all'80%. Il mantenimento di un utilizzo medio inferiore all'80% offre una capacità sufficiente per aumentare lo storage senza riscontrare problemi. La procedura seguente mostra come creare un CloudWatch allarme che avvisi l'utente quando l'utilizzo dello storage SSD del file system si avvicina all'80%.

Per creare un allarme SCU del file system

È possibile utilizzare la `StorageCapacityUtilization` metrica per creare un allarme che viene attivato quando uno o più file system FSx for ONTAP hanno raggiunto una soglia di utilizzo dello storage.

1. Aprire la console all'indirizzo https://console.aws.amazon.com/cloudwatch/. CloudWatch

2. Nel riquadro di navigazione a sinistra, in Allarmi, scegli Tutti gli allarmi. Quindi, scegli Crea allarme. Nella procedura guidata per la creazione di un allarme, scegli Seleziona metrica.
3. Nell'esploratore di grafici, scegli la scheda Query da più sorgenti.
4. Nel generatore di query, scegliete quanto segue:
   - Per Namespace, seleziona AWS/FSX > Metriche dettagliate del file system.
   - Per il nome della metrica, selezionate MAX (). StorageCapacityUtilization
   - Per Filtra per, puoi facoltativamente includere o escludere file system specifici in base al loro ID. Se lasci il campo Filter by vuoto, l'allarme si attiverà quando uno dei tuoi file system supera la soglia di utilizzo della capacità di archiviazione dell'allarme.
   - Lascia vuote le altre opzioni e scegli Graph query.
5. Scegli Select Metric (Seleziona parametro). Tornando alla procedura guidata, nella sezione Metrica, assegna un'etichetta alla metrica. Ti consigliamo di mantenere il Periodo a 5 minuti.
6. In Condizioni, scegli il tipo di soglia statica, ogni volta che la metrica è maggiore/uguale a 80.
7. Scegli Avanti per andare alla pagina Configura azioni.

Per configurare le azioni di allarme

È possibile configurare una serie di azioni da attivare quando l'allarme raggiunge la soglia configurata. In questo esempio, abbiamo scelto un argomento Simple Notification Service (SNS), ma puoi scoprire altre azioni in Using Amazon CloudWatch alarms nella Amazon User Guide. CloudWatch

1. Nella sezione Notifiche, scegli un argomento SNS a cui inviare una notifica quando l'allarme è attivo. `ALARM` Puoi scegliere un argomento esistente o crearne uno nuovo. Riceverai una notifica di iscrizione che dovrai confermare prima di ricevere notifiche di allarme all'indirizzo email.
2. Seleziona Successivo.

Per terminare l'allarme

Segui queste istruzioni per completare il processo di creazione della CloudWatch sveglia.

1. Nella pagina Aggiungi nome e descrizione, assegna un nome e, facoltativamente, una descrizione alla sveglia, quindi scegli Avanti.
2. Controlla tutto ciò che hai configurato nella pagina di anteprima e creazione, quindi scegli Crea allarme.

Visualizzazione dei risparmi sull'efficienza dello storage

Se abilitata, puoi vedere quanta capacità di storage stai risparmiando nella console Amazon FSx, nella CloudWatch console Amazon e nella CLI ONTAP.

Per visualizzare i risparmi in termini di efficienza dello storage (console)

I risparmi in termini di efficienza di storage visualizzati nella console Amazon FSx per un file system FSx for ONTAP includono i risparmi derivanti da e. FlexClones SnapShots

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli il file system FSx for ONTAP per il quale desideri visualizzare il risparmio in termini di efficienza di storage dall'elenco dei file system.
3. Scegliete Riepilogo nella scheda Monitoraggio e prestazioni nel secondo pannello nella pagina dei dettagli del file system.
4. Il grafico sui risparmi in termini di efficienza dello storage mostra lo spazio risparmiato in percentuale della dimensione dei dati logici e in byte fisici.

Per visualizzare i risparmi in termini di efficienza dello storage (ONTAPCLI)

È possibile ottenere risparmi in termini di efficienza dello storage solo grazie alla compattazione, alla compressione e alla deduplicazione, senza gli effetti delle istantanee, eseguendo il FlexClones comando `storage aggregate show-efficiency` tramite la CLI. ONTAP Per ulteriori informazioni, consulta Storage Aggregate Show-efficiency nel Documentation Center. NetApp ONTAP

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.
2. Il storage aggregate show-efficiency comando visualizza informazioni sull'efficienza di archiviazione di tutti gli aggregati. L'efficienza di archiviazione viene visualizzata su quattro diversi livelli:

   - Totale

- Aggregazione
- Volume
- Istantanea e volume FlexClone

```
::*> aggr show-efficiency

Aggregate: aggr1
     Node: node1

Total Data Reduction Efficiency Ratio:  3.29:1
Total Storage Efficiency Ratio:         4.29:1
Aggregate: aggr2
     Node: node1

Total Data Reduction Efficiency Ratio:  4.50:1
Total Storage Efficiency Ratio:         5.49:1

cluster::*> aggr show-efficiency -details

Aggregate: aggr1
     Node: node1

Total Data Reduction Ratio:                   2.39:1
Total Storage Efficiency Ratio:               4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:              5.03:1
Compression Efficiency:                       1.00:1

Snapshot Volume Storage Efficiency:           8.81:1
FlexClone Volume Storage Efficiency:          1.00:1
Number of Efficiency Disabled Volumes:        1

Aggregate: aggr2
     Node: node1
Total Data Reduction Ratio:                   2.39:1
Total Storage Efficiency Ratio:               4.29:1

Aggregate level Storage Efficiency
```

```
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:               5.03:1
Compression Efficiency:                        1.00:1

Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1
```

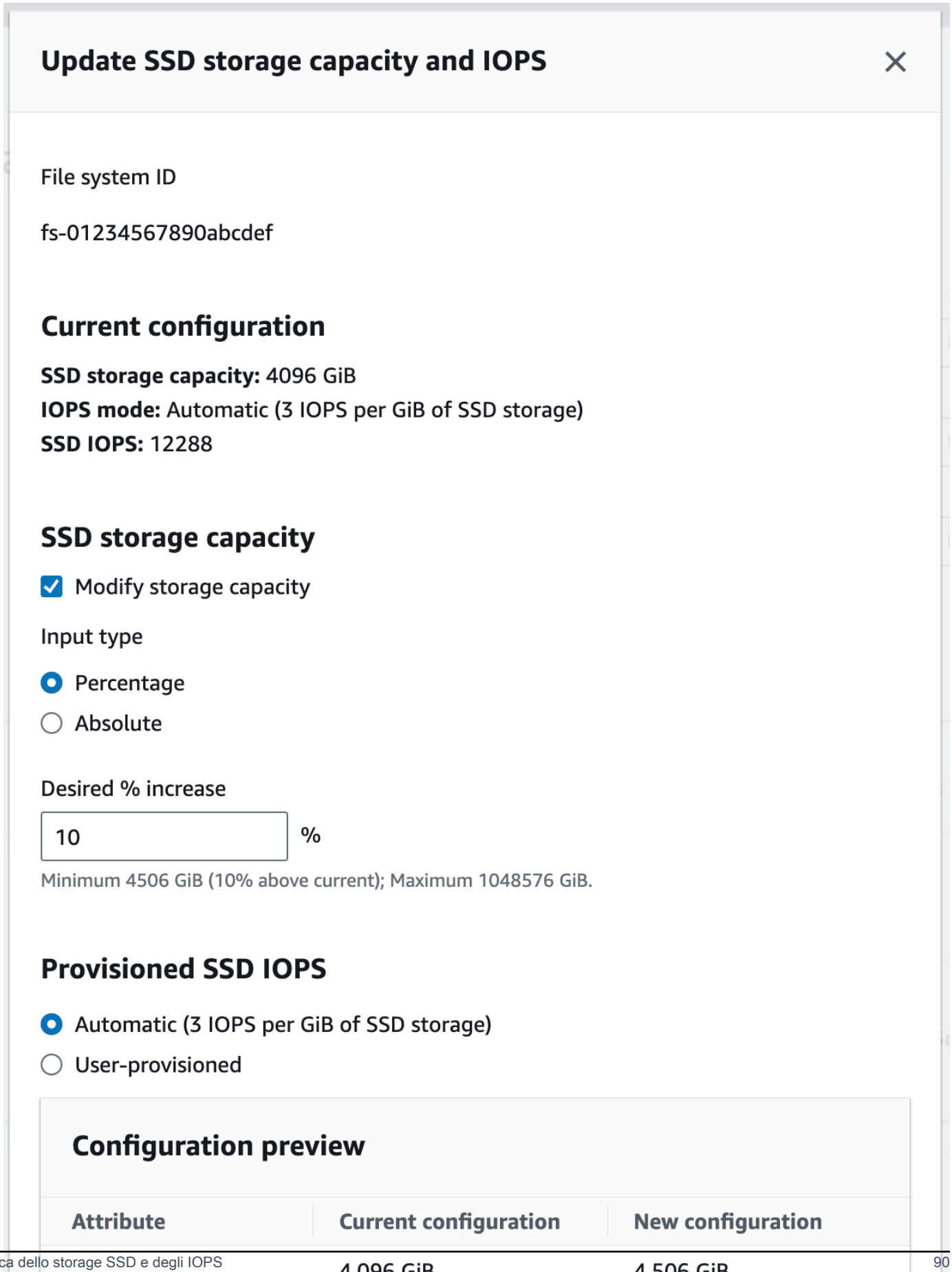
Modifica della capacità di archiviazione SSD e degli IOPS assegnati

Puoi aumentare lo storage basato su SSD di un file system e aumentare o diminuire la quantità di IOPS SSD assegnati utilizzando la console Amazon FSx, l'API e l'API. AWS CLI

Per aggiornare la capacità di archiviazione SSD o effettuare il provisioning degli IOPS per un file system (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione a sinistra, scegli File system. Nell'elenco File system, selezionare il file system FSx for ONTAP per cui si desidera aggiornare la capacità di archiviazione SSD e gli IOPS SSD.
3. Scegliete Azioni > Aggiorna la capacità di archiviazione. Oppure, nella sezione Riepilogo, scegli Aggiorna accanto al valore della capacità di archiviazione SSD del file system.

   Viene visualizzata la finestra di dialogo Aggiorna capacità di archiviazione SSD e IOPS.


Update SSD storage capacity and IOPS
File system ID
fs-01234567890abcdef
Current configuration
SSD storage capacity: 4096 GiB
IOPS mode: Automatic (3 IOPS per GiB of SSD storage)
SSD IOPS: 12288
SSD storage capacity
Modify storage capacity
Input type
Percentage
Absolute
Desired % increase
10
%
Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.
Provisioned SSD IOPS
Automatic (3 IOPS per GiB of SSD storage)
User-provisioned
Configuration preview
Attribute
Current configuration
New configuration
SSD storage capacity
4,096 GiB
(2,048 GiB per HA pair)
4,506 GiB
(2,253 GiB per HA pair)
Mode: Automatic
Mode: Automatic

4. Per aumentare la capacità di archiviazione SSD, scegli Modifica capacità di archiviazione.
5. Per Tipo di input, scegli una delle seguenti opzioni:
   - Per inserire la nuova capacità di archiviazione SSD come variazione percentuale rispetto al valore corrente, scegli Percentuale.
   - Per inserire il nuovo valore in GiB, scegli Absolute.
6. A seconda del tipo di input, inserisci un valore per l'aumento percentuale desiderato.
   - Per Percentuale, inserisci il valore di aumento percentuale. Questo valore deve essere almeno il 10 percento superiore al valore corrente.
   - Per Absolute, inserisci il nuovo valore in GiB, fino al valore massimo consentito di 196.608 GiB.
7. Per Provisioned SSD IOPS, sono disponibili due opzioni per modificare il numero di IOPS SSD assegnati per il file system:
   - Se desideri che Amazon FSx ricalibri automaticamente gli IOPS degli SSD per mantenere 3 IOPS SSD assegnati per GiB di capacità di storage SSD (fino a un massimo di 160.000), scegli Automatic.
   - Se desideri specificare il numero di IOPS SSD, scegli User-provisioned. Inserisci un numero assoluto di IOPS che sia almeno tre volte la quantità di GiB del tuo livello di storage SSD e inferiore o uguale a 160.000.

   > **Note**
   >
   > Per ulteriori informazioni sul numero massimo di IOPS SSD che è possibile fornire per il file system FSx for ONTAP, vedere. Impatto della capacità di throughput sulle prestazioni

8. Scegli Aggiorna.

   > **Note**
   >
   > Nella parte inferiore del prompt, viene mostrata un'anteprima della configurazione per la nuova capacità di archiviazione SSD e gli IOPS SSD. Per i file system con scalabilità orizzontale, viene visualizzato anche il valore per coppia HA.

Per aggiornare la capacità di archiviazione SSD e fornire IOPS per un file system (CLI)

Per aggiornare la capacità di archiviazione SSD e gli IOPS assegnati per un file system FSx for ONTAP, utilizzate il AWS CLI comando update-file-systemo l'azione API equivalente. UpdateFileSystem Imposta i seguenti parametri con i tuoi valori:

- `--file-system-id`Imposta l'ID del file system che stai aggiornando.
- Per aumentare la capacità di archiviazione SSD, imposta `--storage-capacity` il valore della capacità di archiviazione di destinazione, che deve essere almeno il 10 percento superiore al valore corrente.
- Per modificare gli IOPS SSD assegnati, utilizza la proprietà. `--ontap-configuration` `DiskIopsConfiguration` Questa proprietà ha due parametri e: `Iops` `Mode`
  - Se si desidera specificare il numero di IOPS assegnati, utilizzare `Iops=`*`number_of_IOPS`* (fino a un massimo di 160.000) e. `Mode=USER_PROVISIONED` Il valore IOPS deve essere maggiore o uguale a tre volte la capacità di archiviazione SSD richiesta. Se non intendi aumentare la capacità di archiviazione, il valore IOPS deve essere maggiore o uguale a tre volte l'attuale capacità di archiviazione SSD.
  - Se desideri che Amazon FSx aumenti automaticamente gli IOPS degli SSD, usa `Mode=AUTOMATIC` e non usa il parametro. `Iops` Amazon FSx manterrà automaticamente 3 IOPS SSD per GiB della capacità di storage SSD fornita (fino a un massimo di 160.000).

> **Note**
>
> Per ulteriori informazioni sul numero massimo di IOPS SSD che è possibile fornire per il file system FSx for ONTAP, vedere. Impatto della capacità di throughput sulle prestazioni

L'esempio seguente aumenta lo storage SSD del file system a 2000 GiB e imposta la quantità di IOPS SSD forniti dall'utente a 7000.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 2000 \
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

Per monitorare lo stato di avanzamento dell'aggiornamento, utilizzare il comando. describe-file-systems AWS CLI Cerca la `AdministrativeActions` sezione nell'output.

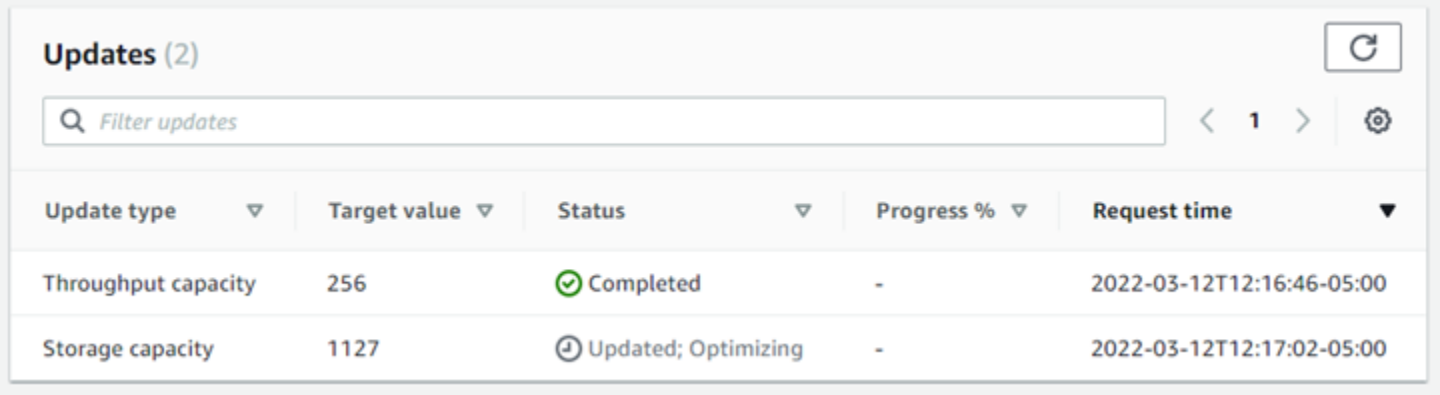
Per ulteriori informazioni, consulta la pagina AdministrativeActiondi riferimento dell'API Amazon FSx for NetApp ONTAP.

Monitoraggio della capacità di storage e degli aggiornamenti IOPS

Puoi monitorare lo stato di avanzamento della capacità di storage SSD e dell'aggiornamento IOPS utilizzando la console Amazon FSx, la CLI e l'API.

Per monitorare lo storage e gli aggiornamenti IOPS (console)

Nella scheda Aggiornamenti della pagina dei dettagli del file system per il file system FSx for ONTAP, è possibile visualizzare i 10 aggiornamenti più recenti per ogni tipo di aggiornamento.



Per quanto riguarda la capacità di archiviazione SSD e gli aggiornamenti IOPS, puoi visualizzare le seguenti informazioni:

Tipo di aggiornamento

I tipi supportati sono Storage capacity, Mode e IOPS. I valori Mode e IOPS sono elencati per tutte le richieste di capacità di archiviazione e scalabilità IOPS.

Target value (Valore target)

Il valore specificato per aggiornare la capacità di archiviazione SSD o IOPS 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.

- Aggiornamento; ottimizzazione: Amazon FSx ha aumentato la capacità di storage SSD del file system. Il processo di ottimizzazione dello storage sta ora riequilibrando i dati in background.
- Completato: l'aggiornamento è stato completato con successo.
- Fallito: la richiesta di aggiornamento non è riuscita. Scegli il punto interrogativo (?) per vedere i dettagli.

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.

Per monitorare lo storage e gli aggiornamenti IOPS (CLI)

È possibile visualizzare e monitorare le richieste di aumento della capacità di archiviazione SSD del file system 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 aumenta la capacità di archiviazione SSD di un file system, vengono generate due `AdministrativeActions` azioni: una `FILE_SYSTEM_UPDATE` e un'`STORAGE_OPTIMIZATIONazione`.

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 la capacità di archiviazione SSD a 2000 GiB e gli IOPS SSD forniti a 7000.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
             }
```

```
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1586797629.095,
        "Status": "PENDING"
    }
]
```

Amazon FSx elabora prima l'`FILE_SYSTEM_UPDATE`azione, aggiungendo i nuovi dischi di storage più grandi 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 comportamento è illustrato nel seguente estratto della risposta di un comando CLI`describe-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 e l'azione non viene più `COMPLETED` visualizzata. `STORAGE_OPTIMIZATION`

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586799169.445,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "ProgressPercent": 41,
        "RequestTime": 1586799169.445,
        "Status": "IN_PROGRESS"
    }
```

```
]
```

Se la capacità di archiviazione o la richiesta di aggiornamento IOPS falliscono, 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": 1586373915.697,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

Aumento dinamico della capacità di archiviazione SSD

È possibile utilizzare la seguente soluzione per aumentare dinamicamente la capacità di archiviazione SSD di un file system FSx for ONTAP quando la quantità di capacità di archiviazione SSD utilizzata supera una soglia specificata. Questo AWS CloudFormation modello distribuisce automaticamente tutti i componenti necessari per definire la soglia di capacità di archiviazione, l' CloudWatch allarme Amazon basato su questa soglia e la AWS Lambda funzione che aumenta la capacità di archiviazione del file system.

La soluzione distribuisce automaticamente tutti i componenti necessari e utilizza i seguenti parametri:

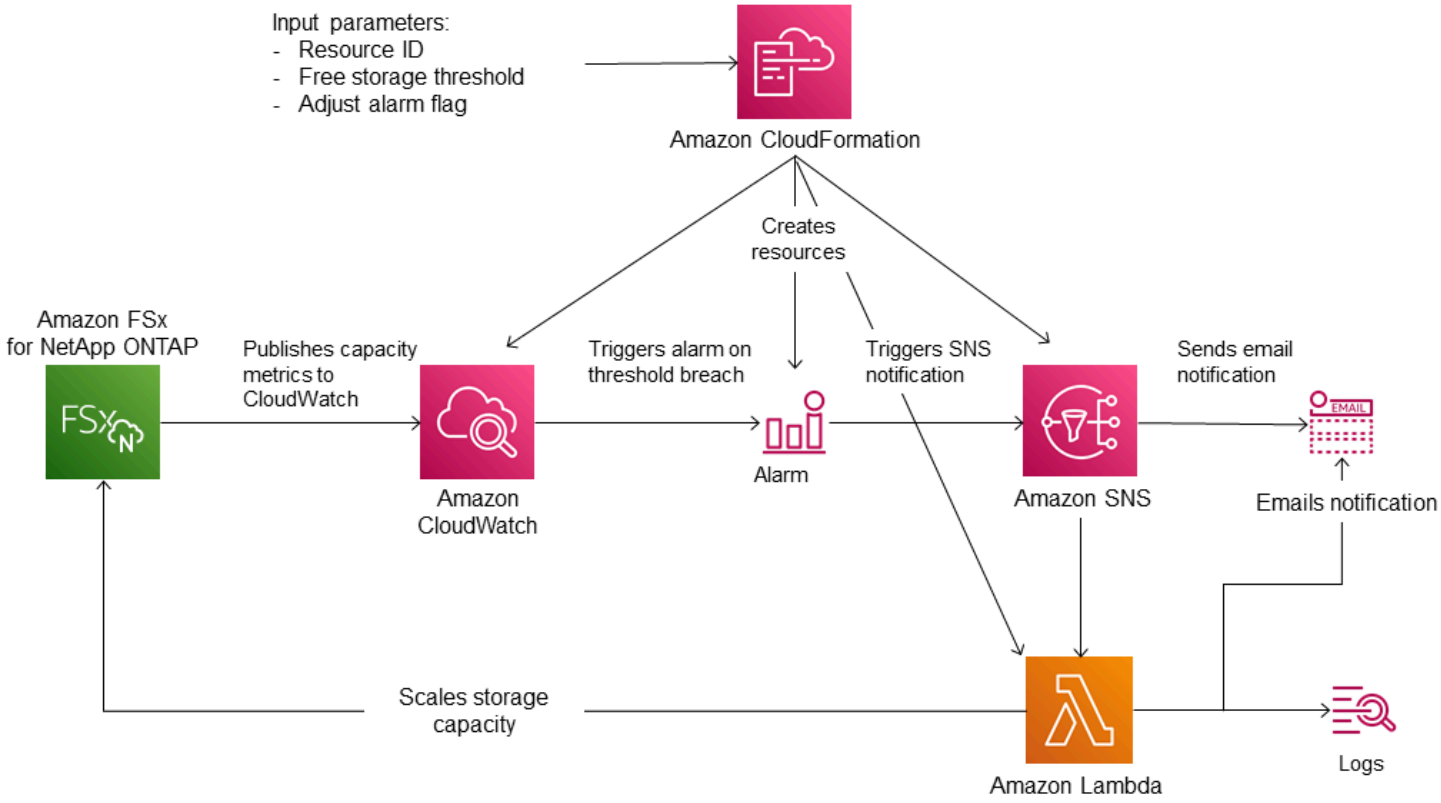
- L'ID del file system FSx for ONTAP.
- La soglia di capacità di archiviazione SSD utilizzata (valore numerico). Questa è la percentuale alla quale verrà CloudWatch attivato l'allarme.

- La percentuale con cui aumentare la capacità di archiviazione (%).
- L'indirizzo e-mail utilizzato per ricevere le notifiche di ridimensionamento.

Argomenti

Panoramica dell'architettura

L'implementazione di questa soluzione consente di creare le seguenti risorse in. Cloud AWS



Il diagramma illustra i passaggi seguenti:

1. Il AWS CloudFormation modello distribuisce un CloudWatch allarme, una AWS Lambda funzione, una coda Amazon Simple Notification Service (Amazon SNS) e tutti i ruoli richiesti (IAM). AWS Identity and Access Management Il ruolo IAM consente alla funzione Lambda di richiamare le operazioni dell'API Amazon FSx.

2. CloudWatch attiva un allarme quando la capacità di storage utilizzata del file system supera la soglia specificata e invia un messaggio alla coda di Amazon SNS. Un allarme viene attivato solo quando la capacità utilizzata del file system supera la soglia ininterrottamente per un periodo di 5 minuti.
3. La soluzione attiva quindi la funzione Lambda sottoscritta a questo argomento di Amazon SNS.
4. La funzione Lambda calcola la nuova capacità di storage del file system in base al valore di aumento percentuale specificato e imposta la nuova capacità di storage del file system.
5. Lo stato di CloudWatch allarme originale e i risultati delle operazioni della funzione Lambda vengono inviati alla coda di Amazon SNS.

Per ricevere notifiche sulle azioni eseguite in risposta all' CloudWatch allarme, devi confermare l'abbonamento all'argomento Amazon SNS seguendo il link fornito nell'e-mail di conferma dell'abbonamento.

AWS CloudFormation modello

Questa soluzione consente AWS CloudFormation di automatizzare l'implementazione dei componenti utilizzati per aumentare automaticamente la capacità di storage di un file system FSx for ONTAP. Per utilizzare questa soluzione, scaricate il modello F. SxOntapDynamicStorageScaling AWS CloudFormation

Il modello utilizza i parametri descritti di seguito. Esaminate i parametri del modello e i relativi valori predefiniti e modificateli in base alle esigenze del file system.

FileSystemId

Nessun valore predefinito. L'ID del file system per il quale si desidera aumentare automaticamente la capacità di archiviazione.

LowFreeDataStorageCapacityThreshold

Nessun valore predefinito. Speciifica la soglia di capacità di archiviazione utilizzata alla quale attivare un allarme e aumentare automaticamente la capacità di archiviazione del file system, specificata in percentuale (%) della capacità di archiviazione corrente del file system. Si ritiene che la capacità di archiviazione disponibile del file system sia scarsa quando lo storage utilizzato supera questa soglia.

EmailAddress

Nessun valore predefinito. Speciifica l'indirizzo e-mail da utilizzare per l'abbonamento SNS e riceve gli avvisi sulla soglia di capacità di archiviazione.

PercentIncrease

L'impostazione predefinita è 20%. Speciifica la quantità di cui aumentare la capacità di archiviazione, espressa come percentuale della capacità di archiviazione corrente.

> **Note**
>
> La scalabilità dello storage viene tentata una volta ogni volta che l' CloudWatch allarme entra nello stato. `ALARM` Se l'utilizzo della capacità di archiviazione SSD rimane al di sopra della soglia dopo un tentativo di scalabilità dello storage, l'operazione di ridimensionamento dello storage non viene più tentata.

MaxF SxSizeinGi B

L'impostazione predefinita è 196608. Speciifica la capacità di archiviazione massima supportata per l'archiviazione SSD.

Implementazione automatizzata con AWS CloudFormation

La procedura seguente configura e implementa uno AWS CloudFormation stack per aumentare automaticamente la capacità di storage di un file system FSx for ONTAP. L'implementazione richiede alcuni minuti. Per ulteriori informazioni sulla creazione di uno CloudFormation stack, consulta Creazione di uno stack sulla AWS CloudFormation console nella Guida per l'AWS CloudFormation utente.

> **Note**
>
> L'implementazione di questa soluzione comporta la fatturazione per i servizi associati. AWS Per ulteriori informazioni, consulta le pagine dei dettagli sui prezzi di tali servizi.

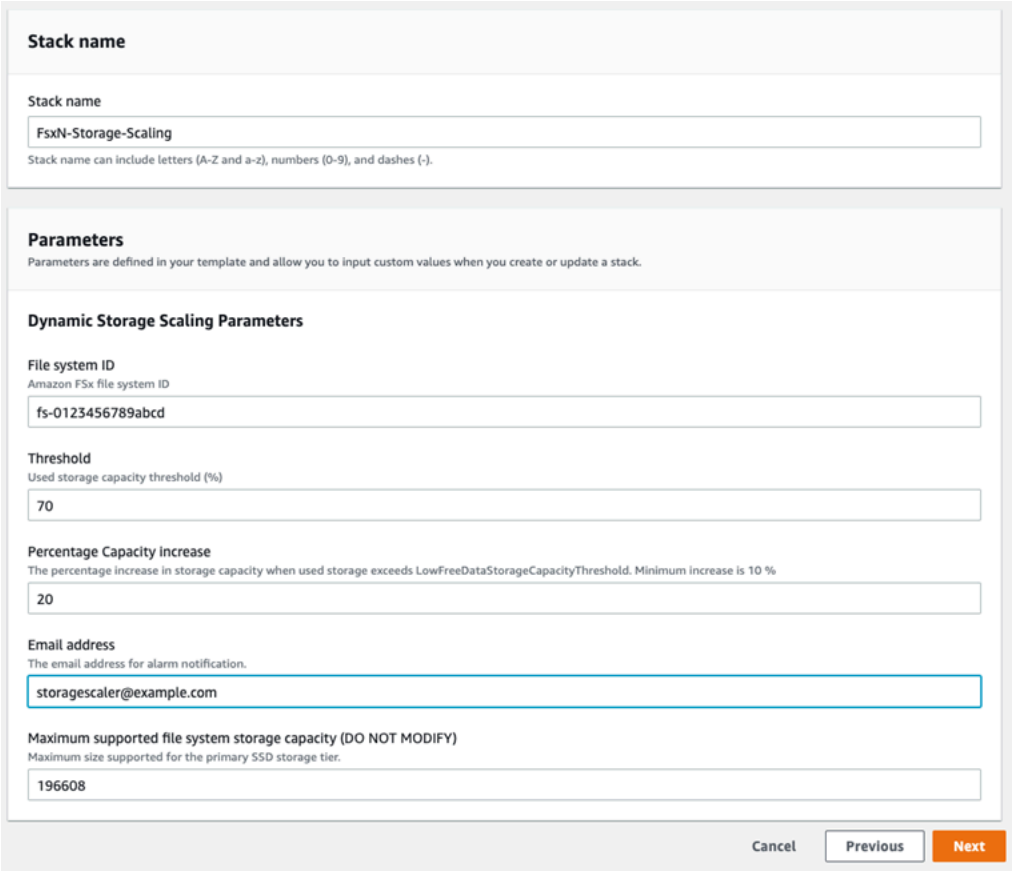
Prima di iniziare, devi avere l'ID del file system Amazon FSx in esecuzione su Amazon Virtual Private Cloud (Amazon VPC) nel tuo. Account AWS Per ulteriori informazioni sulla creazione di risorse Amazon FSx, consulta. Guida introduttiva ad Amazon FSx for ONTAP NetApp

Per lanciare lo stack di soluzioni per l'aumento automatico della capacità di storage

1. Scarica il SxOntapDynamicStorageScaling AWS CloudFormation modello F.

> **Note**
>
> Amazon FSx è attualmente disponibile solo in regioni specifiche AWS . È necessario avviare questa soluzione in una AWS regione in cui è disponibile Amazon FSx. Per ulteriori informazioni, consulta gli endpoint e le quote di Amazon FSx nel. Riferimenti generali di AWS

2. Dalla AWS CloudFormation console, scegli Crea stack > Con nuove risorse.
3. Choose Template è pronto. Nella sezione Specificare il modello, scegli Carica un file modello e carica il modello che hai scaricato.
4. In Specificare i dettagli dello stack, inserisci i valori per la tua soluzione di aumento automatico della capacità di archiviazione.



5. Immettere un nome per lo stack.

6. Per Parametri, esaminate i parametri del modello e modificateli per soddisfare le esigenze del file system. Quindi scegli Successivo.

> **Note**
>
> Per ricevere notifiche e-mail quando viene tentato il ridimensionamento con questo CloudFormation modello, conferma l'e-mail di sottoscrizione SNS che ricevi dopo la distribuzione del modello.

7. Immettete le impostazioni delle opzioni desiderate per la soluzione personalizzata, quindi scegliete Avanti.
8. Per Revisione, rivedi e conferma le impostazioni della soluzione. È necessario selezionare la casella di controllo per confermare che il modello crea risorse IAM.
9. 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 qualche minuto.

Aggiornamento dello stack

Dopo aver creato lo stack, potete aggiornarlo utilizzando lo stesso modello e fornendo nuovi valori per i parametri. Per ulteriori informazioni, consulta Aggiornamento degli stack direttamente nella Guida per l'AWS CloudFormation utente.

Capacità di archiviazione del volume

I volumi FSx for ONTAP sono risorse virtuali utilizzate per raggruppare i dati, determinare come vengono archiviati i dati e determinare il tipo di accesso ai dati. I volumi, come le cartelle, non consumano di per sé la capacità di storage del file system. Solo i dati archiviati in un volume utilizzano lo storage SSD e, a seconda della politica di suddivisione in più livelli del volume, lo storage in pool di capacità. Le dimensioni di un volume vengono impostate al momento della creazione e possono essere modificate in un secondo momento. È possibile monitorare e gestire la capacità di storage dei volumi FSx for ONTAP utilizzando l'API AWS Management Console, AWS CLI and e l'ONTAP CLI.

Argomenti

- Suddivisione dei dati su più livelli

- Istantanee e capacità di archiviazione di volumi
- Capacità dei file di volume
- Aggiornamento della capacità di archiviazione di un volume
- Attivazione del dimensionamento automatico del volume
- Monitoraggio della capacità di archiviazione del volume
- Impostazione della politica di suddivisione in più livelli di un volume
- Impostazione dei giorni minimi di raffreddamento
- Impostazione della politica di recupero nel cloud di un volume
- Visualizzazione della capacità dei file di un volume
- Aumento del numero massimo di file su un volume
- Attivazione della modalità di scrittura su cloud di un volume

Suddivisione dei dati su più livelli

Un file system Amazon FSx for NetApp ONTAP ha due livelli di storage: storage primario e storage con pool di capacità. Lo storage principale è uno storage SSD fornito, scalabile e ad alte prestazioni, creato appositamente per la parte attiva del set di dati. Lo storage con pool di capacità è un livello di storage completamente elastico che può scalare fino a petabyte ed è ottimizzato in termini di costi per i dati a cui si accede raramente.

I dati di ogni volume vengono automaticamente suddivisi su più livelli nel livello di storage del pool di capacità in base alla politica di suddivisione in più livelli, al periodo di raffreddamento e alle impostazioni delle soglie del volume. Le sezioni seguenti descrivono le politiche di suddivisione in più livelli dei ONTAP volumi e le soglie utilizzate per determinare quando i dati vengono trasferiti a più livelli nel pool di capacità.

Politiche di suddivisione in livelli di volume

È possibile determinare come utilizzare i livelli di storage del file system FSx for ONTAP scegliendo la policy di tiering per ogni volume del file system. Scegli la politica di suddivisione in più livelli quando crei un volume e puoi modificarla in qualsiasi momento con la console Amazon FSx AWS CLI, l'API o NetApp utilizzando strumenti di gestione. Puoi scegliere tra una delle seguenti politiche che determinano quali dati, se presenti, vengono suddivisi in livelli per lo storage del pool di capacità.

> **Note**
>
> La suddivisione in più livelli consente di spostare i dati dei file e le istantanee al livello del pool di capacità. Tuttavia, i metadati dei file rimangono sempre a livello SSD. Per ulteriori informazioni, consulta Come viene utilizzata l'archiviazione SSD.

- Automatico: questa policy sposta tutti i dati non disponibili (dati utente e istantanee) al livello del pool di capacità. La velocità di raffreddamento dei dati è determinata dal periodo di raffreddamento della policy, che per impostazione predefinita è 31 giorni, ed è configurabile su valori compresi tra 2 e 183 giorni. Quando i blocchi di dati freddi sottostanti vengono letti in modo casuale (come nel tipico accesso ai file), vengono resi disponibili a caldo e scritti sul livello di storage principale. Quando i blocchi di dati freddi vengono letti in sequenza (ad esempio, mediante una scansione antivirus), rimangono freddi e rimangono sul livello di storage del pool di capacità. Questa è la politica predefinita per la creazione di un volume utilizzando la console Amazon FSx.
- Solo snapshot: questa policy sposta solo i dati delle snapshot nel livello di storage del pool di capacità. La velocità con cui le istantanee vengono trasferite su più livelli nel pool di capacità è determinata dal periodo di raffreddamento della policy, che per impostazione predefinita è impostato su 2 giorni ed è configurabile su valori compresi tra 2 e 183 giorni. Quando i dati delle istantanee fredde vengono letti, vengono resi caldi e scritti sul livello di storage principale. Questa è la politica predefinita per la creazione di un volume utilizzando l' AWS CLI API Amazon FSx o la CLI NetApp ONTAP.
- Tutti: questa policy contrassegna tutti i dati degli utenti e i dati delle istantanee come freddi e li archivia nel livello del pool di capacità. Quando i blocchi di dati vengono letti, rimangono freddi e non vengono scritti sul livello di storage principale. Quando i dati vengono scritti su un volume con la politica All tiering, vengono comunque inizialmente scritti sul livello di storage SSD e vengono suddivisi su più livelli nel pool di capacità tramite un processo in background. Tieni presente che i metadati dei file rimangono sempre sul livello SSD.
- Nessuna: questa politica mantiene tutti i dati del volume sul livello di storage principale e impedisce che vengano spostati su uno storage con pool di capacità. Se si imposta un volume su questa politica dopo aver utilizzato qualsiasi altra politica, i dati esistenti nel volume che si trovava nello storage con pool di capacità vengono spostati nello storage SSD mediante un processo in background, a condizione che l'utilizzo dell'SSD sia inferiore al 90%. Questo processo in background può essere accelerato leggendo intenzionalmente i dati o modificando la politica di recupero dal cloud del volume. Per ulteriori informazioni, consulta Politiche di recupero dal cloud.

Come best practice, durante la migrazione di dati che si prevede di archiviare a lungo termine in pool di capacità di storage, si consiglia di utilizzare la politica di suddivisione automatica sul volume. Con la suddivisione automatica, i dati vengono archiviati sul livello di storage SSD per un minimo di 2 giorni (in base al periodo di raffreddamento del volume) prima di essere trasferiti al livello del pool di capacità. La conservazione dei dati su SSD per almeno 2 giorni consente a ONTAP di eseguire risparmi di compressione e deduplicazione post-elaborazione sui dati, che vengono preservati quando i dati vengono suddivisi su più livelli nel pool di capacità. ONTAP esegue solo la compressione e la deduplicazione post-elaborazione dei dati sullo storage SSD, quindi la selezione di questa policy può aiutarti a massimizzare i risparmi di archiviazione a lungo termine. Puoi anche massimizzare la velocità di trasferimento dei primi backup creati dei tuoi volumi, poiché i dati di cui viene eseguito il backup si trovano su unità di archiviazione SSD.

Per ulteriori informazioni sull'impostazione o la modifica della politica di suddivisione in più livelli di un volume, consulta. Impostazione della politica di suddivisione in più livelli di un volume

Periodo di raffreddamento su più livelli

Il periodo di raffreddamento su più livelli di un volume imposta la quantità di tempo necessaria affinché i dati nel livello SSD vengano contrassegnati come freddi. Il periodo di raffreddamento si applica alle politiche di suddivisione in `Auto` `Snapshot-only` più livelli. È possibile impostare il periodo di raffreddamento su un valore compreso tra 2 e 183 giorni. Per ulteriori informazioni sull'impostazione del periodo di raffreddamento, vedere. Impostazione dei giorni minimi di raffreddamento

I dati vengono archiviati su più livelli 24-48 ore dopo la scadenza del periodo di raffreddamento. Il tiering è un processo in background che consuma risorse di rete e ha una priorità inferiore rispetto alle richieste rivolte ai clienti. Le attività di tiering vengono limitate quando ci sono richieste continue rivolte ai clienti.

Politiche di recupero dal cloud

La policy di recupero dal cloud di un volume stabilisce le condizioni che specificano quando i dati letti dal livello del pool di capacità possono essere promossi al livello SSD. Quando la policy di recupero sul cloud è impostata su un valore diverso da quello`Default`, questa policy ha la precedenza sul comportamento di recupero della policy di tiering del volume. Un volume può avere una delle seguenti politiche di recupero nel cloud:

- Predefinito: questa policy recupera i dati a più livelli in base alla politica di tiering sottostante del volume. Questa è la policy di recupero cloud predefinita per tutti i volumi.

- Mai: questa policy non recupera mai dati a più livelli, indipendentemente dal fatto che le letture siano sequenziali o casuali. È simile all'impostazione della politica di tiering del volume su Tutti, tranne per il fatto che è possibile utilizzarla con altre politiche, Auto, solo Snapshot, per suddividere i dati in base al periodo di raffreddamento minimo anziché immediato.
- In lettura: questa policy recupera i dati a più livelli per tutte le letture dei dati basate sul client. Questa politica non ha effetto quando si utilizza la politica All tiering.
- Promuovi: questa policy contrassegna tutti i dati di un volume presenti nel pool di capacità per il recupero sul livello SSD. I dati vengono contrassegnati alla successiva esecuzione dello scanner giornaliero a più livelli in background. Questa policy è utile per le applicazioni con carichi di lavoro ciclici che vengono eseguiti raramente, ma che richiedono prestazioni di livello SSD quando vengono eseguite. Questa politica non ha effetto quando si utilizza la politica All tiering.

Per informazioni sull'impostazione della politica di recupero nel cloud di un volume, consulta. Impostazione della politica di recupero nel cloud di un volume

Soglie di suddivisione in più livelli

L'utilizzo della capacità di archiviazione SSD di un file system determina la modalità di ONTAP gestione del comportamento di suddivisione in più livelli per tutti i volumi. In base all'utilizzo della capacità di archiviazione SSD di un file system, le seguenti soglie impostano il comportamento del tiering su più livelli come descritto. Per informazioni su come monitorare l'utilizzo della capacità del livello di archiviazione SSD di un volume, vedere. Monitoraggio della capacità di archiviazione del volume

> **Note**
>
> Ti consigliamo di non superare l'80% di utilizzo della capacità di archiviazione del livello di archiviazione SSD. Per i file system con scalabilità orizzontale, questa raccomandazione si applica sia all'utilizzo medio totale di tutti gli aggregati del file system sia all'utilizzo di ogni singolo aggregato. Ciò garantisce il corretto funzionamento del tiering su più livelli e comporta un sovraccarico per i nuovi dati. Se il livello di archiviazione SSD è costantemente superiore all'80% di utilizzo della capacità di archiviazione, è possibile aumentare la capacità del livello di archiviazione SSD. Per ulteriori informazioni, consulta Aggiornamento dello storage SSD e degli IOPS del file system.

FSx for ONTAP utilizza le seguenti soglie di capacità di storage per gestire il tiering sui volumi:

- <= 50% di utilizzo del livello di storage SSD: a questa soglia, il livello di storage SSD è considerato sottoutilizzato e solo i volumi che utilizzano la politica All tiering dispongono di uno storage dei dati su più livelli in base al pool di capacità. I volumi con policy Auto e Snapshot non suddividono i dati in livelli superiori a questa soglia.
- > 50% di utilizzo del livello di storage SSD: i volumi con politiche di tiering Auto e Snapshot suddividono i dati in base all'impostazione dei giorni di raffreddamento minimi su più livelli. L'impostazione predefinita è 31 giorni.
- >= 90% di utilizzo del livello di storage SSD: a questa soglia, Amazon FSx dà la priorità alla conservazione dello spazio nel livello di storage SSD. I dati non disponibili provenienti dal livello del pool di capacità non vengono più spostati nel livello di storage SSD quando vengono letti per volumi utilizzando le policy Auto e Snapshot.
- >= 98% di utilizzo del livello di storage SSD: tutte le funzionalità di tiering si interrompono quando il livello di storage SSD raggiunge o supera il 98% di utilizzo. È possibile continuare a leggere dai livelli di storage, ma non è possibile scrivere sui livelli.

Istantanee e capacità di archiviazione di volumi

Un'istantanea è un'immagine di sola lettura di un volume Amazon FSx for NetApp ONTAP in un determinato momento. Le istantanee offrono protezione contro l'eliminazione o la modifica accidentale dei file nei volumi. Con le istantanee, gli utenti possono visualizzare e ripristinare facilmente singoli file o cartelle da un'istantanea precedente.

Le istantanee vengono archiviate insieme ai dati del file system e consumano la capacità di archiviazione del file system. Tuttavia, le istantanee consumano la capacità di archiviazione solo per le porzioni di file che sono state modificate dall'ultima istantanea. Le istantanee non sono incluse nei backup dei volumi del file system.

Le istantanee sono abilitate per impostazione predefinita sui volumi, utilizzando la politica di snapshot predefinita. Le istantanee vengono archiviate nella `.snapshot` directory alla radice di un volume. È possibile gestire la capacità di archiviazione dei volumi per le istantanee nei seguenti modi:

- Politiche snapshot: seleziona una policy snapshot integrata o scegli una policy personalizzata che hai creato nella CLI ONTAP o nell'API REST.
- Eliminazione manuale delle istantanee: recupera la capacità di archiviazione eliminando le istantanee manualmente.
- Crea una politica di eliminazione automatica delle istantanee: crea una politica che elimini più istantanee rispetto alla politica di eliminazione automatica delle istantanee predefinita.

- Disattiva le istantanee automatiche: conserva la capacità di archiviazione disattivando le istantanee automatiche.

Per ulteriori informazioni, consulta Utilizzo degli snapshot.

Capacità dei file di volume

I volumi Amazon FSx for NetApp ONTAP dispongono di puntatori di file che vengono utilizzati per archiviare metadati di file come nome del file, ora dell'ultimo accesso, autorizzazioni, dimensioni e per fungere da puntatori a blocchi di dati. Questi puntatori di file sono chiamati inode e ogni volume ha una capacità limitata per il numero di inode, chiamata capacità del file di volume. Quando un volume si sta esaurendo o esaurisce i file disponibili (inode), non è possibile scrivere dati aggiuntivi su quel volume.

Il numero di oggetti del file system (file, directory, copie istantanee) che un volume può contenere è determinato dal numero di inode che contiene. Il numero di inode in un volume aumenta proporzionalmente alla capacità di archiviazione del volume (e al numero di componenti del volume per i volumi). FlexGroup Per impostazione predefinita, FlexVol i volumi (o FlexGroup componenti) con una capacità di archiviazione di 648 GiB o più hanno tutti lo stesso numero di inode: 21.251.126. Se si crea un volume più grande di 648 GiB e si desidera che contenga più di 21.251.126 inode, è necessario aumentare manualmente il numero massimo di inode (file). Per ulteriori informazioni sulla visualizzazione del numero massimo di file per un volume, vedere. Visualizzazione della capacità dei file di un volume

Il numero predefinito di inode su un volume è 1 inode per ogni 32 KB di capacità di archiviazione del volume, fino a una dimensione del volume di 648 GiB. Per un volume da 1 GiB:

Volume_size_in_bytes × (1 file ÷ inode_size_in_bytes) = numero_massimo_di_file

1.073.741.824 byte × (1 file ÷ 32.768 byte) = 32.768 file

È possibile aumentare il numero massimo di inode che un volume può contenere, fino a un massimo di 1 inode per ogni 4 KB di capacità di archiviazione. Per un volume da 1 GiB. questo aumenta il numero massimo di inode o file da 32.768 a 262.144:

1.073.741.824 byte × (1 file ÷ 4096 byte) = 262.144 file

Un volume FSx for ONTAP può contenere un massimo di 2 miliardi di inode.

Per informazioni sulla modifica del numero massimo di file che un volume può archiviare, vedere. Aumento del numero massimo di file su un volume

Aggiornamento della capacità di archiviazione di un volume

È possibile gestire la capacità di storage dei volumi aumentando o diminuendo manualmente le dimensioni del volume utilizzando l'API AWS Management Console, AWS CLI e l'ONTAP CLI. È inoltre possibile abilitare il dimensionamento automatico del volume in modo che la dimensione del volume aumenti o si riduca automaticamente quando raggiunge determinate soglie di capacità di storage utilizzate. È possibile utilizzare la CLI ONTAP per gestire il dimensionamento automatico dei volumi.

Per modificare la capacità di archiviazione di un volume (console)

- Puoi aumentare o diminuire la capacità di storage di un volume utilizzando la console e l'API Amazon FSx. AWS CLI Per ulteriori informazioni, consulta Aggiornamento di un volume.

È inoltre possibile utilizzare la ONTAP CLI per modificare la capacità di archiviazione di un volume utilizzando il `volume modify`comando.

Per modificare le dimensioni di un volume (ONTAP CLI)

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.
2. Utilizza il comando volume modify ONTAP CLI per modificare la capacità di archiviazione di un volume. Esegui il comando seguente, utilizzando i tuoi dati al posto dei seguenti valori:

   - Sostituisci *`svm_name`*con il nome della macchina virtuale di archiviazione (SVM) su cui viene creato il volume.
   - Sostituisci *`vol_name`*con il nome del volume che desideri ridimensionare.
   - Sostituiscilo *`vol_size`*con la nuova dimensione del volume nel formato *`integer`*`[KB|MB|GB|TB|PB]`, `100GB` ad esempio per aumentare la dimensione del volume a 100 gigabyte.

```
::> volume modify -vserver svm_name -volume vol_name -size vol_size
```

Attivazione del dimensionamento automatico del volume

Dimensionamento automatico del volume in modo che il volume cresca automaticamente fino a una dimensione specificata quando raggiunge una soglia di spazio utilizzata. È possibile eseguire questa operazione per i tipi di FlexVol volume (il tipo di volume predefinito per FSx for ONTAP) utilizzando il comando ONTAP `volume autosize`CLI.

Per abilitare il dimensionamento automatico dei volumi (ONTAP CLI)

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *management_endpoint_ip* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.
2. Utilizzate il `volume autosize` comando come illustrato, sostituendo i seguenti valori:

   - Sostituisci *svm_name*con il nome della SVM su cui viene creato il volume.
   - Sostituisci *vol_name*con il nome del volume che desideri ridimensionare.
   - Sostituisci *grow_threshold*con un valore percentuale di spazio utilizzato (ad esempio`90`) in base al quale il volume aumenterà automaticamente di dimensione (fino al *max_size*valore).
   - Sostituiscilo *max_size*con la dimensione massima che il volume può raggiungere. Usa il formato *integer*`[KB|MB|GB|TB|PB]`, ad esempio`300TB`. La dimensione massima è 300 TB. L'impostazione predefinita è il 120% della dimensione del volume.
   - Sostituisci *min_size* con la dimensione minima a cui verrà ridotto il volume. *Utilizzate lo stesso formato di max_size.*
   - Sostituite *shrink_threshold* con la percentuale di spazio utilizzata alla quale il volume si ridurrà automaticamente di dimensione.

```
::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -
grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-
percent shrink_threshold -minimum-size min_size
```

Monitoraggio della capacità di archiviazione del volume

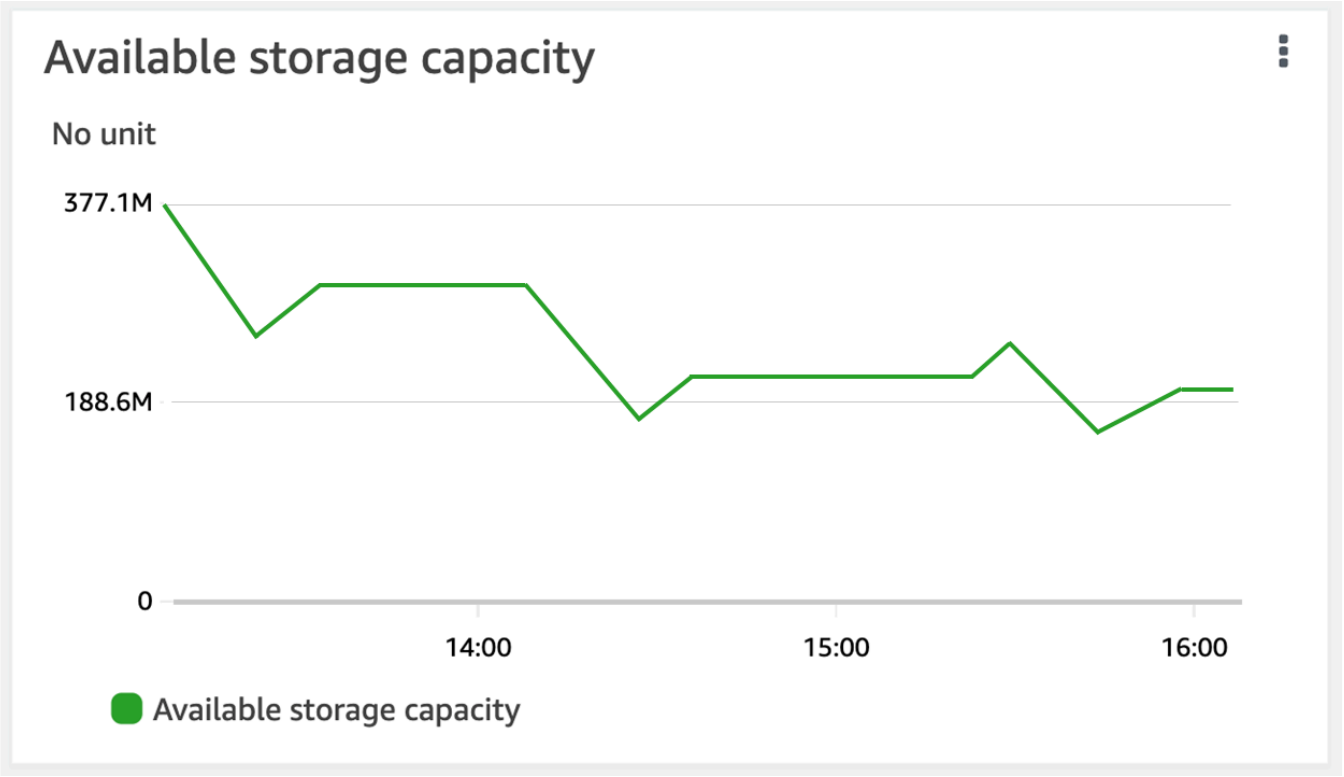
Puoi visualizzare lo spazio di archiviazione disponibile di un volume e la sua distribuzione di storage in AWS Management Console e nella AWS CLI CLI di NetApp ONTAP.

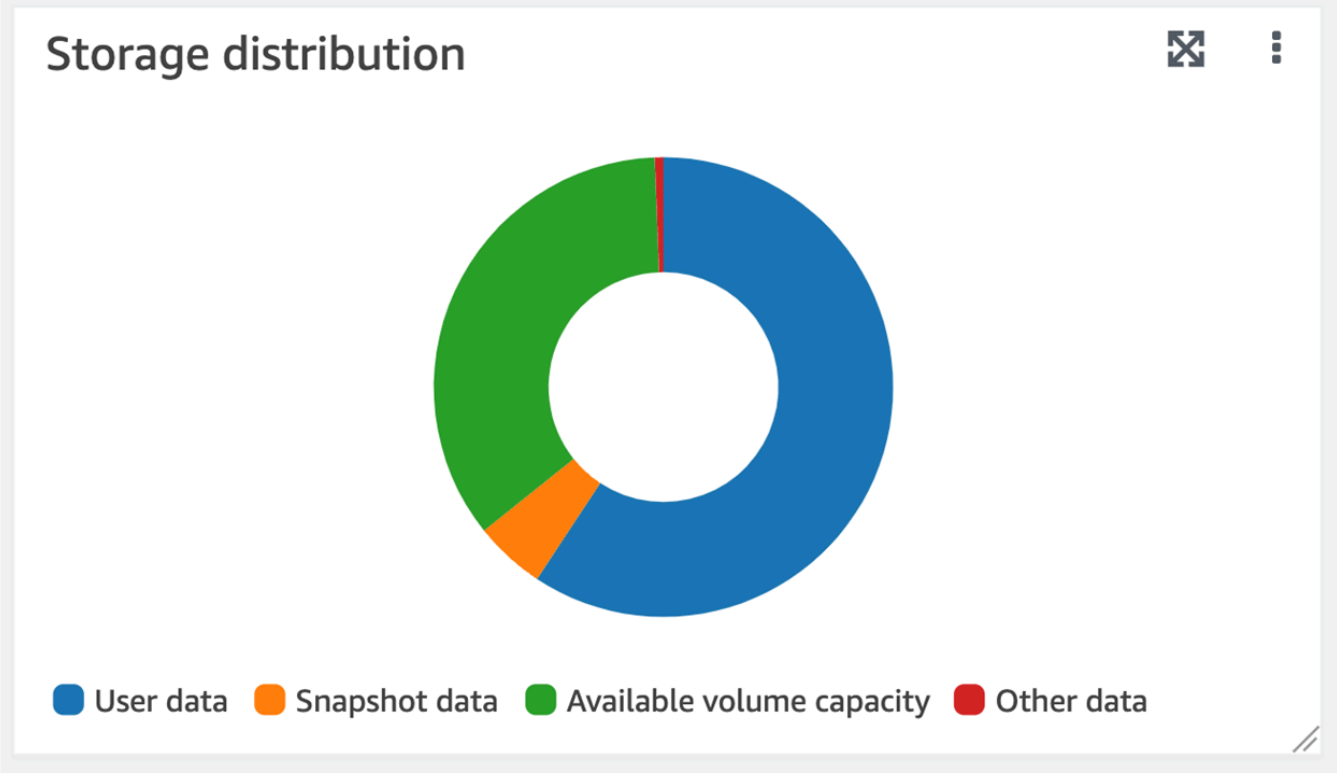
Per monitorare la capacità di archiviazione di un volume (console)

Il grafico di archiviazione disponibile mostra la quantità di capacità di archiviazione gratuita su un volume nel tempo. Il grafico di distribuzione dello storage mostra come la capacità di archiviazione di un volume è attualmente distribuita in 4 categorie:

- Dati utente
- Dati delle istantanee
- Capacità di volume disponibile
- Altri dati

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli Volumes nella colonna di navigazione a sinistra, quindi scegli il volume ONTAP per cui desideri visualizzare le informazioni sulla capacità di storage. Viene visualizzata la pagina dei dettagli del volume.
3. Nel secondo pannello, scegli la scheda Monitoraggio. Vengono visualizzati i grafici di archiviazione disponibile e di distribuzione dello spazio di archiviazione, insieme a molti altri grafici.


Available storage capacity
No unit
377.1M
188.6M
0
14:00
15:00
16:00
Available storage capacity


Storage distribution
User data
Snapshot data
Available volume capacity
Other data

Per monitorare la capacità di archiviazione di un volume (ONTAPCLI)

È possibile monitorare come viene consumata la capacità di archiviazione del volume utilizzando il comando `volume show-space` ONTAP CLI. Per ulteriori informazioni, consulta `volume show-space`il NetApp ONTAP Documentation Center.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Visualizza l'utilizzo della capacità di archiviazione di un volume eseguendo il comando seguente, che sostituisce i seguenti valori:

   - Sostituisci *`svm_name`*con il nome della SVM su cui è stato creato il volume.
   - Sostituisci *`vol_name`*con il nome del volume per il quale stai impostando la politica di suddivisione dei dati su più livelli.

   ```
   ::> volume show-space -vserver svm_name -volume vol_name
   ```

   Se il comando ha esito positivo, verrà visualizzato un output simile al seguente:

   ```
   Vserver : svm_name
   Volume  : vol_name
   Feature                                     Used      Used%
   --------------------------------     ----------     ------
   User Data                                  140KB         0%
   Filesystem Metadata                      164.4MB         1%
   Inodes                                   10.28MB         0%
   Snapshot Reserve                         563.2MB         5%
   Deduplication                               12KB         0%
   Snapshot Spill                            9.31GB        85%
   Performance Metadata                       668KB         0%

   Total Used                               10.03GB        91%
   ```

```
Total Physical Used                          10.03GB        91%
```

L'output di questo comando mostra la quantità di spazio fisico occupata da diversi tipi di dati su questo volume. Mostra anche la percentuale della capacità totale del volume consumata da ogni tipo di dati. In questo esempio, `Snapshot Spill` `Snapshot Reserve` consumano complessivamente il 90 percento della capacità del volume.

`Snapshot Reserve`mostra la quantità di spazio su disco riservata alla memorizzazione delle copie istantanee. Se lo spazio di archiviazione delle copie istantanee supera lo spazio di riserva, viene riversato nel file system e tale quantità è mostrata sotto. `Snapshot Spill`

Per aumentare la quantità di spazio disponibile, è possibile aumentare la dimensione del volume oppure eliminare le istantanee che non si utilizzano, come illustrato nelle procedure seguenti.

Per i tipi di FlexVol volume (il tipo di volume predefinito per i volumi FSx for ONTAP), puoi anche abilitare il dimensionamento automatico del volume. Quando si abilita il dimensionamento automatico, la dimensione del volume aumenta automaticamente quando raggiunge determinate soglie. È inoltre possibile disabilitare le istantanee automatiche. Entrambe queste funzionalità sono illustrate nelle sezioni seguenti.

Impostazione della politica di suddivisione in più livelli di un volume

Puoi modificare la politica di suddivisione in più livelli di un volume utilizzando l'API AWS Management Console, AWS CLI and e l'ONTAP CLI.

Per modificare la politica di suddivisione in più livelli dei dati di un volume (console)

Utilizzare la procedura seguente per modificare la politica di suddivisione dei dati su più livelli di un volume utilizzando. AWS Management Console

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli Volumes nel riquadro di navigazione a sinistra, quindi scegli il volume ONTAP per il quale desideri modificare la politica di data-tiering.
3. Scegli Aggiorna volume dal menu a discesa Azioni. Viene visualizzata la finestra Aggiorna volume.
4. Per la politica di suddivisione in più livelli del pool di capacità, scegli la nuova politica per il volume. Per ulteriori informazioni, consulta Politiche di suddivisione in livelli di volume.
5. Scegli Aggiorna per applicare la nuova politica al volume.

Per impostare la politica di tiering (CLI) di un volume

- Modifica la politica di suddivisione in più livelli di un volume utilizzando il comando CLI update-volume (UpdateVolumeè l'azione equivalente dell'API Amazon FSx). Il seguente esempio di comando CLI imposta la politica di tiering dei dati di un volume su. SNAPSHOT_ONLY

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

In caso di richiesta riuscita, il sistema risponde con la descrizione del volume.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 2,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

Per modificare la politica di suddivisione in più livelli di un volume (ONTAP CLI)

È possibile utilizzare il comando `volume modify` ONTAP CLI per impostare la politica di tiering di un volume. Per ulteriori informazioni, consulta il Centro di `volume modify`documentazione NetApp ONTAP.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Accedere alla modalità avanzata CLI di ONTAP utilizzando il seguente comando.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Utilizzate il comando seguente per modificare la politica di suddivisione in più livelli dei dati del volume, sostituendo i seguenti valori:

   - Sostituire *`svm_name`*con il nome della SVM su cui viene creato il volume.
   - Sostituisci *`vol_name`*con il nome del volume per il quale stai impostando la politica di suddivisione dei dati su più livelli.
   - Sostituire *`tiering_policy`*con la politica desiderata. I valori validi sono `snapshot-only`, `auto`, `all` o `none`. Per ulteriori informazioni, consulta Politiche di suddivisione in livelli di volume.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -tiering-
   policy tiering_policy
   ```

Impostazione dei giorni minimi di raffreddamento

I giorni di raffreddamento minimi per un volume impostano la soglia utilizzata per determinare quali dati sono caldi e quali sono freddi. Puoi impostare i giorni di raffreddamento minimi di un volume utilizzando un'API AWS CLI e l'ONTAP CLI.

Per impostare i giorni di raffreddamento minimi di un volume (CLI)

- Modifica la configurazione di un volume utilizzando il comando update-volume CLI (è l'azione equivalente UpdateVolumedell'API Amazon FSx). Il seguente esempio di comando CLI imposta un volume `CoolingPeriod` su 104 giorni.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration
 TieringPolicy={CoolingPeriod=104}
```

  Il sistema risponde con la descrizione del volume per una richiesta riuscita.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 104,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
```

```
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

Per impostare i giorni di raffreddamento minimi di un volume (ONTAP CLI)

Utilizza il comando `volume modify` ONTAP CLI per impostare il numero minimo di giorni di raffreddamento per un volume esistente. Per ulteriori informazioni, consulta il Centro di `volume modify`documentazione NetApp ONTAP.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Accedere alla modalità avanzata CLI di ONTAP utilizzando il seguente comando.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Utilizzate il comando seguente per modificare i giorni minimi di raffreddamento del volume, sostituendo i seguenti valori:

   - Sostituisci *`svm_name`*con il nome della SVM su cui è stato creato il volume.
   - Sostituisci *`vol_name`*con il nome del volume per il quale stai impostando i giorni di raffreddamento.
   - Sostituire *`cooling_days`* con il valore desiderato, un numero intero compreso tra 2 e 183.

```
FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-
days cooling_days
```

Il sistema risponde come segue in caso di richiesta andata a buon fine.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Impostazione della politica di recupero nel cloud di un volume

Utilizza il comando `volume modify` ONTAP CLI per impostare la policy di recupero dal cloud per un volume esistente. Per ulteriori informazioni, consulta l'ONTAP `volume modify`Documentation Center NetApp .

Per impostare la policy di recupero nel cloud di un volume (ONTAP CLI)

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *management_endpoint_ip* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Accedere alla modalità avanzata CLI di ONTAP utilizzando il seguente comando.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Utilizza il comando seguente per impostare la politica di recupero nel cloud del volume, sostituendo i seguenti valori:

   - Sostituisci *svm_name*con il nome della SVM su cui è stato creato il volume.
   - Sostituisci *vol_name*con il nome del volume per il quale stai impostando la politica di recupero dal cloud.

- Sostituisci *retrieval_policy* con il valore desideratodefault, on-readnever, o. promote

```
FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-
policy retrieval_policy
```

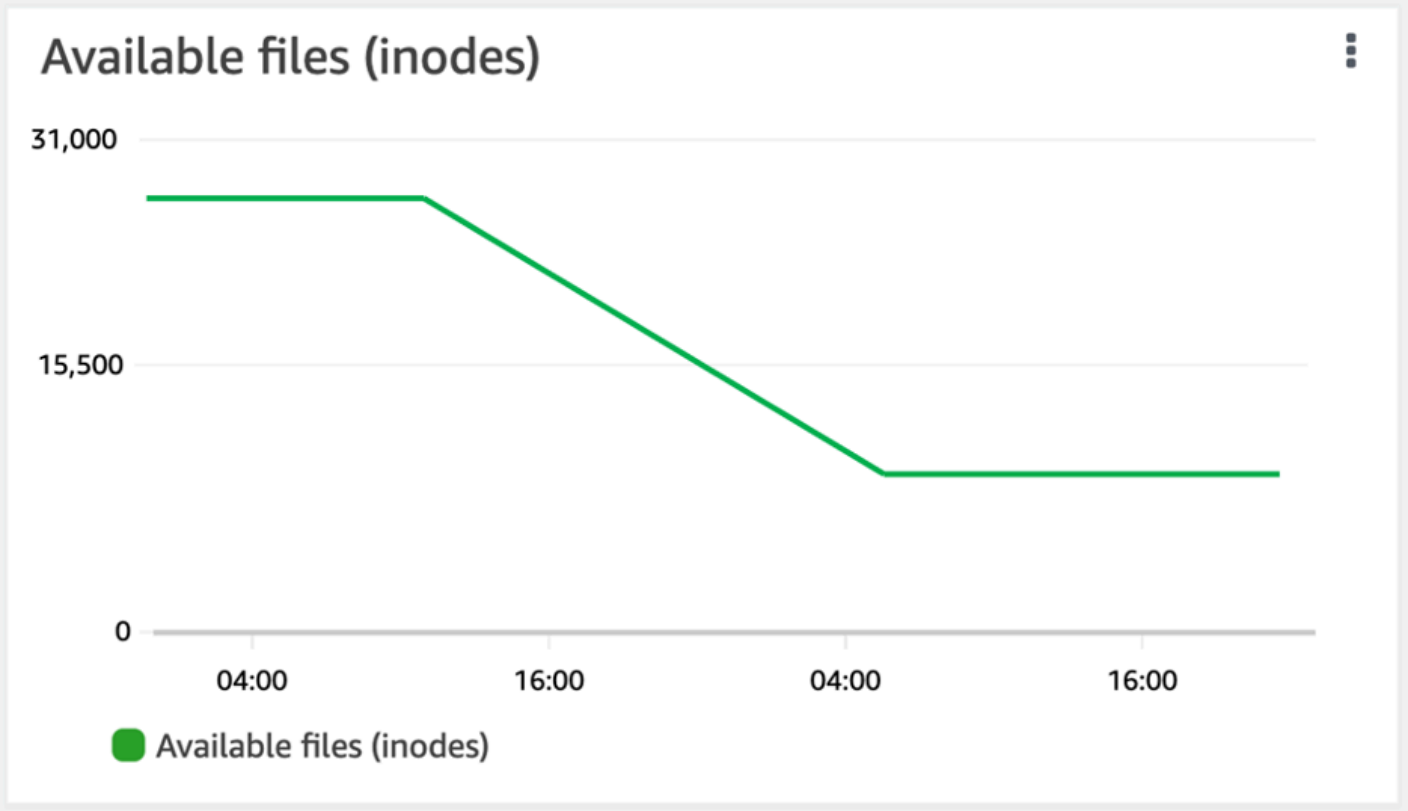
Il sistema risponde come segue in caso di richiesta riuscita.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Visualizzazione della capacità dei file di un volume

È possibile utilizzare uno dei seguenti metodi per visualizzare il numero massimo di file consentiti e il numero di file già utilizzati su un volume.

- Le metriche CloudWatch del volume FilesCapacity eFilesUsed.
- Nella console Amazon FSx, vai al grafico dei file disponibili (inode) nella scheda Monitoraggio del volume. L'immagine seguente mostra i file disponibili (inode) su un volume che diminuisce nel tempo.



Aumento del numero massimo di file su un volume

I volumi FSx for ONTAP possono esaurire la capacità dei file quando il numero di inode o puntatori di file disponibili è esaurito.

Per aumentare il numero massimo di file su un volume (ONTAPCLI)

Si utilizza il comando `volume modify` ONTAP CLI per aumentare il numero massimo di file su un volume. Per ulteriori informazioni, vedere `volume modify`nel NetApp ONTAP Documentation Center.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Completa una delle operazioni riportate di seguito, a seconda del caso d'uso. Sostituisci *svm_name*e *vol_name*con i tuoi valori.

   - Per configurare un volume in modo che abbia sempre il numero massimo di file (inode) disponibili, effettuate le seguenti operazioni:

     1. Accedere alla modalità avanzata nella CLI di ONTAP utilizzando il comando seguente.

        ```
        ::> set adv
        ```

     2. Dopo aver eseguito questo comando, vedrai questo output. Entra y per continuare.

        ```
        Warning: These advanced commands are potentially dangerous; use them only
         when
        directed to do so by NetApp personnel.
        Do you want to continue? {y|n}: y
        ```

     3. Immettete il seguente comando per utilizzare sempre il numero massimo di file sul volume:

        ```
        ::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
        ```

   - Per specificare manualmente il numero totale di file consentiti sul volume*max_number_files* `= (current_size_of_volume) × (1 file ÷ 4 KiB)`, con un valore massimo possibile di 2 miliardi, utilizzate il seguente comando:

     ```
     ::> volume modify -vserver svm_name -volume vol_name -files max_number_files
     ```

Attivazione della modalità di scrittura su cloud di un volume

Usa il comando `volume modify` ONTAP CLI per abilitare o disabilitare la modalità di scrittura cloud per un volume esistente. Per ulteriori informazioni, consulta il Centro di `volume modify`documentazione NetApp ONTAP.

I prerequisiti per impostare la modalità di scrittura su cloud sono:

- Il volume deve essere un volume esistente. È possibile abilitare la funzionalità solo su un volume esistente.
- Il volume deve essere un volume di lettura-scrittura (RW).

- Il volume deve avere la politica All tiering. Per ulteriori informazioni sulla modifica della politica di suddivisione in più livelli di un volume, consulta. Impostazione della politica di suddivisione in più livelli di un volume

La modalità di scrittura su cloud è utile in casi come le migrazioni, ad esempio, in cui grandi quantità di dati vengono trasferite a un file system utilizzando il protocollo NFS.

Per impostare la modalità di scrittura su cloud di un volume (ONTAP CLI)

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *management_endpoint_ip* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Accedere alla modalità avanzata CLI di ONTAP utilizzando il seguente comando.

   ```
   FSx::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. Utilizzate il seguente comando per impostare la modalità di scrittura su cloud del volume, sostituendo i seguenti valori:

   - Sostituisci *svm_name*con il nome della SVM su cui viene creato il volume.
   - Sostituisci *vol_name*con il nome del volume per il quale stai impostando la modalità di scrittura su cloud.
   - Sostituisci *vol_cw_mode* con `true` per abilitare la modalità di scrittura su cloud sul volume o `false` per disabilitarla.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-
   enabled vol_cw_mode
   ```

   Il sistema risponde come segue in caso di richiesta andata a buon fine.

```
Volume modify successful on volume vol_name of Vserver svm_name.
```

Proteggere i tuoi dati

Oltre a replicare automaticamente i dati del file system per garantire un'elevata durabilità, Amazon FSx offre le seguenti opzioni per proteggere ulteriormente i dati archiviati nei file system:

- I backup nativi di Amazon FSx supportano le esigenze di conservazione e conformità dei backup all'interno di Amazon FSx. Puoi anche utilizzarli AWS Backup per gestire, automatizzare e proteggere centralmente i tuoi backup nel cloud. Servizi AWS
- Le istantanee consentono agli utenti di annullare facilmente le modifiche ai file e confrontare le versioni dei file ripristinando i file alle versioni precedenti.
- Replica del file system Amazon FSx su un secondo file system per fornire protezione e ripristino dei dati. La replica, se abilitata, avviene su base automatica e pianificata.
- SnapLockpuò proteggere i file trasferendoli allo stato WORM (Write Once, Read Many), che impedisce la modifica o l'eliminazione per un periodo di conservazione specificato.

Argomenti

Utilizzo dei backup

Con FSx for ONTAP, è possibile eseguire backup giornalieri automatici e backup avviati dall'utente dei volumi sul file system. I backup FSx for ONTAP sono per volume, quindi ogni backup contiene solo i dati di un determinato volume. I backup Amazon FSx sono altamente durevoli e incrementali.

Tutti i backup di Amazon FSx (backup giornalieri automatici e backup avviati dall'utente) sono incrementali. Ciò significa che vengono salvati solo i dati sul volume che sono stati modificati dopo il backup più recente. Ciò riduce al minimo il tempo necessario per creare il backup e lo spazio di archiviazione necessario per il backup, il che consente di risparmiare sui costi di archiviazione evitando la duplicazione dei dati. Quando si elimina un backup, vengono rimossi solo i dati esclusivi di quel backup. Ogni backup di Amazon FSx contiene tutte le informazioni necessarie per creare un nuovo volume dal backup, ripristinando efficacemente un' point-in-time istantanea del volume del file system.

La creazione di backup regolari per i volumi è una best practice che aiuta a supportare le esigenze di conservazione dei dati e conformità. Lavorare con i backup di Amazon FSx è semplice, che si tratti di creare backup, ripristinare da un backup o eliminare un backup.

Amazon FSx supporta il backup di ONTAP FlexVol volumi (su tutti i file system) e di FlexGroup volumi con un `OntapVolumeType` of `RW` (lettura-scrittura).

> **Note**
>
> Amazon FSx non supporta il backup di volumi di protezione dei dati (DP), volumi di condivisione del carico (LS) o volumi di destinazione. FlexCache

Esistono limiti al numero di backup che è possibile archiviare per file system e per volume. Per ulteriori informazioni, consulta Quote che è possibile incrementare e Quote di risorse per ogni file system.

Argomenti

Come funzionano i backup

I backup di Amazon FSx utilizzano istantanee, immagini di sola lettura dei volumi point-in-time, per mantenere l'incrementalità tra i backup. Ogni volta che viene eseguito un backup, Amazon FSx scatta prima un'istantanea del volume. L'istantanea di backup viene archiviata nel volume e occupa spazio sul livello di archiviazione SSD. Amazon FSx confronta quindi questo snapshot con lo snapshot di backup precedente (se ne esiste uno) e copia solo i dati modificati nel backup.

Se non esiste alcuna istantanea di backup precedente, l'intero contenuto dello snapshot di backup più recente viene copiato nel backup. Dopo aver eseguito correttamente lo snapshot di backup più recente, Amazon FSx elimina lo snapshot di backup precedente. Lo snapshot utilizzato per il backup più recente rimane nel volume fino all'esecuzione del backup successivo, quando il processo si ripete. Per ottimizzare i costi di storage di backup, ONTAP preserva i risparmi in termini di efficienza di storage di un volume nei relativi backup.

Amazon FSx non è in grado di eseguire il backup di volumi offline.

Requisiti di storage

Per eseguire il backup dei volumi, sia il volume che il file system devono disporre di una capacità di archiviazione SSD sufficiente per archiviare un'istantanea di backup. Quando si esegue un'istantanea di backup, la capacità di storage aggiuntiva consumata dall'istantanea non può far sì che il volume superi il 98% di utilizzo dello storage SSD. In tal caso, il backup avrà esito negativo. È possibile aumentare lo storage SSD di un volume o di un file system in qualsiasi momento per garantire che i backup non vengano interrotti.

Lavorare con backup giornalieri automatici

I backup giornalieri automatici dei volumi del file system sono abilitati per impostazione predefinita quando si crea un file system. È possibile abilitare o disabilitare i backup giornalieri automatici per un file system in qualsiasi momento. I backup giornalieri automatici vengono eseguiti durante la finestra di backup giornaliera, che viene impostata automaticamente quando si crea un file system. È possibile modificare la finestra di backup giornaliera in qualsiasi momento. Per migliorare le prestazioni di backup, si consiglia di scegliere un'ora del giorno per il backup giornaliero che non rientri nei normali orari di funzionamento delle applicazioni che utilizzano i volumi. Per ulteriori informazioni, consulta Prestazioni di backup e ripristino.

È possibile impostare il periodo di conservazione per i backup giornalieri automatici tra 1 e 90 giorni nella console durante la creazione di un file system o in qualsiasi momento. Il periodo di

conservazione dei backup giornalieri automatici predefinito è di 30 giorni. Il servizio elimina un backup giornaliero automatico una volta scaduto il periodo di conservazione. Utilizzando la CLI o l'API, è possibile impostare il periodo di conservazione tra 0 e 90 giorni; impostandolo su 0, i backup giornalieri automatici vengono disattivati.

La finestra di backup giornaliera e il periodo di conservazione dei backup sono impostazioni a livello di file system che si applicano a tutti i volumi del file system. Puoi utilizzare la console Amazon FSx AWS CLI, o l'API per modificare la finestra di backup e il periodo di conservazione dei backup per i tuoi file system e per attivare o disattivare i backup giornalieri automatici. Per ulteriori informazioni, consulta Aggiornamento di un file system.

Non è possibile creare un backup del volume se il volume è offline. Per ulteriori informazioni, consulta Backup e volumi offline.

> **Note**
>
> I backup giornalieri automatici hanno un periodo di conservazione massimo di 90 giorni, ma i backup avviati dall'utente che crei, che includono i backup creati utilizzando AWS Backup, vengono conservati per sempre a meno che tu o il servizio non li elimini. AWS Backup

Puoi eliminare manualmente un backup giornaliero automatico utilizzando la console, la CLI e l'API. Quando elimini un volume, elimini anche i backup giornalieri automatici per quel volume. Amazon FSx offre la possibilità di creare un backup finale di un volume prima di eliminarlo. Il backup finale viene conservato per sempre, a meno che tu non lo elimini. Per ulteriori informazioni, consulta. Eliminazione di backup

Utilizzo dei backup avviati dall'utente

Con Amazon FSx, puoi eseguire manualmente il backup dei volumi del tuo file system in qualsiasi momento utilizzando l'API AWS Management Console AWS CLI, e. I backup avviati dall'utente sono incrementali rispetto ad altri backup che potrebbero essere stati creati per un volume e vengono conservati per sempre, a meno che non vengano eliminati. I backup avviati dall'utente vengono conservati anche dopo l'eliminazione del volume o del file system su cui sono stati creati i backup. Puoi eliminare i backup avviati dall'utente solo utilizzando la console Amazon FSx, l'API o la CLI. Non vengono mai eliminati automaticamente da Amazon FSx. Per ulteriori informazioni, consulta Eliminazione di backup.

Non è possibile creare un backup del volume se il volume è offline. Per ulteriori informazioni, consulta Backup e volumi offline.

Copiare i tag nei backup

Quando crei o aggiorni un volume utilizzando la CLI o l'API, puoi `CopyTagsToBackups` abilitare la copia automatica di qualsiasi tag sul volume nei relativi backup. Tuttavia, se si aggiungono tag durante la creazione di un backup avviato dall'utente, inclusa l'assegnazione di un nome a un backup quando si utilizza la console, il servizio non copia i tag dal volume, anche se è abilitato. `CopyTagsToBackups`

Prestazioni di backup e ripristino

Numerosi fattori possono influenzare le prestazioni delle operazioni di backup e ripristino. Le operazioni di backup e ripristino sono processi in background, il che significa che hanno una priorità inferiore rispetto alle operazioni di I/O del client. Le operazioni di I/O del client includono la lettura e la scrittura dei dati NFS, CIFS e iSCSI. Tutti i processi in background, incluse le operazioni di backup e ripristino, utilizzano solo la parte inutilizzata della capacità di throughput del file system e il completamento può richiedere da pochi minuti a qualche ora a seconda delle dimensioni del backup e della quantità di capacità di throughput inutilizzata sul file system.

Altri fattori che influiscono sulle prestazioni di backup e ripristino includono il livello di storage in cui vengono archiviati i dati e il profilo del set di dati. Ti consigliamo di creare i primi backup dei volumi quando la maggior parte dei dati si trova su unità di archiviazione SSD. I set di dati contenenti principalmente file di piccole dimensioni hanno in genere prestazioni inferiori rispetto a set di dati di dimensioni simili che contengono principalmente file di grandi dimensioni. Questo perché l'elaborazione di un numero elevato di file di piccole dimensioni richiede più cicli di CPU e sovraccarico di rete rispetto all'elaborazione di un numero inferiore di file di grandi dimensioni.

In genere, puoi aspettarti le seguenti velocità di backup durante il backup dei dati archiviati nel livello di archiviazione SSD:

- 750 MBps su diversi backup simultanei contenenti principalmente file di grandi dimensioni.
- 100 MBps su diversi backup simultanei contenenti principalmente file di piccole dimensioni.

In genere, puoi aspettarti le seguenti velocità di ripristino:

- 250 MBps su diversi ripristini simultanei contenenti principalmente file di grandi dimensioni.
- 100 MBps su diversi ripristini simultanei contenenti principalmente file di piccole dimensioni.

Utilizzo AWS Backup con Amazon FSx

AWS Backup è un modo semplice ed economico per proteggere i dati eseguendo il backup dei volumi Amazon FSx for ONTAP. NetApp AWS Backup è un servizio di backup unificato progettato per semplificare la creazione, il ripristino e l'eliminazione dei backup, fornendo al contempo report e audit 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.
- Monitora tutte le attività recenti di backup, copia e ripristino.

AWS Backup utilizza la funzionalità di backup integrata di Amazon FSx. I backup creati utilizzando la AWS Backup console hanno lo stesso livello di coerenza e prestazioni del file system, sono incrementali rispetto a qualsiasi altro backup Amazon FSx eseguito sul tuo volume (avviato dall'utente o automatico) e offrono le stesse opzioni di ripristino dei backup eseguiti tramite la console Amazon FSx. Se gestisci questi backup, ottieni funzionalità aggiuntive, come la possibilità di creare backup pianificati con una frequenza oraria. AWS Backup È possibile aggiungere un ulteriore livello di difesa per proteggere i backup da eliminazioni involontarie o dolose archiviandoli in un Vault. AWS Backup

I backup creati da AWS Backup sono considerati backup avviati dall'utente e vengono conteggiati ai fini della quota di backup avviata dall'utente per Amazon FSx. Per ulteriori informazioni, consulta Quote che è possibile incrementare. Puoi visualizzare e ripristinare i backup creati da AWS Backup nella console Amazon FSx, nella CLI e nell'API. Tuttavia, non puoi eliminare i backup creati AWS Backup nella console Amazon FSx, nella CLI o nell'API. Per ulteriori informazioni, consulta la sezione Guida introduttiva alla Developer AWS Backup Guide.AWS Backup

AWS Backup non è possibile eseguire il backup di volumi offline.

Ripristino dei backup su un nuovo volume

È possibile ripristinare un backup di un volume su un nuovo volume, ripristinando efficacemente un' point-in-time istantanea di un volume utilizzando la console, la CLI o l'API.

Quando si ripristina un backup, tutti i dati vengono prima scritti sul livello di archiviazione SSD prima che il servizio inizi a suddividere i dati su più livelli nello storage del pool di capacità in base alla politica di tiering impostata per il volume ripristinato. Quando si ripristina un backup su un volume con una politica di suddivisione in più livelli di`All`, un processo periodico in background assegna i dati al pool di capacità. Quando si ripristina un backup su un volume con una politica di tiering pari `Snapshot Only` o`Auto`, i dati vengono suddivisi su più livelli nel pool di capacità se l'utilizzo dell'SSD per il file system è superiore al 50% e la velocità di raffreddamento è determinata dal periodo di raffreddamento della policy di tiering.

Quando ripristini un backup di FlexGroup volume su un file system con un numero diverso di coppie ad alta disponibilità (HA) rispetto al file system originale, Amazon FSx potrebbe aggiungere ulteriori volumi costituenti per garantire che i componenti siano distribuiti uniformemente.

Per step-by-step istruzioni su come ripristinare un backup su un nuovo volume, consulta. Ripristino di un backup su un nuovo volume

> **Note**
>
> Un volume ripristinato ha sempre lo stesso stile di volume del volume originale. Non è possibile modificare lo stile del volume durante il ripristino.

Eliminazione di backup

Puoi eliminare i backup giornalieri automatici e i backup avviati dall'utente dei tuoi volumi. 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. Per istruzioni su come eliminare i backup, consulta. Eliminazione di un backup

Non puoi eliminare backup creati da AWS Backup, che hanno tipo AWS Backup, nella console Amazon FSx, nella CLI o nell'API. Per informazioni sull'eliminazione dei backup creati da AWS Backup, consulta Eliminazione dei backup nella Guida per gli sviluppatori. AWS Backup

Non è possibile eliminare il backup di un volume se il volume è offline. Per ulteriori informazioni, consulta Backup e volumi offline.

> **Important**
>
> Non eliminare l'istantanea comune sul volume perché viene utilizzata per mantenere l'incrementalità tra i backup. L'eliminazione dell'istantanea comune sul volume farà sì che il backup successivo riguardi l'intero volume anziché un semplice backup incrementale.

Backup e volumi offline

Non è possibile creare o eliminare backup di volumi se tale volume è offline. Utilizzate il comando `volume show`ONTAPCLI per determinare lo stato e lo stato correnti di un volume.

Per riportare online un volume offline, utilizzate il comando `volume online`ONTAPCLI come nell'esempio seguente:

```
::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

Creazione di un backup avviato dall'utente

La procedura seguente descrive come utilizzare la console Amazon FSx per creare un backup di un volume avviato dall'utente.

Non è possibile creare un backup del volume se il volume è offline. Per ulteriori informazioni, consulta Backup e volumi offline.

Per creare un backup di un volume (console) avviato dall'utente

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il ONTAP file system per cui desideri eseguire il backup di un volume.
3. Scegli la scheda Volumi.
4. Scegli il volume di cui desideri eseguire il backup.
5. Da Azioni, scegli Crea backup.
6. 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. + - = _:/

7. Scegliere Create backup (Crea backup).

È stato ora creato un backup di uno dei volumi del file system. Puoi trovare una tabella di tutti i tuoi backup nella console Amazon FSx 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 si crea un backup avviato dall'utente come descritto nella procedura descritta in questa procedura, il backup è di tipo `USER_INITIATED` corrispondente e mantiene lo `CREATING` stato fino a quando non è completamente disponibile.

Ripristino di un backup su un nuovo volume

Le seguenti procedure descrivono come ripristinare un backup FSx for ONTAP su un nuovo volume utilizzando and. AWS Management Console AWS CLI

Per ripristinare un backup di un volume su un nuovo volume (Console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione, scegli Backup, quindi scegli il backup del volume FSx for ONTAP che desideri ripristinare.
3. Nel menu Azioni in alto a destra, scegli Ripristina backup. Viene visualizzata la pagina Crea volume da backup.
4. Scegliete la macchina virtuale FSx for ONTAP File system and Storage su cui ripristinare il backup dai menu a discesa.
5. In Dettagli del volume, sono disponibili diverse selezioni. Innanzitutto, inserisci il nome del volume. È possibile utilizzare fino a 203 caratteri alfanumerici o di sottolineatura (_).
6. Per Dimensione del volume, immettete un numero intero compreso tra 20 e 314572800 per specificare la dimensione in mebibyte (MiB).
7. Per Tipo di volume, scegliete Read-Write (RW) per creare un volume leggibile e scrivibile o Data Protection (DP) per creare un volume di sola lettura che può essere utilizzato come destinazione di una relazione or. NetApp SnapMirror SnapVault Per ulteriori informazioni, consulta Tipi di volume.
8. Per Junction path, inserite una posizione all'interno del file system in cui montare il volume. Il nome deve avere una barra iniziale, ad esempio `/vol3`.

9. Per l'efficienza dello storage, scegli Enabled per abilitare le funzionalità di ONTAP efficienza dello storage (deduplicazione, compressione e compattazione). Per ulteriori informazioni, consulta FSx per l'efficienza dello storage ONTAP.
10. Per lo stile di sicurezza Volume, scegli Unix (Linux), NTFS o Mixed. Lo stile di sicurezza di un volume determina se dare la preferenza agli ACL NTFS o UNIX per l'accesso multiprotocollo. La modalità MIXED non è richiesta per l'accesso multiprotocollo ed è consigliata solo per utenti esperti.
11. Per la policy Snapshot, scegli una policy di snapshot per il volume. Per ulteriori informazioni sulle politiche relative alle snapshot, vedere. Politiche relative alle istantanee

    Se si sceglie Politica personalizzata, è necessario specificare il nome della politica nel campo Custom-Policy. La politica personalizzata deve già esistere sulla SVM o nel file system. Puoi creare una policy di snapshot personalizzata con la ONTAP CLI o l'API REST. Per ulteriori informazioni, consulta Create a Snapshot Policy nella documentazione del NetApp ONTAP prodotto.
12. Per il periodo di raffreddamento della politica di tiering, i valori validi sono 2-183 giorni. Il periodo di raffreddamento della politica di tiering di un volume definisce il numero di giorni prima che i dati a cui non è stato effettuato l'accesso vengano contrassegnati come freddi e trasferiti nello storage con pool di capacità. Questa impostazione influisce solo sulle `Snapshot-only` politiche `Auto` and.
13. Nella sezione Avanzate, per SnapLockConfigurazione, puoi lasciare l'impostazione predefinita Disabilitato o scegliere Abilitato per configurare un SnapLock volume. Per ulteriori informazioni sulla configurazione di uno o più SnapLock Compliance SnapLock Enterprise volumi, consulta Creazione di un volume di SnapLock conformità eCreazione di un volume SnapLock Enterprise. Per ulteriori informazioni su SnapLock, consulta Proteggi i tuoi dati con SnapLock.
14. Scegli Conferma per creare il volume.

Per ripristinare un backup di un volume su un nuovo volume (CLI)

Utilizza il comando create-volume-from-backupCLI o il comando CreateVolumeFromBackupAPI equivalente per ripristinare il backup di un volume su un nuovo volume.

- ```
  $ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
        --name demo --ontap-configuration JunctionPath=/demo, SizeInMegabytes=100000,
   \
        StorageVirtualMachineId=svm-0f04a9c7c27e1908b, TieringPolicy={Name=ALL}
  ```
  ```

La risposta del sistema per una richiesta riuscita:


```
{
      "Volume": {
          "CreationTime": 1692721488.428,
          "FileSystemId": "fs-07ab735385276ed60",
          "Lifecycle": "CREATING",
          "Name": "demo",
          "OntapConfiguration": {
              "FlexCacheEndpointType": "NONE",
              "JunctionPath": "/demo",
              "SizeInMegabytes": 100000,
              "StorageEfficiencyEnabled": true,
              "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
              "StorageVirtualMachineRoot": false,
              "TieringPolicy": {
                  "Name": "ALL"
              },
              "OntapVolumeType": "DP",
              "SnapshotPolicy": "default",
              "CopyTagsToBackups": false,
          },
          "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
          "VolumeId": "fsvol-0b6ec764c9c5f654a",
          "VolumeType": "ONTAP",

      }
  }
```


Eliminazione di un backup

Puoi eliminare i backup giornalieri automatici e i backup avviati dall'utente utilizzando la console Amazon FSx, la CLI e l'API, come descritto nelle seguenti procedure.

Per eliminare i backup creati utilizzando, consulta Eliminazione dei backup nella Guida per AWS Backup gli sviluppatori. AWS Backup

Per eliminare un backup (console)

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

2. Dalla dashboard della console, scegli Backup 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 mostrato sia 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.

Per eliminare un backup (CLI)

- Utilizzate il comando delete-backup CLI o l'azione DeleteBackup API equivalente per eliminare un backup del volume FSx for ONTAP, come illustrato nell'esempio seguente.

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

La risposta del sistema include l'ID del backup da eliminare e lo stato del relativo ciclo di vita, indicando che la richiesta ha avuto esito positivo. `DELETED`

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

Utilizzo degli snapshot

Un'istantanea è un'immagine di sola lettura di un volume Amazon FSx for NetApp ONTAP in un determinato momento. Le istantanee offrono protezione contro l'eliminazione o la modifica accidentale dei file nei volumi. Con le istantanee, gli utenti possono visualizzare e ripristinare facilmente singoli file o cartelle da un'istantanea precedente per annullare le modifiche, recuperare i contenuti eliminati e confrontare le versioni dei file.

Un'istantanea contiene i dati che sono stati modificati dall'ultima istantanea che consuma la capacità di archiviazione SSD del file system. Le istantanee non sono incluse in nessun backup di volume. Le istantanee sono abilitate per impostazione predefinita sui volumi utilizzando la policy relativa alle `default` istantanee. Le istantanee vengono archiviate nella `.snapshot` directory alla radice di un

volume. È possibile archiviare un massimo di 1.023 istantanee per volume in qualsiasi momento. Una volta raggiunto questo limite, è necessario eliminare un'istantanea esistente prima di poter creare una nuova istantanea del volume.

Argomenti

Politiche relative alle istantanee

La policy relativa alle istantanee definisce il modo in cui il sistema crea le istantanee per un volume. La policy specifica quando creare le istantanee, quante copie conservare e come denominarle. Esistono tre policy di snapshot integrate per FSx for ONTAP:

- `default`
- `default-1weekly`
- `none`

Per impostazione predefinita, ogni volume è associato alla politica di snapshot del file system. `default` Consigliamo di utilizzare questa policy per la maggior parte dei carichi di lavoro.

La `default` policy crea automaticamente le istantanee secondo la seguente pianificazione, con l'eliminazione delle copie delle istantanee più vecchie per fare spazio alle copie più recenti:

- Fino a sei snapshot orarie acquisite cinque minuti dopo l'ora.
- Fino a due snapshot quotidiane acquisite da lunedì a sabato 10 minuti dopo la mezzanotte.
- Fino a due snapshot settimanali acquisite ogni domenica 15 minuti dopo la mezzanotte.

> **Note**
>
> Gli orari delle istantanee si basano sul fuso orario del file system, che per impostazione predefinita è il Coordinated Universal Time (UTC). Per informazioni sulla modifica del fuso orario, vedere Visualizzazione e impostazione del fuso orario del sistema nella documentazione di NetApp Support.

La `default-1weekly` politica funziona allo stesso modo della `default` politica, tranne per il fatto che conserva solo un'istantanea della pianificazione settimanale.

La `none` policy non scatta alcuna istantanea. È possibile assegnare questa politica ai volumi per evitare che vengano scattate istantanee automatiche.

Puoi anche creare una policy di snapshot personalizzata utilizzando la CLI ONTAP o l'API REST. Per ulteriori informazioni, consulta Create a Snapshot Policy nella documentazione del NetApp prodotto ONTAP. Puoi scegliere una policy di snapshot durante la creazione o l'aggiornamento di un volume nella console Amazon FSx, o nell' AWS CLI API Amazon FSx. Per ulteriori informazioni, consulta Creazione di volumi e Aggiornamento di un volume.

Ripristino di singoli file e cartelle

Utilizzando le istantanee sul file system Amazon FSx, gli utenti possono ripristinare rapidamente le versioni precedenti di singoli file o cartelle. In questo modo possono recuperare i file eliminati o modificati archiviati nel file system condiviso. Lo fanno in modalità self-service direttamente sul desktop senza l'assistenza dell'amministratore. Questo approccio self-service aumenta la produttività e riduce il carico di lavoro amministrativo.

I client Linux e macOS possono visualizzare le istantanee nella `.snapshot` directory alla radice di un volume. I client Windows possono visualizzare le istantanee nella `Previous Versions` scheda di Windows Explorer (facendo clic con il pulsante destro del mouse su un file o una cartella).

Ripristina i file dalle istantanee

Per ripristinare un file da un'istantanea (client Linux e macOS)

1. Se il file originale esiste ancora e non vuoi che venga sovrascritto dal file in un'istantanea, usa il tuo client Linux o macOS per rinominare il file originale o spostarlo in un'altra directory.

2. Nella `.snapshot` directory, individua l'istantanea che contiene la versione del file che desideri ripristinare.
3. Copia il file dalla `.snapshot` directory alla directory in cui il file esisteva originariamente.

Per ripristinare un file da un'istantanea (client Windows)

Gli utenti dei client Windows possono ripristinare i file nelle versioni precedenti utilizzando la familiare interfaccia Windows File Explorer.

1. Per ripristinare un file, gli utenti scelgono il file da ripristinare, quindi scelgono Ripristina versioni precedenti dal menu contestuale (con il pulsante destro del mouse).
2. Gli utenti possono quindi visualizzare e ripristinare una versione precedente dall'elenco Versioni precedenti.

I dati nelle istantanee sono di sola lettura. Se si desidera apportare modifiche ai file e alle cartelle elencati nella scheda Versioni precedenti, è necessario salvare una copia dei file e delle cartelle che si desidera modificare in una posizione scrivibile e apportare modifiche alle copie.

Eliminazione di snapshot

Le istantanee consumano la capacità di archiviazione solo per i dati su un volume che è stato modificato dall'ultima istantanea. Per questo motivo, se il carico di lavoro scrive i dati rapidamente, le istantanee di vecchi dati possono occupare una quantità significativa della capacità di archiviazione di un volume.

Ad esempio, l'output del comando `volume show-space`ONTAPCLI mostra 140 KB di. `User Data` Tuttavia, il volume aveva 9,8 GB di spazio `User Data` prima dell'eliminazione dei dati utente. Anche se hai eliminato i file dal volume, un'istantanea potrebbe comunque fare riferimento ai vecchi dati utente. Per questo motivo, `Snapshot Reserve` e `Snapshot Spill` nell'esempio precedente, occupano un totale di 9,8 GB di spazio, anche se sul volume non sono presenti praticamente dati utente.

Per liberare spazio sui volumi, puoi eliminare le istantanee più vecchie che non ti servono più. È possibile farlo creando un criterio di eliminazione automatica delle istantanee o eliminando manualmente le istantanee. L'eliminazione di un'istantanea elimina i dati modificati memorizzati nell'istantanea.

Crea una politica di eliminazione automatica delle istantanee

È possibile creare una policy per eliminare automaticamente le istantanee quando la quantità di spazio disponibile nel volume si sta esaurendo. Utilizzate il comando ONTAPCLI Volume Snapshot autodelete edit per stabilire una politica di eliminazione automatica per un volume.

Quando usi questo comando, usa i tuoi dati per sostituire i seguenti valori segnaposto:

- Sostituisci *svm_name*con il nome della SVM su cui è stato creato il volume.
- Sostituisci *vol_name*con il nome del volume.

Per`-trigger`, assegna uno dei seguenti valori:

- `volume`— Utilizzare `volume` se si desidera che la soglia al di sopra della quale le istantanee vengono eliminate corrisponda a una soglia di capacità totale del volume utilizzato. Le soglie di capacità del volume utilizzato che determinano l'eliminazione delle istantanee sono determinate dalla dimensione del volume, con una soglia scalabile dall'85 al 98% della capacità utilizzata. I volumi più piccoli hanno una soglia più piccola, mentre i volumi più grandi ne hanno una più grande.
- `snap_reserve`— Utilizzalo `snap_reserve` se desideri che le istantanee vengano eliminate in base a ciò che può essere conservato nella tua riserva di istantanee.

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true
 -trigger [volume|snap_reserve]
```

Per ulteriori informazioni, consultate il comando Volume Snapshot autodelete edit nel Centro documentazione ONTAP. NetApp

Eliminazione di snapshot

Utilizza il comando volume snapshot deleteONTAPCLI per eliminare manualmente le istantanee, sostituendo i seguenti valori segnaposto con i tuoi dati:

- Sostituisci *svm_name*con il nome della SVM su cui è stato creato il volume.
- Sostituisci *vol_name*con il nome del volume.

- Sostituisci *snapshot_name*con il nome dell'istantanea. Questo comando supporta caratteri jolly (*) per. *snapshot_name* Pertanto, è possibile eliminare tutte le istantanee orarie, ad esempio utilizzando. `hourly*`

> **Important**
>
> Se hai abilitato i backup Amazon FSx, Amazon FSx conserva uno snapshot per il backup Amazon FSx più recente di ogni volume. Queste istantanee vengono utilizzate per mantenere l'incrementalità tra i backup e non devono essere eliminate utilizzando questo metodo.

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

Disattivazione delle istantanee automatiche

Le istantanee automatiche sono abilitate dalla politica di snapshot predefinita per i volumi nel file system FSx for ONTAP. Se non hai bisogno di istantanee dei tuoi dati (ad esempio, se utilizzi dati di test), puoi disabilitare le istantanee impostando la politica di snapshot del volume sull'noneutilizzo dell' AWS Management Console API AWS CLI e e della ONTAP CLI, come descritto nelle seguenti procedure.

Per disabilitare le istantanee automatiche (console)AWS

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il file system ONTAP per cui desideri aggiornare un volume.
3. Scegli la scheda Volumi.
4. Scegli il volume che desideri aggiornare.
5. Per Azioni, scegli Aggiorna volume.

   Viene visualizzata la finestra di dialogo Aggiorna volume con le impostazioni correnti del volume.
6. Per la politica Snapshot, scegliete Nessuno.
7. Scegli Aggiorna per aggiornare il volume.

Per disabilitare le istantanee automatiche (AWS CLI)

- Utilizzate il comando AWS CLI update-volume (o il comando UpdateVolumeAPI equivalente) per impostare `SnapshotPolicy` to`none`, come illustrato nell'esempio seguente.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=none, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Per disabilitare le istantanee automatiche (ONTAPCLI)

Imposta la politica delle istantanee del volume in modo da utilizzare la politica `none` predefinita per disattivare le istantanee automatiche.

1. Usa il comando `volume snapshot policy show`ONTAPCLI per mostrare la `none` politica.

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                         Number of Is
Policy Name              Schedules Enabled Comment
------------------------ --------- ------- ---------------------------------
none                               0 false   Policy for no automatic snapshots.
    Schedule               Count     Prefix                SnapMirror Label
    ---------------------- -----     --------------------- ------------------
    -                          -     -                     -
```

2. Utilizzate il comando `volume modify`ONTAPCLi per impostare la politica delle istantanee del volume in modo da `none` disabilitare le istantanee automatiche. Sostituisci i seguenti valori segnaposto con i tuoi dati:

   - *`svm_name`*— usa il nome del tuo SVM.
   - *`vol_name`*— usa il nome del tuo volume.

   Quando ti viene richiesto di continuare, inserisci**y**.

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none

Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
 Snapshot copies on this volume
        that do not match any of the prefixes of the new Snapshot policy will not
 be deleted. However, when
        the new Snapshot policy takes effect, depending on the new retention
 count, any existing Snapshot copies
        that continue to use the same prefixes might be deleted. See the 'volume
 modify' man page for more information.
Do you want to continue? {y|n}: y
Volume modify successful on volume vol_name of Vserver svm_name.
```

Riserva istantanee

La riserva di copie istantanee imposta una percentuale specifica della capacità di storage di un volume per l'archiviazione di copie istantanee, con un valore predefinito del 5%. La riserva di copie Snapshot deve disporre di spazio sufficiente per le copie Snapshot, inclusi i backup di volume. Se le copie Snapshot superano lo spazio di riserva dello Snapshot, è necessario eliminare le copie Snapshot esistenti dal file system attivo per ripristinare la capacità di archiviazione necessaria per l'utilizzo del file system. È inoltre possibile modificare la percentuale di spazio su disco assegnata alle copie Snapshot.

Ogni volta che le istantanee occupano più del 100% della riserva Snapshot, iniziano a occupare lo spazio di archiviazione SSD principale. Questo processo si chiama Snapshot spill. Quando le istantanee continuano a occupare lo spazio attivo del file system, il file system rischia di riempirsi. Se il file system si riempie a causa della fuoriuscita di istantanee, è possibile creare file solo dopo aver eliminato un numero sufficiente di istantanee.

Quando è disponibile spazio su disco sufficiente per le istantanee nella riserva Snapshot, l'eliminazione dei file dal livello SSD principale libera spazio su disco per nuovi file, mentre le copie Snapshot che fanno riferimento a tali file consumano solo lo spazio nella riserva di copie Snapshot.

Poiché non è possibile impedire alle istantanee di consumare uno spazio su disco superiore alla quantità a loro riservata (la riserva Snapshot), è importante riservare spazio su disco sufficiente per le istantanee in modo che il livello SSD principale abbia sempre spazio disponibile per creare nuovi file o modificare quelli esistenti.

Se un'istantanea viene creata quando i dischi sono pieni, l'eliminazione dei file dal livello SSD principale non crea spazio libero perché tutti i dati sono referenziati anche dall'istantanea appena creata. È necessario eliminare l'istantanea per liberare spazio di archiviazione e creare o aggiornare qualsiasi file.

È possibile modificare la quantità di riserva Snapshot su un volume utilizzando la NetApp ONTAP CLI. Per ulteriori informazioni, consulta Aggiornamento della riserva Snapshot del volume.

Aggiornamento della riserva Snapshot del volume

È possibile modificare la quantità di riserva Snapshot su un volume utilizzando la NetApp ONTAP CLI o l'API, descritta nella procedura seguente.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *management_endpoint_ip* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.
2. Utilizzate il comando `snap reserve` ONTAP CLI per modificare la percentuale di spazio su disco utilizzata per la riserva di copie Snapshot. Sostituisci *vol_name* con il nome del volume e *percent* `with the percent of disk space you want to reserve for Snapshot copies.`

   ```
   ::> snap reserve vol_name percent
   ```

   L'esempio seguente modifica la riserva di snapshot per vol1 al 25% della capacità di archiviazione dei volumi.

   ```
   ::> snap reserve vol1 25
   ```

Replica pianificata utilizzando NetApp SnapMirror

È possibile utilizzarlo NetApp SnapMirror per pianificare la replica periodica del file system FSx for ONTAP da o verso un secondo file system. Questa funzionalità è disponibile sia per le implementazioni a livello locale che interregionale.

NetApp SnapMirror replica i dati ad alta velocità, in modo da ottenere un'elevata disponibilità dei dati e una replica rapida dei dati su tutti i sistemi ONTAP, indipendentemente dal fatto che si esegua la replica tra due file system Amazon FSx in AWS o da locale a. AWS La replica può essere pianificata ogni 5 minuti, anche se gli intervalli devono essere scelti con cura in base agli RPO (Recovery Point Objectives), agli RTO (Recovery Time Objectives) e a considerazioni relative alle prestazioni.

Quando si replicano i dati sui sistemi di NetApp storage e si aggiornano continuamente i dati secondari, i dati vengono mantenuti aggiornati e disponibili ogni volta che ne hai bisogno. Non sono necessari server di replica esterni. Per ulteriori informazioni sull'utilizzo per NetApp SnapMirror replicare i dati, consulta Informazioni sul servizio di replica nella documentazione di BlueXP. NetApp

Puoi creare un volume di destinazione per la protezione dei dati (DP) per NetApp SnapMirror utilizzare la console Amazon FSx, e AWS CLI l'API Amazon FSx, oltre all'interfaccia a riga di comando di NetApp ONTAP e all'API REST. Per informazioni sulla creazione di un volume di destinazione utilizzando la console Amazon FSx e AWS CLI, consulta. Creazione di volumi

È possibile utilizzare NetApp BlueXP o la CLI NetApp ONTAP per pianificare la replica per il file system.

> **Note**
>
> Esistono due tipi di SnapMirror replica: a livello di volume e SVM Disaster Recovery (SVMDR)SnapMirror. FSx for ONTAP supporta solo SnapMirror la replica a livello di volume.

NetApp Utilizzo di BlueXP per pianificare la replica

È possibile utilizzare NetApp BlueXP per configurare la replica SnapMirror sul file system FSx for ONTAP. Per ulteriori informazioni, vedete Replicazione dei dati tra sistemi nella documentazione di BlueXP. NetApp

Utilizzo della CLI NetApp ONTAP per pianificare la replica

È possibile utilizzare l' NetApp ONTAP CLI per configurare la replica pianificata dei volumi. Per informazioni, consulta Gestire la replica dei SnapMirror volumi nel Centro di documentazione ONTAP. NetApp

Proteggi i tuoi dati con SnapLock

SnapLockè una funzionalità che consente di proteggere i file passando allo stato WORM (Write Once, Read Many), che impedisce la modifica o l'eliminazione per un periodo di conservazione specificato. È possibile utilizzarla SnapLock per soddisfare la conformità normativa, proteggere i dati aziendali critici dagli attacchi ransomware e fornire un ulteriore livello di protezione per i dati da alterazioni o eliminazioni.

Amazon FSx for NetApp ONTAP supporta le modalità di conservazione Compliance ed Enterprise con. SnapLock Per ulteriori informazioni, consultare Conformità SnapLock e SnapLockImpresa.

È possibile creare SnapLock volumi sui file system FSx for ONTAP creati a partire dal 13 luglio 2023. I file system esistenti riceveranno SnapLock supporto durante una prossima finestra di manutenzione settimanale.

Argomenti

Funzionamento di SnapLock

SnapLockpuò aiutarvi a soddisfare gli obiettivi normativi e di governance impedendo che i file vengano eliminati, modificati o rinominati. Quando si crea un SnapLock volume, si affidano i file allo storage WORM (Write Once, Read Many) e si impostano periodi di conservazione dei dati. I file possono essere archiviati in uno stato non cancellabile e non scrivibile per un periodo prestabilito o a tempo indeterminato.

> **Important**
>
> È necessario specificare se un volume utilizzerà SnapLock le impostazioni al momento della creazione. Un non SnapLock volume non può essere convertito in SnapLock volume dopo la creazione.

Modalità di conservazione

SnapLockdispone di due modalità di conservazione: Compliance ed Enterprise. Amazon FSx for NetApp ONTAP li supporta entrambi. Hanno casi d'uso diversi e alcune funzionalità sono diverse, ma entrambe proteggono i dati dalla modifica o dall'eliminazione utilizzando il modello WORM. La tabella seguente illustra alcune delle somiglianze e delle differenze tra queste modalità di conservazione.

Caratteristica SnapLock	Conformità SnapLock	SnapLockImpresa
Descrizione	I file trasferiti a WORM su un volume Compliance non possono essere eliminati fino alla scadenza dei relativi periodi di conservazione.	I file trasferiti a WORM su un volume Enterprise possono essere eliminati dagli utenti autorizzati prima della scadenza dei periodi di conservazione utilizzando l'eliminazione privilegiata.
Casi d'uso	• Per soddisfare mandati governativi o specifici del settore, come la regola SEC 17a-4 (f), la regola FINRA 4511 e il regolamento CFTC 1.31. • Per proteggersi dagli attacchi ransomware.	• Promuovere l'integrità dei dati e la conformità interna di un'organizzazione. • Per testare le impostazi oni di conservazione prima di utilizzare SnapLock Compliance.
Commit automatico	Sì	Sì
Conservazione basata sugli eventi (EBR)*	Sì	Sì

Caratteristica SnapLock	Conformità SnapLock	SnapLockImpresa
Conservazione a fini legali*	Sì	No
Eliminazione con privilegi	No	Sì
Modalità Volume-append	Sì	Sì
SnapLockvolumi dei registri di controllo	Sì	Sì

* Le operazioni EBR e Legal Hold sono supportate nella ONTAP CLI e nell'API REST.

Amministratore di SnapLock

È necessario disporre dei privilegi di SnapLock amministratore per eseguire determinate azioni sui volumi. SnapLock SnapLocki privilegi di amministratore sono definiti nel `vsadmin-snaplock` ruolo nella ONTAP CLI. È necessario essere un amministratore del cluster per creare un account di amministratore di una macchina virtuale di archiviazione (SVM) con il SnapLock ruolo di amministratore.

È possibile eseguire le seguenti azioni con il `vsadmin-snaplock` ruolo nella ONTAP CLI:

- Gestisci il tuo account utente, la password locale e le informazioni chiave
- Gestisci i volumi, tranne lo spostamento dei volumi
- Gestisci quote, qtree, copie istantanee e file
- Esegui SnapLock azioni, tra cui l'eliminazione con privilegi e la conservazione a fini legali
- Configura i protocolli Network File System (NFS) e Server Message Block (SMB)
- Configura i servizi Domain Name System (DNS), Lightweight Directory Access Protocol (LDAP) e Network Information Service (NIS)
- Monitoraggio dei lavori

La procedura seguente descrive in dettaglio come creare un SnapLock amministratore nella ONTAP CLI. È necessario accedere come amministratore del cluster su una connessione sicura, ad esempio Secure Shell Protocol (SSH) per eseguire questa attività.

Per creare un account amministratore SVM con il ruolo vsadmin-snaplock nella CLI ONTAP

- Esegui il comando seguente. *Sostituisci SVM_name e con le tue informazioni. SnapLockAdmin*

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

SnapLockvolumi dei registri di controllo

Un SnapLock volume di log di SnapLock controllo contiene registri di controllo, che contengono i timestamp di eventi, ad esempio quando è stato creato un SnapLock amministratore, quando sono state eseguite operazioni di eliminazione con privilegi o quando è stato inserito un blocco a fini legali sui file. Il volume del registro SnapLock di controllo è un record di eventi non cancellabile.

È necessario creare un volume di registro di SnapLock controllo nella stessa SVM del SnapLock volume per le seguenti azioni:

- Per attivare o disattivare l'eliminazione con privilegi su un volume SnapLock Enterprise.
- Per applicare la conservazione a fini legali a un file in un volume SnapLock Compliance.

> ⚠ Warning
>
> - Il periodo minimo di conservazione per un volume SnapLock di log di controllo è di sei mesi. Fino alla scadenza di questo periodo di conservazione, il volume del registro di SnapLock controllo, la SVM e il file system ad esso associati non possono essere eliminati anche se il volume è stato creato in modalità SnapLock Enterprise.
> - Se un file viene eliminato utilizzando l'eliminazione privilegiata e il periodo di conservazione è più lungo del periodo di conservazione del volume, il volume del registro di controllo eredita il periodo di conservazione del file. Ad esempio, se un file con un periodo di conservazione di 10 mesi viene eliminato utilizzando l'eliminazione privilegiata e il periodo di conservazione del volume del registro di controllo è di sei mesi, il periodo di conservazione del volume del registro di controllo viene esteso a 10 mesi.

È possibile avere un solo volume di log di SnapLock controllo attivo in una SVM, ma può essere condiviso da più SnapLock volumi nella SVM. Per montare correttamente un volume SnapLock di log di controllo, impostate il percorso di giunzione su. `/snaplock_audit_log` Nessun altro volume può utilizzare questo percorso di giunzione, compresi i volumi che non sono volumi di registro di controllo.

È possibile trovare i log di SnapLock controllo nella `/snaplock_log` directory sotto la radice del volume del registro di controllo. Le operazioni di eliminazione con privilegi vengono registrate nella sottodirectory. `privdel_log` Le operazioni di inizio e fine di Legal Hold vengono registrate. `/snaplock_log/legal_hold_logs/` Tutti gli altri registri vengono archiviati nella sottodirectory. `system_log`

Puoi creare un volume di log di SnapLock controllo con la console Amazon FSxAWS CLI, l'API Amazon FSx e l'API CLI ONTAP e REST.

> **Note**
>
> Un volume di protezione dei dati (DP) non può essere utilizzato come volume di log di SnapLock controllo.

La procedura seguente spiega come creare un volume di log di SnapLock controllo sulla console Amazon FSx.

Per creare un volume di log di SnapLock controllo, la console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo volume inCreazione di volumi.
3. Nella sezione Avanzate, per SnapLock Configurazione, scegli Abilitato.

   Seleziona la casella di controllo per confermare l'avviso relativo all'attivazione SnapLock sul volume.
4. Per Audit log volume, scegli Abilitato.

   Assicurati che il percorso di giunzione sia impostato su`/snaplock_audit_log`.
5. Segui il resto della procedura per creare un nuovo volume inCreazione di volumi.
6. Scegli Conferma per creare il volume.

Per attivare il volume del log di SnapLock controllo con l'API Amazon FSx, usa `AuditLogVolume` in. `CreateSnaplockConfiguration`

Accesso ai dati in un volume SnapLock

È possibile utilizzare protocolli di file aperti come NFS e SMB per accedere ai dati in un SnapLock volume. La scrittura di dati su un SnapLock volume o la lettura di dati protetti da WORM non hanno alcun impatto sulle prestazioni.

È possibile copiare file tra SnapLock volumi con NFS e SMB, ma questi non manterranno le proprietà WORM sul volume di destinazione. SnapLock È necessario raccomandare nuovamente i file copiati in WORM per evitare che vengano modificati o eliminati. Per ulteriori informazioni, consulta Immissione dei file nello stato WORM.

È inoltre possibile replicare SnapLock i dati conSnapMirror, ma i volumi di origine e di destinazione devono essere SnapLock volumi con la stessa modalità di conservazione (ad esempio, entrambi devono essere Compliance o Enterprise).

Conformità SnapLock

Amazon FSx for NetApp ONTAP supporta SnapLock i volumi di conformità.

Utilizzo della conformità SnapLock

Questa sezione descrive i casi d'uso e le considerazioni per la modalità di conservazione della conformità.

Casi d'uso per la conformità SnapLock

È possibile scegliere la modalità di conservazione della conformità per i seguenti casi d'uso.

- È possibile utilizzare SnapLock Compliance per soddisfare mandati governativi o specifici del settore, come la regola SEC 17a-4 (f), la regola FINRA 4511 e il regolamento CFTC 1.31. SnapLock La conformità su Amazon FSx for NetApp ONTAP è stata valutata per questi mandati e regolamenti da. Cohasset Associates Per ulteriori informazioni, consulta il report di valutazione della conformità per Amazon FSx for NetApp ONTAP.
- Puoi utilizzare SnapLock Compliance per integrare o migliorare una strategia di protezione dei dati completa per combattere gli attacchi ransomware.

Considerazioni per la conformità SnapLock

Di seguito sono riportati alcuni elementi importanti da considerare sulla modalità di mantenimento della conformità.

- Dopo che un file è passato allo stato WORM (Write Once, Read Many) su un volume SnapLock Compliance, non può essere eliminato da nessun utente prima della scadenza del periodo di conservazione.
- Un volume SnapLock Compliance può essere eliminato solo quando i periodi di conservazione di tutti i file WORM sul volume sono scaduti e i file WORM sono stati eliminati dal volume.
- Non è possibile rinominare un volume SnapLock Compliance dopo la creazione.
- È possibile utilizzarlo SnapMirror per replicare i file WORM, ma il volume di origine e il volume di destinazione devono avere la stessa modalità di conservazione (ad esempio, entrambi devono essere Compliance).
- Un volume SnapLock Compliance non può essere convertito in un volume SnapLock Enterprise e viceversa.

Creazione di un volume di SnapLock conformità

Puoi creare un volume SnapLock Compliance con la console Amazon FSxAWS CLI, l'API Amazon FSx e l'API CLI ONTAP e REST.

Per creare un volume di SnapLock conformità con l'API Amazon FSx, utilizza `SnaplockType` in. `CreateSnaplockConfiguration`

La procedura seguente spiega come creare un volume SnapLock Compliance sulla console Amazon FSx.

Per creare un volume SnapLock Compliance sulla console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo volume inCreazione di volumi.
3. Nella sezione Avanzate, per SnapLock Configurazione, scegli Abilitato.

   Seleziona la casella di controllo per confermare l'avviso relativo all'attivazione SnapLock sul volume.
4. Per la modalità di conservazione, scegli Conformità.
5. Per Audit log Volume, scegli tra Abilitato e Disabilitato.

Se scegli Abilitato, assicurati che il percorso di giunzione sia impostato su`/snaplock_audit_log`.

Per ulteriori informazioni, consulta SnapLockvolumi dei registri di controllo.

6. Per Periodo di conservazione, inserisci i valori per Conservazione predefinita, Conservazione minima e Conservazione massima. Quindi scegli un'unità corrispondente per ciascuna.

   Per ulteriori informazioni, consulta Utilizzo del periodo di conservazione in SnapLock.

7. Per Autocommit, scegli tra Abilitato e Disabilitato.

   Se scegli Abilitato, per il periodo di autocommit, inserisci un valore e scegli l'unità Autocommit corrispondente.

   È possibile specificare un valore compreso tra 5 minuti e 10 anni.

   Per ulteriori informazioni, consulta Commit automatico.

8. Per la modalità di aggiunta del volume, scegli tra Abilitato e Disabilitato.

   Per ulteriori informazioni, consulta Modalità Volume-append.

9. Segui il resto della procedura per creare un nuovo volume inCreazione di volumi.
10. Scegli Conferma per creare il volume.

SnapLockImpresa

Amazon FSx for NetApp ONTAP supporta SnapLock i volumi Enterprise.

Usare Enterprise SnapLock

Questa sezione descrive i casi d'uso e le considerazioni per la modalità di conservazione Enterprise.

Casi d'uso per Enterprise SnapLock

È possibile scegliere la modalità di conservazione Enterprise per i seguenti casi d'uso.

- È possibile utilizzare SnapLock Enterprise per autorizzare solo utenti specifici a eliminare i file.
- È possibile utilizzare SnapLock Enterprise per migliorare l'integrità dei dati e la conformità interna dell'organizzazione.

- È possibile utilizzare SnapLock Enterprise per testare le impostazioni di conservazione prima di utilizzare SnapLock Compliance.

Considerazioni sull'utilizzo di Enterprise SnapLock

Di seguito sono riportati alcuni elementi importanti da considerare sulla modalità di conservazione Enterprise.

- È possibile utilizzare SnapMirror per replicare i file WORM, ma il volume di origine e il volume di destinazione devono avere la stessa modalità di conservazione (ad esempio, entrambi devono essere Enterprise).
- Un SnapLock volume non può essere convertito da Enterprise a Compliance o da Compliance a Enterprise.
- SnapLockEnterprise non supporta Legal Hold.

Eliminazione con privilegi

Una delle differenze principali tra SnapLock Enterprise e SnapLock Compliance è che un SnapLock amministratore può attivare l'eliminazione con privilegi su un volume SnapLock Enterprise per consentire l'eliminazione di un file prima della scadenza del periodo di conservazione del file. L'SnapLockamministratore è l'unico utente che può eliminare i file da un volume SnapLock Enterprise su cui sono state impostate politiche di conservazione attive. Per ulteriori informazioni, consulta Amministratore di SnapLock.

Puoi attivare o disattivare l'eliminazione privilegiata con la console Amazon FSx, AWS CLI l'API Amazon FSx e l'API ONTAP CLI e REST. Per attivare l'eliminazione privilegiata, devi prima creare un volume di log di SnapLock controllo nella stessa SVM del volume. SnapLock Per ulteriori informazioni, consulta SnapLockvolumi dei registri di controllo.

Per attivare l'eliminazione privilegiata con l'API Amazon FSx, `PrivilegedDelete` usa in. `CreateSnaplockConfiguration`

La procedura seguente spiega come attivare l'eliminazione privilegiata sulla console Amazon FSx.

Per attivare l'eliminazione privilegiata su un volume SnapLock Enterprise sulla console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo volume inCreazione di volumi.

3. Nella sezione Avanzate, per SnapLock Configurazione, scegli Abilitato.

   Seleziona la casella di controllo per confermare l'avviso relativo all'attivazione SnapLock sul volume.
4. Per la modalità di conservazione, scegli Enterprise.
5. Per Privileged Delete, scegliete Abilitato.
6. Segui il resto della procedura per creare un nuovo volume inCreazione di volumi.
7. Scegli Conferma per creare il volume.

> **Note**
>
> Non è possibile emettere un comando di eliminazione privilegiata per eliminare un file WORM (write once, read many) con un periodo di conservazione scaduto. È possibile eseguire una normale operazione di eliminazione dopo la scadenza del periodo di conservazione.

Puoi scegliere di disattivare l'eliminazione privilegiata in modo permanente, ma questa azione è irreversibile. Se l'eliminazione con privilegi è disattivata in modo permanente, non è necessario che un volume di registro di SnapLock controllo sia associato al SnapLock volume Enterprise.

Per disattivare definitivamente l'eliminazione privilegiata con l'API Amazon FSx, `PrivilegedDelete` usa in. `CreateSnaplockConfiguration`

Per disattivare definitivamente l'eliminazione privilegiata su un volume SnapLock Enterprise sulla console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo volume inCreazione di volumi.
3. Nella sezione Avanzate, per SnapLock Configurazione, scegli Abilitato.

   Seleziona la casella di controllo per confermare l'avviso relativo all'attivazione SnapLock sul volume.
4. Per la modalità di conservazione, scegli Enterprise.
5. Per Privileged Delete, scegli Disabilitato permanentemente.
6. Segui il resto della procedura per creare un nuovo volume inCreazione di volumi.

7. Scegli Conferma per creare il volume.

Creazione di un volume SnapLock Enterprise

Puoi creare un volume SnapLock Enterprise con la console Amazon FSxAWS CLI, l'API Amazon FSx e l'API CLI ONTAP e REST.

Per creare un volume SnapLock aziendale con l'API Amazon FSx, usa `SnaplockType` in. `CreateSnaplockConfiguration`

Per creare un volume SnapLock Enterprise sulla console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo volume inCreazione di volumi.
3. Nella sezione Avanzate, per SnapLock Configurazione, scegli Abilitato.

   Seleziona la casella di controllo per confermare l'avviso relativo all'attivazione SnapLock sul volume.
4. Per la modalità di conservazione, scegli Enterprise.
5. Per Audit log Volume, scegli tra Abilitato e Disabilitato.

   Se scegli Abilitato, assicurati che il percorso di giunzione sia impostato su/ `snaplock_audit_log`.

   Per ulteriori informazioni, consulta SnapLockvolumi dei registri di controllo.
6. Per Periodo di conservazione, inserisci i valori per Conservazione predefinita, Conservazione minima e Conservazione massima. Quindi scegli un'unità corrispondente per ciascuna.

   Per ulteriori informazioni, consulta Utilizzo del periodo di conservazione in SnapLock.
7. Per Autocommit, scegli tra Abilitato e Disabilitato.

   Se scegli Abilitato, per il periodo di autocommit, inserisci un valore e scegli l'unità Autocommit corrispondente.

   È possibile specificare un valore compreso tra 5 minuti e 10 anni.

   Per ulteriori informazioni, consulta Commit automatico.
8. Per Eliminazione con privilegi, scegli tra Abilitato, Disabilitato e Disabilitato permanentemente.

Per ulteriori informazioni, consulta Eliminazione con privilegi.

9. Per la modalità di aggiunta del volume, scegli tra Abilitato e Disabilitato.

   Per ulteriori informazioni, consulta Modalità Volume-append.

10. Segui il resto della procedura per creare un nuovo volume inCreazione di volumi.
11. Scegli Conferma per creare il volume.

Bypassare la modalità Enterprise

Se utilizzi la console Amazon FSx o l'API Amazon FSx, devi disporre dell'`fsx:BypassSnapLockEnterpriseRetention`autorizzazione IAM per eliminare un volume SnapLock Enterprise che contiene file WORM con politiche di conservazione attive.

Per ulteriori informazioni, consulta Eliminazione di volumi SnapLock.

Utilizzo del periodo di conservazione in SnapLock

Quando si crea un SnapLock volume, è possibile impostare un periodo di conservazione predefinito per il volume oppure impostare il periodo di conservazione per i file Write Once, Read Many (WORM) in modo esplicito. Durante il periodo di conservazione, non è possibile eliminare o modificare i file protetti da WORM. Il periodo di conservazione viene utilizzato per calcolare il tempo di conservazione. Ad esempio, se si esegue la transizione di un file a WORM il 14 luglio 2023 a mezzanotte e si imposta il periodo di conservazione su cinque anni, il periodo di conservazione sarà fino al 14 luglio 2028 a mezzanotte.

Per ulteriori informazioni su WORM, vedere. Immissione dei file nello stato WORM

Politiche relative al periodo di conservazione

Il periodo di conservazione è determinato dai valori assegnati ai seguenti parametri:

- Conservazione predefinita: il periodo di conservazione predefinito assegnato a un file WORM se non viene fornito un periodo di conservazione esplicito.
- Conservazione minima: il periodo di conservazione più breve che può essere assegnato a un file WORM.
- Conservazione massima: il periodo di conservazione più lungo che può essere assegnato a un file WORM.

> **Note**
>
> Anche dopo la scadenza del periodo di conservazione, non è possibile modificare un file WORM. È possibile solo eliminarlo o impostare un nuovo periodo di conservazione per riattivare la protezione WORM.

È possibile specificare il periodo di conservazione utilizzando diverse unità di tempo. La tabella seguente elenca gli intervalli specifici supportati.

Type	Valore	Note
Secondi	0 - 65.535	
Minuti	0 - 65.535	
Ore	0 - 24	
Giorni	0 - 365	
Mesi	0 -12	
Years	0 - 100	
Tempo infinito	-	Conserva i file per sempre. Disponibile per Conservazione predefinita, Conservazione massima e Conservazione minima.
Non specificato*	-	Conserva i file fino a quando non viene impostato un periodo di conservazione. Disponibile solo per la conservazione predefinita.

* Quando si trasferiscono file a WORM con un periodo di conservazione non specificato, viene assegnato il periodo di conservazione minimo configurato per il SnapLock volume. Quando si passa ai file protetti da WORM a un periodo di conservazione assoluto, il nuovo periodo di conservazione deve essere superiore al periodo minimo impostato in precedenza sui file.

Periodo di conservazione scaduto

Dopo la scadenza del periodo di conservazione di un file WORM, è possibile eliminare il file o impostare un nuovo periodo di conservazione per riattivare la protezione WORM. I file WORM non vengono eliminati automaticamente dopo la scadenza del periodo di conservazione. Non è ancora possibile modificare il contenuto di un file WORM, anche dopo la scadenza del periodo di conservazione.

Impostazione del periodo di conservazione di un volume SnapLock

Puoi impostare il periodo di conservazione di un SnapLock volume con la console Amazon FSxAWS CLI, l'API Amazon FSx e l'API CLI ONTAP e REST.

Per impostare il periodo di conservazione con l'API Amazon FSx, utilizza la `SnaplockRetentionPeriod`configurazione.

La procedura seguente spiega come impostare il periodo di conservazione sulla console Amazon FSx.

Per impostare il periodo di conservazione di un SnapLock volume sulla console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo volume inCreazione di volumi.
3. Nella sezione Avanzate, per SnapLock Configurazione, scegli Abilitato.

   Seleziona la casella di controllo per confermare l'avviso relativo all'attivazione SnapLock sul volume.
4. Per Periodo di conservazione, inserisci i valori per Conservazione predefinita, Conservazione minima e Conservazione massima. Quindi scegli un'unità corrispondente per ciascuna.
5. Segui il resto della procedura per creare un nuovo volume inCreazione di volumi.
6. Scegli Conferma per creare il volume.

Immissione dei file nello stato WORM

Questa sezione illustra come passare i file allo stato WORM (Write Once, Read Many). Viene inoltre illustrata la modalità volume-append, che consente di scrivere dati in modo incrementale su file protetti da WORM.

Commit automatico

È possibile utilizzare l'autocommit per trasferire i file a WORM se non sono stati modificati per un periodo di tempo specificato. Puoi attivare l'autocommit con la console Amazon FSx, AWS CLI l'API Amazon FSx e l'API ONTAP CLI e REST.

Puoi specificare un periodo di autocommit compreso tra cinque minuti e 10 anni. La tabella seguente elenca gli intervalli specifici supportati.

Unità	Valore
Minuti	5 - 65.535
Ore	1 - 65.535
Giorni	1 - 3.650
Mesi	1 - 120
Years	1 - 10

Per attivare l'autocommit con l'API Amazon FSx, `AutocommitPeriod` usa in. `CreateSnaplockConfiguration`

La procedura seguente spiega come attivare l'autocommit sulla console Amazon FSx.

Per attivare l'autocommit sulla console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo volume inCreazione di volumi.
3. Nella sezione Avanzate, per SnapLock Configurazione, scegli Abilitato.

   Seleziona la casella di controllo per confermare l'avviso relativo all'attivazione SnapLock sul volume.

4. Per Autocommit, scegli Abilitato.
5. Per il periodo di autocommit, inserisci un valore e scegli l'unità Autocommit corrispondente.

   È possibile specificare un valore compreso tra 5 minuti e 10 anni.
6. Segui il resto della procedura per creare un nuovo volume inCreazione di volumi.
7. Scegli Conferma per creare il volume.

Modalità Volume-append

Non è possibile modificare i dati esistenti in un file protetto da Worm. Tuttavia, SnapLock consente di mantenere la protezione dei dati esistenti utilizzando file allegabili con WORM. Ad esempio, è possibile generare file di registro o conservare i dati di streaming audio o video mentre si scrivono dati su di essi in modo incrementale. Puoi attivare o disattivare la modalità volume-append con la console Amazon FSx, l'API AWS CLI Amazon FSx e l'API CLI e REST. ONTAP

Requisiti per l'aggiornamento della modalità volume-append

- Il SnapLock volume deve essere smontato.
- Il SnapLock volume deve essere privo di copie istantanee e dati utente.

Per attivare la modalità volume-append con l'API Amazon FSx, usa in. `VolumeAppendModeEnabled` `CreateSnaplockConfiguration`

La procedura seguente spiega come attivare la modalità volume-append sulla console Amazon FSx.

Per attivare la modalità volume-append sulla console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo volume inCreazione di volumi.
3. Nella sezione Avanzate, per SnapLock Configurazione, scegli Abilitato.

   Seleziona la casella di controllo per confermare l'avviso relativo all'attivazione SnapLock sul volume.
4. Per la modalità di aggiunta del volume, scegli Abilitato.
5. Segui il resto della procedura per creare un nuovo volume inCreazione di volumi.

6. Scegli Conferma per creare il volume.

Conservazione basata sugli eventi (EBR)

È possibile utilizzare la conservazione basata sugli eventi (EBR) per creare politiche personalizzate con periodi di conservazione associati. Ad esempio, è possibile trasferire tutti i file in un percorso specificato a WORM e impostare il periodo di conservazione per un anno con i `snaplock event-retention policy create` comandi and. `snaplock event-retention apply` Quando si utilizza EBR, è necessario specificare un volume, una directory o un file. Il periodo di conservazione selezionato al momento della creazione della politica EBR viene applicato a tutti i file nel percorso specificato.

EBR è supportato dalla ONTAP CLI e dall'API REST.

> **Note**
>
> ONTAPnon supporta EBR con volumi. FlexGroup

Le seguenti procedure spiegano come creare, applicare, modificare ed eliminare una politica EBR. Devi essere un SnapLock amministratore (avere il `vsadmin-snaplock` ruolo) per completare queste attività nella ONTAP CLI. Per ulteriori informazioni, consulta Amministratore di SnapLock.

Per creare una politica EBR nella CLI ONTAP

Esegui il comando seguente. Sostituisci *p1* e *«10 anni» con le tue informazioni.*

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

Per applicare una politica EBR nella CLI ONTAP

Esegui il comando seguente. Sostituisci *p1* e *slc* con le tue informazioni. È possibile aggiungere un percorso dopo la barra (/) se si desidera specificare un percorso particolare per la politica EBR. Altrimenti, questo comando applica la politica EBR a tutti i file del volume.

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

Per modificare una politica EBR nella CLI ONTAP

Esegui il comando seguente. Sostituisci *p1* e *«5 anni» con le tue informazioni.*

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

Per eliminare una politica EBR nella CLI ONTAP

Esegui il comando seguente. Sostituisci *p1* con le tue informazioni.

```
vs1::> snaplock event-retention policy delete -name p1
```

Comandi correlati nel NetAppDocumentation Center:

- interruzione della conservazione degli eventi snaplock
- snaplock event-retention show-vservers
- snaplock event-retention show
- mostra la politica di conservazione degli eventi di snaplock

Conservazione a fini legali

È possibile conservare i file WORM per un periodo di tempo indefinito utilizzando Legal Hold. La conservazione a fini legali viene generalmente utilizzata per scopi contenziosi. Un file WORM soggetto a conservazione legale non può essere eliminato finché tale conservazione non viene revocata.

Legal Hold è supportato dalla ONTAP CLI e dall'API REST.

> **Note**
>
> ONTAPnon supporta Legal Hold con FlexGroup volumi.

Le seguenti procedure spiegano come avviare e terminare una conservazione a fini legali. Devi essere un SnapLock amministratore (avere il `vsadmin-snaplock` ruolo) per completare queste attività nella ONTAP CLI. Per ulteriori informazioni, consulta Amministratore di SnapLock.

Per avviare una conservazione a fini legali su un file in un volume SnapLock Compliance con la ONTAP CLI

Esegui il comando seguente. *Sostituisci litigation1, slc_vol1 e file1 con le tue informazioni.*

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Per avviare una conservazione a fini legali su tutti i file in un volume SnapLock Compliance con la ONTAP CLI

Esegui il comando seguente. Sostituisci *litigation1 e slc_vol1* con le tue informazioni.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -path /
```

Per terminare una conservazione a fini legali su un file in un volume di SnapLock conformità con la ONTAP CLI

Esegui il comando seguente. *Sostituisci litigation1, slc_vol1 e file1 con le tue informazioni.*

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Per porre fine alla conservazione a fini legali su tutti i file in un volume SnapLock Compliance con la ONTAP CLI

Esegui il comando seguente. Sostituisci *litigation1 e slc_vol1* con le tue informazioni.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -path /
```

> **Note**
>
> Ti consigliamo di monitorarli `-operation-status` con il `snaplock legal-hold show` comando quando esegui un blocco legale per assicurarti che non abbia esito negativo.

Comandi correlati nel NetAppDocumentation Center:

- snaplock legal-hold abort

- file di dump snaplock legal-hold
- controversie legali su snaplock legal-hold dump-
- snaplock legal-hold show

Backup dei volumi SnapLock

È possibile eseguire il backup SnapLock dei volumi per una protezione aggiuntiva dei dati. Quando si ripristina un SnapLock volume, le impostazioni originali del volume, ad esempio la conservazione predefinita, la conservazione minima e la conservazione massima, vengono preservate. Vengono inoltre mantenute le impostazioni Write once, read many (WORM) e Legal Hold.

> **Note**
>
> Non è possibile eseguire il backup di un SnapLock FlexGroup volume.

È possibile ripristinare il backup di un SnapLock volume come volume SnapLock o come non SnapLock volume. Tuttavia, non è possibile ripristinare il backup di un prodotto diverso da un SnapLock volume. SnapLock

Per ulteriori informazioni sui backup, consultare Utilizzo dei backup.

Eliminazione di volumi SnapLock

È possibile eliminare un volume SnapLock Compliance se i periodi di conservazione di tutti i file WORM (Write Once, Read Many) in esso contenuti sono scaduti.

> **Note**
>
> Quando chiudi un account Account AWS che contiene Compliance i SnapLock Enterprise nostri volumi AWS e FSx for ONTAP sospende il tuo account per 90 giorni con i dati intatti. Se non riapri l'account entro questi 90 giorni, AWS elimina i dati, compresi i dati in SnapLock volumi, indipendentemente dalle impostazioni di conservazione.

Puoi eliminare un volume SnapLock Enterprise in qualsiasi momento se disponi delle autorizzazioni appropriate. Devi essere un amministratore di Amazon FSx. Inoltre, indipendentemente dal fatto che utilizzi la console Amazon FSx o l'API Amazon FSx, devi disporre dell'autorizzazione IAM

`fsx:BypassSnapLockEnterpriseRetention` IAM per eliminare un volume SnapLock Enterprise che contiene dati WORM con una politica di conservazione attiva.

> **Warning**
>
> Il periodo minimo di conservazione per un volume di log di SnapLock controllo è di sei mesi. Fino alla scadenza di questo periodo di conservazione non è possibile eliminare il volume del registro di SnapLock controllo, la macchina virtuale di archiviazione (SVM) o il file system associato alla SVM, anche se il volume è stato creato in modalità Enterprise. SnapLock Per ulteriori informazioni, consulta SnapLockvolumi dei registri di controllo.

Per eliminare un volume SnapLock Enterprise sulla console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli Volumes.
3. Scegli il volume che desideri eliminare.
4. Da Azioni, scegli Elimina volume.
5. Per Bypass SnapLock Enterprise Retention, scegli Sì.
6. Nella finestra di dialogo di conferma, scegli una delle seguenti opzioni per Crea backup finale:
   - Scegli Sì per effettuare un backup finale del volume. Viene visualizzato il nome del backup finale.
   - Scegli No se non desideri un backup finale del volume. Ti viene chiesto di confermare che, una volta eliminato il volume, i backup automatici non sono più disponibili.
7. Conferma l'eliminazione del volume inserendo il **`delete`** campo Conferma eliminazione.
8. Scegli Elimina volume/i.

Utilizzo di Microsoft Active Directory in FSx for ONTAP

Amazon FSx funziona con Microsoft Active Directory per l'integrazione con gli ambienti esistenti. Active Directory è il servizio di directory di Microsoft utilizzato per archiviare informazioni sugli oggetti presenti nella rete e per aiutare gli amministratori e gli utenti a trovare e utilizzare tali informazioni. Questi oggetti includono in genere risorse condivise, come file server e account di utenti e computer di rete.

Facoltativamente, puoi aggiungere le tue macchine virtuali di archiviazione (SVM) FSx for ONTAP al tuo dominio Active Directory per fornire l'autenticazione degli utenti e il controllo degli accessi a livello di file e cartella. I client Server Message Block (SMB) possono quindi utilizzare le identità utente esistenti in Active Directory per autenticarsi e accedere ai volumi SVM. Gli utenti possono utilizzare le identità esistenti per controllare l'accesso a singoli file e cartelle. Inoltre, puoi migrare file e cartelle esistenti e le relative configurazioni ACL (Security Access Control List) su Amazon FSx senza alcuna modifica.

Quando unisci Amazon FSx for NetApp ONTAP a un Active Directory, unisci le SVM del file system ad Active Directory in modo indipendente. Ciò significa che puoi avere un file system con alcune SVM unite a un Active Directory e altre SVM che non lo sono.

Dopo aver aggiunto una SVM a un Active Directory, è possibile aggiornare le seguenti proprietà di configurazione di Active Directory:

- Indirizzi IP del server DNS
- Nome utente e password dell'account del servizio Active Directory autogestiti

Argomenti

Prerequisiti per aggiungere una SVM a un Microsoft AD autogestito

Prima di aggiungere un SVM FSx for ONTAP a un dominio Microsoft AD autogestito, assicurati che Active Directory e la rete soddisfino i requisiti descritti nelle sezioni seguenti.

Argomenti

Requisiti di Active Directory locale

Assicurati di disporre già di un Microsoft AD locale o di un altro Microsoft AD autogestito a cui puoi unirti alla SVM. Questo Active Directory dovrebbe avere la seguente configurazione:

- Il livello di funzionalità del dominio del controller di dominio Active Directory è Windows Server 2000 o superiore.
- Active Directory utilizza un nome di dominio che non è in formato SLD (Single Label Domain). Amazon FSx non supporta i domini SLD.
- Se hai definito siti Active Directory, assicurati che le sottoreti nel VPC associato al file system FSx for ONTAP siano definite negli stessi siti di Active Directory e che non esistano conflitti tra le sottoreti VPC e le sottoreti sui siti Active Directory.

> **Note**
>
> Se si utilizza AWS Directory Service, FSx for ONTAP non supporta l'aggiunta di SVM a Simple Active Directory.

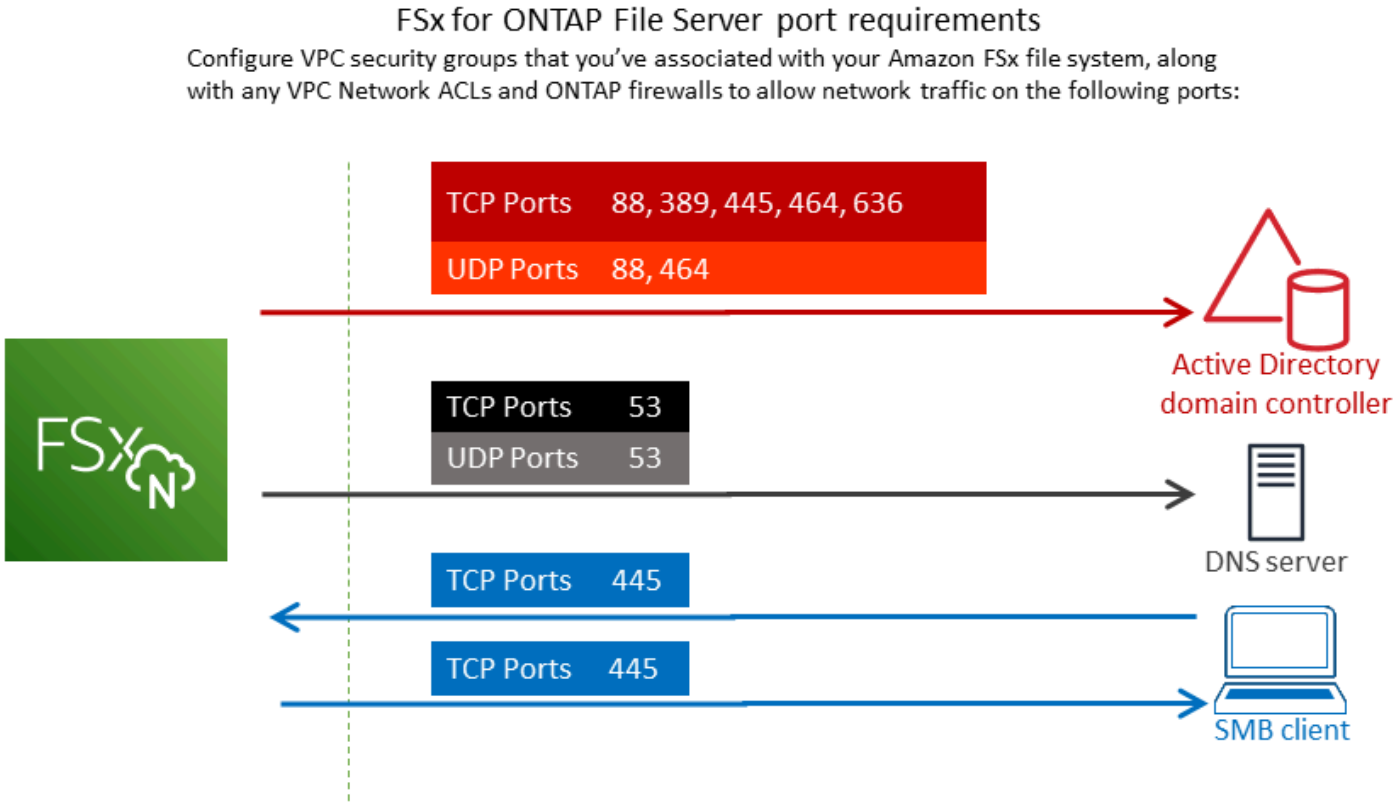
Requisiti relativi alla configurazione della rete

Assicuratevi di disporre delle seguenti configurazioni di rete e di disporre delle informazioni associate.

> **Important**
>
> Affinché una SVM si unisca ad Active Directory, è necessario assicurarsi che le porte documentate in questo argomento consentano il traffico tra tutti i controller di dominio Active Directory e entrambi gli indirizzi IP iSCSI (interfacce logiche iscsi_1 e iscsi_2) sulla SVM.

- Gli indirizzi IP del server DNS e del controller di dominio Active Directory.

- Connettività tra Amazon VPC in cui stai creando il file system e il tuo Active Directory autogestito utilizzando AWS Direct Connect, AWS VPNo. AWS Transit Gateway
- Il gruppo di sicurezza e gli ACL di rete VPC per le sottoreti su cui si sta creando il file system devono consentire il traffico sulle porte e nelle direzioni mostrate nel diagramma seguente.



Il ruolo di ciascuna porta è descritto nella tabella seguente.

Protocollo	Porte	Ruolo
TCP/UDP	53	Domain Name System (DNS)
TCP/UDP	88	Autenticazione Kerberos
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)
TCP	445	Condivisione di file SMB di Servizi directory
TCP/UDP	464	Modifica/reimpostazione della password

Protocollo	Porte	Ruolo
TCP	636	Lightweight Directory Access Protocol su TLS/SSL (LDAPS)

- Queste regole del traffico devono inoltre essere rispecchiate sui firewall che si applicano a ciascuno dei controller di dominio Active Directory, server DNS, client FSx e amministratori FSx.

> **Important**
>
> Sebbene i gruppi di sicurezza Amazon VPC richiedano l'apertura delle porte solo nella direzione di avvio del traffico di rete, la maggior parte dei firewall Windows e degli ACL di rete VPC richiedono che le porte siano aperte in entrambe le direzioni.

Requisiti degli account di servizio Active Directory

Assicurati di disporre di un account di servizio nel tuo account Microsoft AD autogestito con autorizzazioni delegate per aggiungere computer al dominio. Un account di servizio è un account utente di Active Directory autogestito a cui sono state delegate determinate attività.

All'account di servizio devono essere delegate almeno le seguenti autorizzazioni nell'unità organizzativa a cui si accede alla SVM:

- Possibilità di reimpostare le password
- Possibilità di impedire agli account di leggere e scrivere dati
- Possibilità di impostare la `msDS-SupportedEncryptionTypes` proprietà sugli oggetti del computer
- Capacità convalidata di scrittura sull'hostname DNS
- Capacità convalidata di scrivere sul nome principale del servizio
- Capacità di creare ed eliminare oggetti informatici
- Capacità convalidata di leggere e scrivere le restrizioni relative all'account

Queste rappresentano il set minimo di autorizzazioni necessarie per unire gli oggetti del computer ad Active Directory. Per ulteriori informazioni, consulta l'argomento della documentazione di Windows Server Errore: accesso negato quando utenti non amministratori a cui è stato delegato il controllo tentano di aggiungere computer a un controller di dominio.

Per ulteriori informazioni sulla creazione di un account di servizio con le autorizzazioni corrette, consulta. Delega delle autorizzazioni al tuo account di servizio Amazon FSx

> **Important**
>
> Amazon FSx richiede un account di servizio valido per tutta la durata del file system Amazon FSx. Amazon FSx deve essere in grado di gestire completamente il file system ed eseguire attività che richiedono l'annullamento e il ricongiungimento delle risorse al tuo dominio Active Directory. Queste attività includono la sostituzione di un file system o SVM guasto o l'applicazione di patch al software ONTAP. NetApp Mantieni aggiornate le informazioni di configurazione di Active Directory con Amazon FSx, incluse le credenziali dell'account di servizio. Per ulteriori informazioni, vedi Mantenere aggiornata la configurazione di Active Directory con Amazon FSx.

Se è la prima volta che utilizzate AWS FSx for ONTAP, assicuratevi di completare i passaggi di configurazione iniziali prima di iniziare l'integrazione con Active Directory. Per ulteriori informazioni, consulta Configurazione di FSx per ONTAP.

> **Important**
>
> Non spostare oggetti informatici creati da Amazon FSx nell'unità organizzativa dopo la creazione delle SVM o eliminare Active Directory mentre la SVM è unita ad essa. In questo modo le tue SVM potrebbero essere configurate in modo errato.

Procedure consigliate per l'utilizzo di Active Directory

Ecco alcuni suggerimenti e linee guida da prendere in considerazione quando unisci Amazon FSx for NetApp ONTAP SVM alla tua Microsoft Active Directory autogestita. Tieni presente che sono consigliate come best practice, ma non obbligatorie.

Delega delle autorizzazioni al tuo account di servizio Amazon FSx

Assicurati di configurare l'account di servizio che fornisci ad Amazon FSx con le autorizzazioni minime richieste. Inoltre, separa l'unità organizzativa (OU) dagli altri problemi relativi ai controller di dominio.

Per aggiungere le SVM Amazon FSx al tuo dominio, assicurati che l'account del servizio disponga di autorizzazioni delegate. I membri del gruppo Domain Admins dispongono di autorizzazioni sufficienti per eseguire questa attività. Tuttavia, è consigliabile utilizzare un account di servizio che disponga solo delle autorizzazioni minime necessarie per eseguire questa operazione. La procedura seguente mostra come delegare solo le autorizzazioni necessarie per aggiungere le SVM FSx for ONTAP al proprio dominio.

Esegui questa procedura su un computer che fa parte della tua directory e su cui è installato lo snap-in MMC Active Directory User and Computers.

Per creare un account di servizio per il dominio Microsoft Active Directory

1. Assicurati di aver effettuato l'accesso come amministratore di dominio per il tuo dominio Microsoft Active Directory.
2. Aprire lo snap-in MMC per utenti e computer di Active Directory.
3. Nel riquadro attività, espandere il nodo del dominio.
4. Individua e apri il menu contestuale (fai clic con il pulsante destro del mouse) per l'unità organizzativa che desideri modificare, quindi scegli Controllo delegato.
5. Nella pagina Delegation of Control Wizard, scegli Avanti.
6. Scegli Aggiungi per aggiungere un utente specifico o un gruppo specifico per Utenti e gruppi selezionati, quindi scegli Avanti.
7. Nella pagina Tasks to Delegate (Operazioni da delegare), selezionare Create a custom task to delegate (Crea un'operazione personalizzata per eseguire la delega), quindi scegliere Next (Avanti).
8. Scegli Solo i seguenti oggetti nella cartella, quindi scegli Oggetti computer.
9. Scegliete Crea oggetti selezionati in questa cartella e Elimina gli oggetti selezionati in questa cartella. Quindi scegli Successivo.
10. In Mostra queste autorizzazioni, assicurati che siano selezionate Generale e Specifico della proprietà.
11. Per Autorizzazioni, scegli quanto segue:

    - Reimpostazione della password
    - Leggi e scrivi le restrizioni dell'account
    - Nome host DNS di scrittura convalidato
    - Nome principale del servizio di scrittura convalidato

- Scrivi MSDs- SupportedEncryptionTypes

12. Scegli Next (Avanti), quindi scegli Finish (Fine).
13. Chiudere lo snap-in MMC Utente e computer di Active Directory.

> **Important**
>
> Non spostare oggetti informatici creati da Amazon FSx nell'unità organizzativa dopo la creazione delle SVM. In questo modo le tue SVM verranno configurate in modo errato.

Mantenere aggiornata la configurazione di Active Directory con Amazon FSx

Per una disponibilità ininterrotta delle SVM Amazon FSx, aggiorna la configurazione Active Directory (AD) autogestita di una SVM quando modifichi la configurazione AD autogestita.

Ad esempio, supponiamo che il tuo AD utilizzi una politica di reimpostazione della password basata sul tempo. In questo caso, non appena la password viene reimpostata, assicurati di aggiornare la password dell'account del servizio con Amazon FSx. A tale scopo, utilizza la console Amazon FSx, l'API Amazon FSx o. AWS CLI Allo stesso modo, se gli indirizzi IP del server DNS cambiano per il tuo dominio Active Directory, non appena si verifica la modifica aggiorna gli indirizzi IP del server DNS con Amazon FSx.

Se c'è un problema con la configurazione AD autogestita aggiornata, lo stato SVM passa a Misconfiguration. Questo stato mostra un messaggio di errore e un'azione consigliata accanto alla descrizione SVM nella console, nell'API e nella CLI. Se si verifica un problema con la configurazione AD della SVM, assicuratevi di intraprendere le azioni correttive consigliate per le proprietà di configurazione. Se il problema viene risolto, verificate che lo stato della SVM cambi in Created.

Per ulteriori informazioni, consultare Aggiornamento di una configurazione SVM Active Directory esistente utilizzando l'API AWS Management Console, e AWS CLI e Modificare una configurazione di Active Directory utilizzando la CLI ONTAP.

Utilizzo di gruppi di sicurezza per limitare il traffico all'interno del VPC

Per limitare il traffico di rete nel tuo cloud privato virtuale (VPC), puoi implementare il principio del privilegio minimo nel tuo VPC. In altre parole, puoi limitare le autorizzazioni al minimo necessario.

A tale scopo, utilizzate le regole del gruppo di sicurezza. Per ulteriori informazioni, vedi Gruppi di sicurezza Amazon VPC.

Creazione di regole per i gruppi di sicurezza in uscita per l'interfaccia di rete del file system

Per una maggiore sicurezza, prendi in considerazione la configurazione di un gruppo di sicurezza con regole del traffico in uscita. Queste regole dovrebbero consentire il traffico in uscita solo verso i controller dei domini AD autogestiti o all'interno della sottorete o del gruppo di sicurezza. Applica questo gruppo di sicurezza al VPC associato all'interfaccia di rete elastica del tuo file system Amazon FSx. Per ulteriori informazioni, consulta Controllo degli accessi ai file system con Amazon VPC.

Unire SVM a Microsoft Active Directory

La tua organizzazione potrebbe gestire identità e dispositivi utilizzando Active Directory, sia in locale che nel cloud. Con FSx for ONTAP, puoi aggiungere le tue SVM direttamente al tuo dominio Active Directory esistente nei seguenti modi:

- Aggiungere nuove SVM a un'Active Directory al momento della creazione:
  - Utilizzando l'opzione di creazione Standard nella console Amazon FSx per creare un nuovo file system FSx for ONTAP, puoi unire la SVM predefinita a un'Active Directory autogestita. Per ulteriori informazioni, consulta Per creare un file system (console).
  - Utilizzo della console Amazon FSx o dell'API Amazon FSx per creare una nuova SVM su un file system FSx for ONTAP esistente. AWS CLI Per ulteriori informazioni, consulta Creazione di una macchina virtuale di archiviazione.
- Unire SVM esistenti a un Active Directory:
  - Utilizzo dell'API AWS Management Console AWS CLI, e per aggiungere una SVM a un'Active Directory e per riprovare a unire una SVM a un'Active Directory se il tentativo iniziale di unione non è riuscito. È inoltre possibile aggiornare alcune proprietà di configurazione di Active Directory per le SVM che sono già unite a un Active Directory. Per ulteriori informazioni, consulta Gestione delle configurazioni SVM Active Directory.
  - Utilizzo della CLI NetApp ONTAP o dell'API REST per unire, ritentare di unire e rimuovere configurazioni SVM Active Directory. Per ulteriori informazioni, consulta Gestione della configurazione SVM Active Directory tramite la CLI NetApp .

> **Important**
>
> - Amazon FSx registra i record DNS per una SVM solo se utilizzi Microsoft DNS come servizio DNS predefinito. Se utilizzi un DNS di terze parti, devi configurare manualmente le voci DNS per le tue SVM Amazon FSx dopo averle create.
> - Se si utilizza AWS Managed Microsoft AD, è necessario specificare un gruppo come AWS Delegated FSx Administrators AWS , Delegated Administrators o un gruppo personalizzato con autorizzazioni delegate all'unità organizzativa.

Quando si aggiunge un SVM FSx for ONTAP direttamente a un Active Directory autogestito, l'SVM risiede nella stessa foresta di Active Directory (il contenitore logico più importante in una configurazione Active Directory che contiene domini, utenti e computer) e nello stesso dominio di Active Directory degli utenti e delle risorse esistenti, inclusi i file server esistenti.

Informazioni necessarie per aggiungere un SVM a un Active Directory

È necessario fornire le seguenti informazioni su Active Directory quando si unisce un SVM a un Active Directory, indipendentemente dall'operazione API scelta:

- Il nome NetBIOS dell'oggetto computer Active Directory da creare per la SVM. Questo è il nome della SVM in Active Directory, che deve essere univoco all'interno di Active Directory. Non utilizzare il nome NetBIOS del dominio principale. Il nome NetBIOS non può superare i 15 caratteri.
- Il nome di dominio completo (FQDN) del tuo Active Directory. Il nome di dominio completo non può superare i 255 caratteri.

  > **Note**
  >
  > Il nome di dominio completo non può essere nel formato SLD (Single Label Domain). Amazon FSx non supporta i domini SLD.

- Fino a tre indirizzi IP dei server DNS o degli host di dominio del tuo dominio.

  Gli indirizzi IP del server DNS e gli indirizzi IP dei controller di dominio Active Directory possono rientrare in qualsiasi intervallo di indirizzi IP, ad eccezione di:

  - Indirizzi IP che entrano in conflitto con gli indirizzi IP di proprietà di Amazon Web Services. Regione AWS Per un elenco di indirizzi AWS IP per regione, consulta gli intervalli di indirizzi AWS IP.
  - Indirizzi IP nel seguente intervallo di blocchi CIDR: 198.19.0.0/16
- Nome utente e password per un account di servizio sul tuo dominio Active Directory per Amazon FSx da utilizzare per aggiungere SVM al dominio Active Directory. Per ulteriori informazioni sui requisiti degli account di servizio, consulta. Requisiti degli account di servizio Active Directory
- (Facoltativo) L'unità organizzativa (OU) del dominio a cui aderisci alla SVM.

> **Note**
>
> Se si aggiunge la SVM a un' AWS Directory Service Active Directory, è necessario fornire un'unità organizzativa che rientri nell'unità organizzativa predefinita AWS Directory Service creata per gli oggetti di directory a cui sono correlati. AWS Questo perché AWS Directory Service non fornisce l'accesso all'`Computers`unità organizzativa predefinita di Active Directory. Ad esempio, se il dominio Active Directory è`example.com`, è possibile specificare la seguente unità organizzativa:`OU=Computers,OU=example,DC=example,DC=com`.

- (Facoltativo) Il gruppo di dominio a cui stai delegando l'autorità per eseguire azioni amministrative sul tuo file system. Ad esempio, questo gruppo di domini potrebbe gestire le condivisioni di file Windows SMB, acquisire la proprietà di file e cartelle e così via. Se non specifichi questo gruppo, Amazon FSx delega questa autorità al gruppo Domain Admins nel tuo dominio Active Directory per impostazione predefinita.

Gestione delle configurazioni SVM Active Directory

Questa sezione descrive come utilizzare l'API AWS Management Console AWS CLI, FSx e la CLI ONTAP per effettuare le seguenti operazioni:

- Unire una SVM esistente a un Active Directory
- Modifica di una configurazione SVM Active Directory esistente
- Rimozione di SVM da un Active Directory

Per rimuovere una SVM da un Active Directory, è necessario utilizzare l' NetApp ONTAP CLI.

Argomenti

Unire una SVM a un Active Directory utilizzando l'API e AWS Management ConsoleAWS CLI

Utilizzare la procedura seguente per unire una SVM esistente a un Active Directory. In questa procedura, la SVM non è già aggiunta a un Active Directory.

Per unire una SVM a un Active Directory () AWS Management Console

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli la SVM che desideri aggiungere a un Active Directory:

   - Nel riquadro di navigazione a sinistra, scegli File system, quindi scegli il file system ONTAP con l'SVM che desideri aggiornare.
   - Scegli la scheda Storage virtual machines.

   —Oppure—

   - Per visualizzare un elenco di tutte le SVM disponibili, nel riquadro di navigazione a sinistra, espandi ONTAP e scegli Storage virtual machines. Viene visualizzato un elenco di tutte le SVM del Regione AWS tuo account in.

   Seleziona la SVM che desideri aggiungere a un Active Directory dall'elenco.
3. In alto a destra del pannello di riepilogo SVM, scegliete Azioni > Unisci/Aggiorna Active Directory. Viene visualizzata la finestra Unisci SVM a Active Directory.
4. Immettete le seguenti informazioni per l'Active Directory a cui state unendo l'SVM:

   - Il nome NetBIOS dell'oggetto computer Active Directory da creare per la SVM. Questo è il nome della SVM in Active Directory, che deve essere univoco all'interno di Active Directory. Non utilizzare il nome NetBIOS del dominio principale. Il nome NetBIOS non può superare i 15 caratteri.

- Il nome di dominio completo (FQDN) del tuo Active Directory. Il nome di dominio non può superare i 255 caratteri.
- Indirizzi IP dei server DNS: gli indirizzi IPv4 dei server DNS del tuo dominio.
- Nome utente dell'account di servizio: il nome utente dell'account di servizio nell'Active Directory esistente. Non includere un prefisso o un suffisso di dominio. Ad esempio`EXAMPLE\ADMIN`, solo per. `ADMIN`
- Password dell'account di servizio: la password per l'account di servizio.
- Conferma password: la password per l'account di servizio.
- (Facoltativo) Unità organizzativa (OU): il nome del percorso distinto dell'unità organizzativa a cui desideri unire la tua SVM.
- Gruppo di amministratori di file system delegati: nome del gruppo in Active Directory che può amministrare il file system.

  Se si utilizza AWS Managed Microsoft AD, è necessario specificare un gruppo come AWS Delegated FSx Administrators AWS , Delegated Administrators o un gruppo personalizzato con autorizzazioni delegate all'unità organizzativa.

  Se ti stai unendo a un Active Directory autogestito, usa il nome del gruppo in Active Directory. Il gruppo predefinito è`Domain Admins`.

5. Scegliete Unisciti ad Active Directory per aggiungere la SVM ad Active Directory utilizzando la configurazione fornita.

Per unire una SVM a un'Active Directory (AWS CLI)

- Per unire un SVM FSx for ONTAP a un Active Directory, utilizzate il comando update-storage-virtual-machineCLI (o l'operazione UpdateStorageVirtualMachineAPI equivalente), come illustrato nell'esempio seguente.

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
\
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Dopo aver creato correttamente la macchina virtuale di storage, Amazon FSx ne restituisce la descrizione in formato JSON, come illustrato nell'esempio seguente.


```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
```

```
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],

  }
}
```

Aggiornamento di una configurazione SVM Active Directory esistente utilizzando l'API AWS Management Console, e AWS CLI

Utilizzare la procedura seguente per aggiornare la configurazione Active Directory di una SVM già unita a un Active Directory.

Per aggiornare una configurazione SVM Active Directory () AWS Management Console

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli la SVM da aggiornare come segue:

   - Nel riquadro di navigazione a sinistra, scegli File system, quindi scegli il file system ONTAP con l'SVM che desideri aggiornare.
   - Scegli la scheda Storage virtual machines.

   —Oppure—

   - Per visualizzare un elenco di tutte le SVM disponibili, nel riquadro di navigazione a sinistra, espandi ONTAP e scegli Storage virtual machines.

   Seleziona la SVM che desideri aggiornare dall'elenco.
3. Nel pannello Riepilogo SVM, scegliete Azioni > Unisci/Aggiorna Active Directory. Viene visualizzata la finestra di configurazione di Update SVM Active Directory.
4. È possibile aggiornare le seguenti proprietà di configurazione di Active Directory in questa finestra.

- Indirizzi IP dei server DNS: gli indirizzi IPv4 dei server DNS del tuo dominio.
- Nome utente dell'account di servizio: il nome utente dell'account di servizio nell'Active Directory esistente. Non includere un prefisso o un suffisso di dominio. Per `EXAMPLE\ADMIN`, utilizza `ADMIN`.
- Password dell'account di servizio: la password per l'account del servizio Active Directory.

5. Dopo aver inserito gli aggiornamenti, scegli Aggiorna Active Directory per apportare le modifiche.

Utilizzate la seguente procedura per aggiornare la configurazione di Active Directory di una SVM già unita a un Active Directory.

Per aggiornare una configurazione SVM Active Directory () AWS CLI

- Per aggiornare la configurazione di Active Directory di una SVM con l'API AWS CLI o, utilizzate il comando update-storage-virtual-machineCLI (o l'operazione API UpdateStorageVirtualMachineequivalente), come illustrato nell'esempio seguente.

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-abcdef0123456789a\
    --active-directory-configuration \
    SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}'
```

Gestione della configurazione SVM Active Directory tramite la CLI NetApp

È possibile utilizzare la CLI NetApp ONTAP per aggiungere e annullare l'iscrizione della SVM a un Active Directory e per modificare una configurazione SVM Active Directory esistente.

Aggiungere una SVM a un Active Directory utilizzando la CLI ONTAP

È possibile unire SVM esistenti a un'Active Directory utilizzando la CLI di ONTAP, come descritto nella procedura seguente. È possibile eseguire questa operazione anche se la SVM è già aggiunta a un Active Directory.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Crea una voce DNS per Active Directory fornendo il nome DNS completo della directory (`corp.example.com`) e almeno un indirizzo IP del server DNS.

```
::>vserver services name-service dns create -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1, dns_ip_2
```

Per verificare la connessione ai server DNS, esegui il comando seguente. Sostituisci *svm_name* con le tue informazioni.

```
FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name

                            Name Server
Vserver       Name Server     Status       Status Details
------------- --------------- ------------ --------------------------
svm_name      172.31.14.245   up           Response time (msec): 0
svm_name      172.31.25.207   up           Response time (msec): 1
2 entries were displayed.
```

3. Per aggiungere il tuo SVM ad Active Directory, esegui il seguente comando. Nota che dovrai specificare un nome `computer_name` che non esiste già in Active Directory e fornire il nome DNS della directory per cui. `-domain` Ad esempio`-OU`, inserisci le unità organizzative a cui desideri che l'SVM si unisca, oltre al nome DNS completo in formato DC.

```
::>vserver cifs create -vserver svm_name -cifs-server computer_name -
domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
```

Per verificare lo stato della connessione ad Active Directory, esegui il seguente comando:

```
::>vserver cifs check -vserver svm_name

              Vserver : svm_name
            Cifs NetBIOS Name : svm_netBIOS_name
                  Cifs Status : Running
                         Site : Default-First-Site-Name
Node Name       DC Server Name  DC Server IP    Status   Status Details
--------------- --------------  --------------- ------   --------------
```

```
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245   up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245   up       Response time (msec): 20
2 entries were displayed.
```

4. Se non riesci ad accedere alle condivisioni dopo questa iscrizione, stabilisci se l'account che stai utilizzando per accedere alla condivisione dispone delle autorizzazioni. Ad esempio, se utilizzi l'`Admin`account predefinito (un amministratore delegato) con un Active Directory AWS gestito, dovrai eseguire il seguente comando in ONTAP. `netbios_domain`Corrisponde al nome di dominio di Active Directory (in questo caso si `netbios_domain` `example` usa). `corp.example.com`

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
 svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

Modificare una configurazione di Active Directory utilizzando la CLI ONTAP

È possibile utilizzare l'ONTAP CLI per modificare una configurazione di Active Directory esistente.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Esegui il comando seguente per disattivare temporaneamente il server CIFS di SVM:

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Se devi modificare le voci DNS di Active Directory, esegui il seguente comando:

```
::>vserver services name-service dns modify -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1,dns_ip_2
```

È possibile convalidare lo stato della connessione ai server DNS di Active Directory utilizzando il comando. `vserver services name-service dns check -vserver svm_name`

```
::>vserver services name-service dns check -vserver svm_name
                              Name Server
Vserver       Name Server     Status       Status Details
------------- --------------- ------------ --------------------------
svmciad       dns_ip_1        up           Response time (msec): 1
svmciad       dns_ip_2        up           Response time (msec): 1
2 entries were displayed.
```

4. Se è necessario modificare la configurazione di Active Directory stessa, è possibile modificare i campi esistenti utilizzando il seguente comando, sostituendo:

   - *computer_name*, se si desidera modificare il nome NetBIOS (account macchina) dell'SVM.
   - *domain_name, se si desidera modificare il nome* del dominio. Dovrebbe corrispondere alla voce di dominio DNS indicata nel passaggio 3 di questa sezione (). `corp.example.com`
   - `organizational_unit`, se si desidera modificare l'unità organizzativa (`OU=Computers,OU=example,DC=corp,DC=example,DC=com`).

   Dovrai reinserire le credenziali di Active Directory utilizzate per aggiungere questo dispositivo ad Active Directory.

   ```
   ::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
   domain domain_name -OU organizational_unit
   ```

   È possibile verificare lo stato della connessione ad Active Directory utilizzando il `vserver cifs check -vserver svm_name` comando.

5. Al termine della modifica della configurazione di Active Directory e DNS, riattiva il server CIFS eseguendo il comando seguente:

   ```
   ::>vserver cifs modify -vserver svm_name -status-admin up
   ```

Annulla l'accesso a un Active Directory dal tuo SVM utilizzando la CLI NetApp di ONTAP

L' NetApp ONTAP CLI può essere utilizzata anche per annullare l'accesso alla SVM da Active Directory seguendo i passaggi seguenti:

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *management_endpoint_ip* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Eliminare il server CIFS che ha separato il dispositivo da Active Directory eseguendo il comando seguente. Affinché ONTAP elimini l'account macchina per il tuo SVM, fornisci le credenziali originariamente utilizzate per aggiungere l'SVM ad Active Directory.

   ```
   FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
   ```

3. Se devi modificare le voci DNS di Active Directory, esegui il seguente comando:

   ```
   FsxId0123456789a::vserver cifs delete -vserver svm_name

   In order to delete an Active Directory machine account for the CIFS server, you
    must supply the name and password of a Windows account with
   sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

   Enter the user name: user_name

   Enter the password:

   Warning: There are one or more shares associated with this CIFS server
            Do you really want to delete this CIFS server and all its shares? {y|n}: y
   ```

4. Eliminare i server DNS per Active Directory eseguendo il comando seguente:

   ```
   ::vserver services name-service dns delete -vserver svm_name
   ```

Se visualizzi un avviso come il seguente, che indica che `dns` deve essere rimosso in quanto tale, `ns-switch` e non intendi aggiungere nuovamente questo dispositivo a un Active Directory, puoi rimuovere le voci. `ns-switch`

```
Warning: "DNS" is present as one of the sources in one or more ns-switch databases
 but no valid DNS configuration was found for Vserver
         "svm_name". Remove "DNS" from ns-switch using the "vserver services name-
service ns-switch" command. Configuring "DNS" as a source
         in the ns-switch setting when there is no valid configuration can cause
 protocol access issues.
```

5. (Facoltativo) Rimuovi le `ns-switch` voci di `dns` eseguendo il comando seguente. Verifica l'ordine delle fonti, quindi rimuovi la `dns` voce dal `hosts` database modificandola `sources` in modo che contenga solo le altre fonti elencate. In questo esempio, l'unica altra fonte è`files`.

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts

                    Vserver: svm_name
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

6. (Facoltativo) Rimuovere la `dns` voce modificando l'opzione `sources` per includere solo `files` l'host del database.

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

Amazon FSx per NetApp prestazioni ONTAP

Di seguito è riportata una panoramica delle prestazioni del file system Amazon FSx for NetApp ONTAP, con una discussione sulle opzioni di prestazioni e throughput disponibili e utili suggerimenti sulle prestazioni.

Argomenti

Come vengono misurate le prestazioni per i file system FSx for ONTAP

Le prestazioni del file system vengono misurate in base alla latenza, al throughput e alle operazioni di I/O al secondo (IOPS).

Latenza

Amazon FSx for NetApp ONTAP offre latenze di file operation inferiori al millisecondo con storage su unità a stato solido (SSD) e decine di millisecondi di latenza per lo storage con pool di capacità. Inoltre, Amazon FSx dispone di due livelli di cache di lettura su ogni file server, unità NVMe (non volatile memory express) e in memoria, per fornire latenze ancora più basse quando si accede ai dati letti più frequentemente.

Throughput e IOPS

Ogni file system Amazon FSx offre fino a decine di GB/s di throughput e milioni di IOPS. La quantità specifica di throughput e IOPS che il carico di lavoro può generare sul file system dipende dalla capacità di throughput totale e dalla configurazione della capacità di storage del file system, oltre alla natura del carico di lavoro, inclusa la dimensione del set di lavoro attivo.

Supporto per SMB Multichannel e NFS NConnect

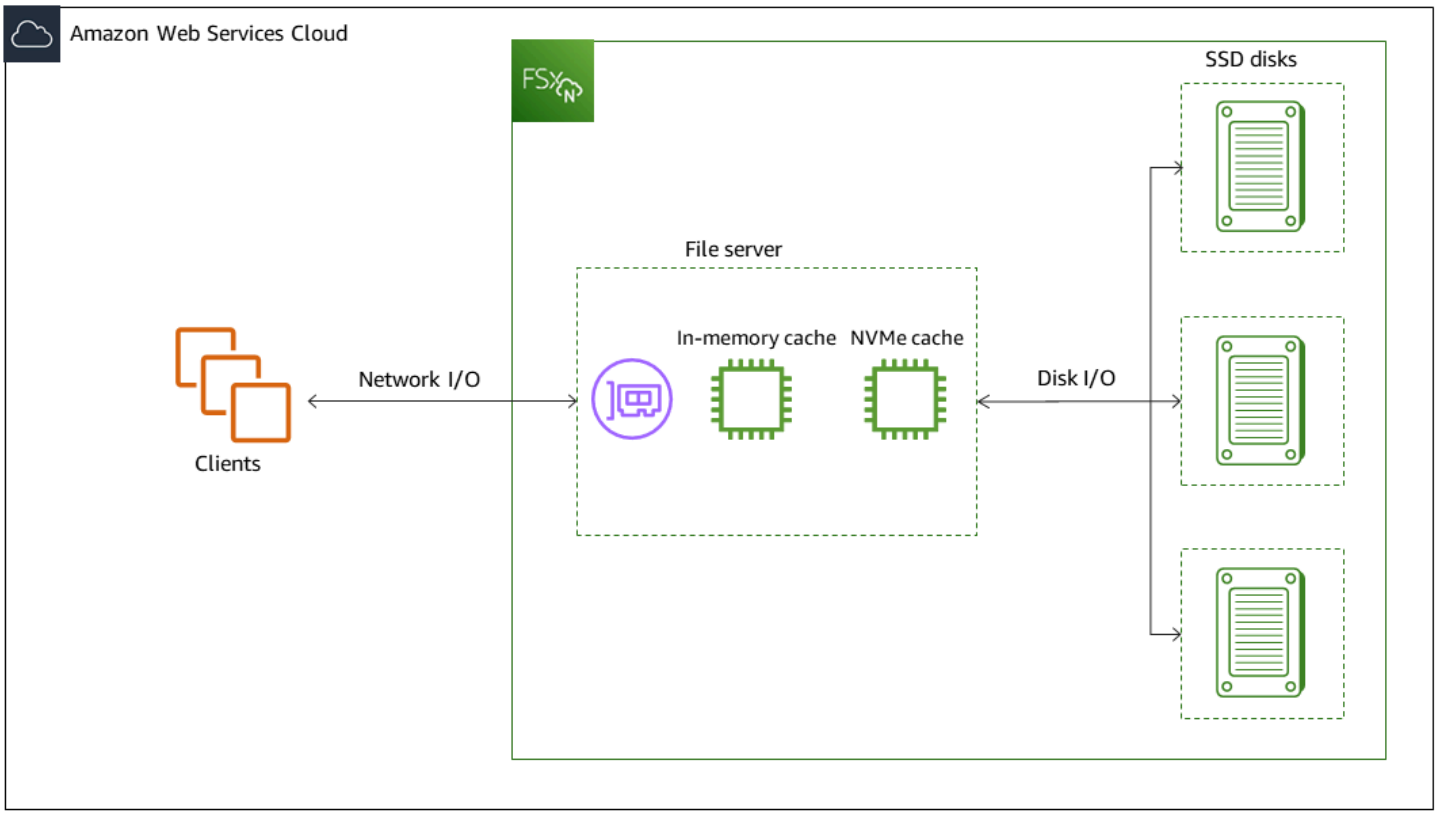
Con Amazon FSx, puoi configurare SMB Multichannel per fornire più connessioni tra ONTAP e client in un'unica sessione SMB. SMB Multichannel utilizza più connessioni di rete tra client e server contemporaneamente per aggregare la larghezza di banda della rete e massimizzarne l'utilizzo. Per informazioni sull'utilizzo della NetApp ONTAP CLI per configurare SMB Multichannel, vedere Configurazione di SMB Multichannel per prestazioni e ridondanza.

I client NFS possono utilizzare l'opzione di `nconnect` montaggio per avere più connessioni TCP (fino a 16) associate a un singolo montaggio NFS. Un client NFS di questo tipo multiplexa le operazioni sui file su più connessioni TCP in modo ininterrotto e quindi ottiene un throughput più elevato dalla larghezza di banda di rete disponibile. Supporto per `nconnect` NFSv3 e NFSv4.1+. La larghezza di banda di rete delle istanze Amazon EC2 descrive il limite di larghezza di banda full duplex di 5 Gbps per flusso di rete. Puoi superare questo limite utilizzando più flussi di rete con o multicanale SMB. `nconnect` Consultate la documentazione del vostro client NFS per confermare se `nconnect` è supportato nella vostra versione client. Per ulteriori informazioni sul NetApp ONTAP supporto per`nconnect`, consulta il ONTAPsupporto per NFSv4.1.

Dettagli sulle prestazioni

Per comprendere nel dettaglio il modello di prestazioni di Amazon FSx for NetApp ONTAP, puoi esaminare i componenti architetturali di un file system Amazon FSx. Le istanze di calcolo dei client, esistenti AWS o locali, accedono al file system tramite una o più interfacce di rete elastiche (ENI). Queste interfacce di rete risiedono nell'Amazon VPC associato al file system. Dietro ogni file system ENI c'è un NetApp ONTAP file server che fornisce dati in rete ai client che accedono al file system. Amazon FSx fornisce una cache in memoria veloce e una cache NVMe su ogni file server per migliorare le prestazioni per i dati a cui si accede più frequentemente. A ciascun file server sono collegati i dischi SSD che ospitano i dati del file system.

Questi componenti sono illustrati nel diagramma seguente.



A questi componenti architettonici (interfaccia di rete, cache in memoria, cache NVMe e volumi di storage) corrispondono le caratteristiche prestazionali principali di un file system Amazon FSx NetApp for ONTAP che determinano il throughput complessivo e le prestazioni IOPS.

- Prestazioni di I/O di rete: throughput/IOPS delle richieste tra i client e il file server (in forma aggregata)
- Dimensioni della cache in memoria e NVMe sul file server: dimensione del set di lavoro attivo che può essere utilizzato per la memorizzazione nella cache
- Prestazioni di I/O del disco: throughput/IOPS delle richieste tra il file server e i dischi di storage

Esistono due fattori che determinano queste caratteristiche prestazionali del file system: la quantità totale di IOPS SSD e la capacità di throughput configurata per tale file. Le prime due caratteristiche prestazionali, le prestazioni di I/O di rete e le dimensioni della cache in memoria e NVMe, sono determinate esclusivamente dalla capacità di throughput, mentre la terza, le prestazioni di I/O del disco, è determinata da una combinazione di capacità di throughput e IOPS SSD.

I carichi di lavoro basati su file sono in genere caratterizzati da picchi di traffico, caratterizzati da periodi brevi e intensi di I/O elevati con tempi di inattività abbondanti tra i burst. Per supportare carichi di lavoro con picchi di lavoro, oltre alle velocità di base che un file system può supportare 24 ore su

24, 7 giorni su 7, Amazon FSx offre la possibilità di raggiungere velocità più elevate per periodi di tempo sia per le operazioni di I/O di rete che di I/O su disco. Amazon FSx utilizza un meccanismo di crediti di I/O di rete per allocare throughput e IOPS in base all'utilizzo medio: i file system accumulano crediti quando il loro throughput e l'utilizzo di IOPS sono inferiori ai limiti di base e possono utilizzare questi crediti per eseguire operazioni di I/O.

Le operazioni di scrittura utilizzano il doppio della larghezza di banda di rete rispetto alle operazioni di lettura. Un'operazione di scrittura deve essere replicata sul file server secondario, quindi una singola operazione di scrittura genera il doppio della velocità di trasmissione di rete.

Impatto del tipo di implementazione sulle prestazioni

È possibile creare due tipi di file system con FSx for ONTAP. I file system con una singola coppia di file server ad alta disponibilità (HA) sono chiamati file system scalabili. I file system con più coppie HA sono chiamati file system con scalabilità orizzontale. Per ulteriori informazioni, consulta Coppie ad alta disponibilità (HA).

I file system FSx for ONTAP Multi-AZ e Single-AZ forniscono latenze operative dei file costanti inferiori al millisecondo con lo storage SSD e decine di millisecondi di latenza con storage con pool di capacità. Inoltre, i file system che soddisfano i seguenti requisiti forniscono una cache di lettura NVMe per ridurre le latenze di lettura e aumentare gli IOPS per i dati letti di frequente:

- File system Multi-AZ
- File system scalabili Single-AZ creati dopo il 28 novembre 2022 con almeno 2 GBps di capacità di throughput

Le tabelle seguenti mostrano la quantità di capacità di throughput fino a cui i file system possono scalare in base a fattori quali il numero di coppie ad alta disponibilità (HA) e la disponibilità. Regioni AWS

Scale-up

Queste specifiche prestazionali si applicano ai file system con scalabilità verticale.

Throughput massimo dello storage SSD per coppia HA per file system con scalabilità verticale

	Regione Stati Uniti orientali (Ohio), regione Stati Uniti orientali (Virginia settentrionale), regione Stati Uniti occidentali (Oregon) ed Europa (Irlanda)		Tutti gli altri Regioni AWS in cui è disponibile FSx for ONTAP	
	Velocità di lettura (MBps)	Velocità di scrittura (MBps)	Velocità di lettura (MBps)	Velocità di scrittura (MBps)
AZ singolo	4.096*	1.000	2.048	750
Multi-AZ	4.096*	1.800	2.048	1.300

> **Note**
>
> * Per fornire 4 GBps di capacità di throughput, il file system deve essere configurato con un minimo di 5.120 GiB di capacità di archiviazione SSD e 160.000 IOPS SSD.

Scale-out

Queste specifiche prestazionali si applicano ai file system con scalabilità orizzontale.

Velocità effettiva massima dello storage SSD per coppia HA per file system con scalabilità orizzontale

	Velocità di lettura (MBps)	Velocità di scrittura (MBps)
Scalabilità orizzontale Single-AZ	6.144*	1.100*

> **Note**
>
> * Per coppia HA (fino a 12). Per ulteriori informazioni, consulta Coppie ad alta disponibilità (HA).

Impatto della capacità di storage sulle prestazioni

Il throughput massimo del disco e i livelli di IOPS che il file system è in grado di raggiungere sono i seguenti:

- il livello di prestazioni del disco fornito dai file server, in base alla capacità di trasmissione selezionata per il file system
- il livello di prestazioni del disco fornito dal numero di IOPS SSD predisposti per il file system

Per impostazione predefinita, lo storage SSD del file system offre i seguenti livelli di velocità effettiva del disco e IOPS:

- Velocità effettiva del disco (MBps per TiB di storage): 768
- IOPS su disco (IOPS per TiB di storage): 3.072

Impatto della capacità di throughput sulle prestazioni

Ogni file system Amazon FSx ha una capacità di throughput che configuri al momento della creazione del file system. La capacità di throughput del file system determina il livello delle prestazioni di I/O della rete o la velocità con cui ciascuno dei file server che ospitano il file system può fornire i dati dei file attraverso la rete ai client che vi accedono. Livelli più elevati di capacità di throughput sono associati a una maggiore quantità di memoria e storage NVMe (Non-volatile Memory Express) per la memorizzazione nella cache dei dati su ciascun file server e a livelli più elevati di prestazioni di I/O su disco supportati da ciascun file server.

Facoltativamente, è possibile fornire un livello più elevato di IOPS SSD durante la creazione del file system. Il livello massimo di IOPS SSD che il file system può raggiungere dipende anche dalla capacità di throughput del file system, anche in caso di provisioning di IOPS SSD aggiuntivi.

Le tabelle seguenti mostrano il set completo di specifiche per la capacità di throughput, insieme ai livelli di base e di burst e alla quantità di memoria per la memorizzazione nella cache sul file server corrispondente. Regioni AWS

Single-AZ (scale-up)

Queste specifiche prestazionali si applicano ai file system scalabili Single-AZ creati dopo il 28 novembre 2022 nei paesi specificati. Regioni AWS

Specifiche prestazionali per i file system nei seguenti paesi Regioni AWS: Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon) ed Europa (Irlanda)

FSxcapacità di trasmissione (MBps)	Capacità di trasmissione della rete (MBps)		IOPS di rete	Caching in memoria (GB)	Caching di lettura NVMe (GB)	Velocità effettiva del disco (MBps)		IOPS dell'unità SSD *	
	Linea di base	Scoppio				Linea di base	Scoppio	Linea di base	Scoppio
128	188	1.500	Decine di migliaia di valori base	16	–	128	1.250	6.000	40.000
256	375	1.500		32	–	256	1.250	12.000	40.000
512	750	1.500	Centinaia di migliaia di valori di base	64	–	512	1.250	20.000	40.000
1,024	1.500	–		128	–	1,024	1.250	40.000	–
2.048	3.125	–		256	1.900	2.048	–	80.000	–
4,096	6.250	–		512	5.400	4,096	–	160.000	–

> **Note**
>
> * Gli IOPS SSD vengono utilizzati solo quando si accede a dati che non sono memorizzati nella cache in memoria del file server o nella cache NVMe.

Queste specifiche prestazionali si applicano ai file system scalabili Single-AZ in tutti gli altri paesi in cui è disponibile Regioni AWS FSx for ONTAP.

Specifiche prestazionali per i file system in [tutti gli altri paesi in Regioni AWS cui è disponibile FSx for ONTAP]

Capacità di trasmissione FSx (MBps)	Capacità di trasmissione della rete (MBps)		IOPS di rete	Caching in memoria (GB)	Velocità effettiva del disco (MBps)		IOPS dell'unità SSD *	
	Linea di base	Scoppio			Linea di base	Scoppio	Linea di base	Scoppio
128	150	1.250	Decine di migliaia di valori base	16	128	600	6.000	18.750
256	300	1.250		32	256	600	12.000	18.750
512	625	1.250	Centinaia di migliaia di valori di base	64	512	600	18.750	–
1,024	1.500	–		128	1,024	–	40.000	–
2.048	3.125	–		256	2.048	–	80.000	–

> **Note**
>
> * Gli IOPS SSD vengono utilizzati solo quando si accede a dati che non sono memorizzati nella cache in memoria del file server o nella cache NVMe.

Single-AZ (scale-out)

Queste specifiche prestazionali si applicano ai file system con scalabilità orizzontale.

Specifiche prestazionali per i file system con scalabilità orizzontale

Capacità di trasmissione FSx (MBps)	Capacità di trasmissione della rete (MBps)		IOPS di rete	Caching in memoria (GB)	Velocità effettiva del disco (MBps)		IOPS dell'unità SSD *	
	Linea di base	Scoppio			Linea di base	Scoppio	Linea di base	Scoppio
3.072**	6.250	–	Centinaia di migliaia di valori base	128	3.072	–	100.000	–
6.144**	12.500	–		256	6.144	–	200.000	–

> **Note**
>
> * Gli IOPS SSD vengono utilizzati solo quando si accede a dati che non sono memorizzati nella cache in memoria del file server o nella cache NVMe.
> ** Per coppia HA (fino a 12). Per ulteriori informazioni, consulta Coppie ad alta disponibilità (HA).

Multi-AZ (scale-up)

Queste specifiche prestazionali si applicano ai file system scalabili Multi-AZ creati dopo il 28 novembre 2022 nei paesi specificati. Regioni AWS

Specifiche prestazionali per i file system nei seguenti paesi Regioni AWS: Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon) ed Europa (Irlanda)

Capacità di trasmissione FSx (MBps)	Capacità di trasmissione della rete (MBps)		IOPS di rete	Caching in memoria (GB)	Memorizzazione nella cache NVMe (GB)	Velocità effettiva del disco (MBps)		IOPS dell'unità SSD *	
	Linea di base	Scoppio				Linea di base	Scoppio	Linea di base	Scoppio
128	188	1.500	Decine di migliaia di valori base	16	238	128	1.250	6.000	40.000
256	375	1.500		32	475	256	1.250	12.000	40.000
512	750	1.500	Centinaia di migliaia di valori di base	64	950	512	1.250	20.000	40.000
1,024	1.500	–		128	1.900	1,024	1.250	40.000	–
2.048	3.125	–		256	3.800	2.048	–	80.000	–
4,096	6.250	–		512	7.600	4,096	–	160.000	–

> **Note**
>
> * Gli IOPS SSD vengono utilizzati solo quando si accede a dati che non sono memorizzati nella cache in memoria del file server o nella cache NVMe.

Queste specifiche prestazionali si applicano ai file system scalabili Multi-AZ in tutti gli altri paesi in cui è disponibile Regioni AWS FSx for ONTAP.

Specifiche prestazionali per i file system in tutti gli altri paesi in Regioni AWS cui è disponibile FSx for ONTAP

Capacità di trasmissione FSx (MBps)	Capacità di trasmissione della rete (MBps)		IOPS di rete	Caching in memoria (GB)	Memorizzazione nella cache NVMe (GB)	Velocità effettiva del disco (MBps)		IOPS dell'unità SSD *	
	Linea di base	Scoppio				Linea di base	Scoppio	Linea di base	Scoppio
128	150	1.250	Decine di migliaia di valori base	16	150	128	600	6.000	18.750
256	300	1.250		32	300	256	600	12.000	18.750
512	625	1.250	Centinaia di migliaia di valori base	64	600	512	600	18.750	–
1,024	1.500	–		128	1.200	1,024	–	40.000	–
2.048	3.125	–		256	2.400	2.048	–	80.000	–

> **Note**
>
> * Gli IOPS SSD vengono utilizzati solo quando si accede a dati che non sono memorizzati nella cache in memoria del file server o nella cache NVMe.

Esempio: capacità di archiviazione e capacità di throughput

L'esempio seguente illustra in che modo la capacità di storage e la capacità di throughput influiscono sulle prestazioni del file system.

Un file system scalabile configurato con 2 TiB di capacità di storage SSD e 512 MBps di capacità di throughput presenta i seguenti livelli di throughput:

- Throughput di rete: 625 MBps di base e 1.250 MBps di burst (vedere la tabella sulla capacità di throughput)
- Velocità effettiva del disco: 512 MBps di base e 600 MBps di burst.

Il carico di lavoro che accede al file system sarà quindi in grado di aumentare il throughput di base fino a 625 MBps e a burst fino a 1.250 MBps per le operazioni sui file eseguite sui dati ad accesso attivo memorizzati nella cache in memoria del file server e nella cache NVMe.

Amministrazione delle risorse FSx for ONTAP

Utilizzando l'interfaccia a AWS Management Console riga AWS CLI di comando e l'API e ONTAP, è possibile eseguire le seguenti azioni amministrative per le risorse FSx for ONTAP:

- Creazione, elenco, aggiornamento ed eliminazione di file system, macchine virtuali di storage (SVM), volumi, backup e tag.
- Gestione dell'accesso, account e password amministrativi, requisiti di password, protocolli SMB e iSCSI, accessibilità di rete per le destinazioni di montaggio dei file system esistenti

Argomenti

Gestione dei file system FSx for ONTAP

Un file system è la risorsa Amazon FSx principale, analoga a un cluster ONTAP locale. È necessario specificare la capacità di archiviazione e la capacità di throughput dell'unità a stato solido (SSD) per il file system e scegliere un cloud privato virtuale (VPC) in cui creare il file system. Ogni file system

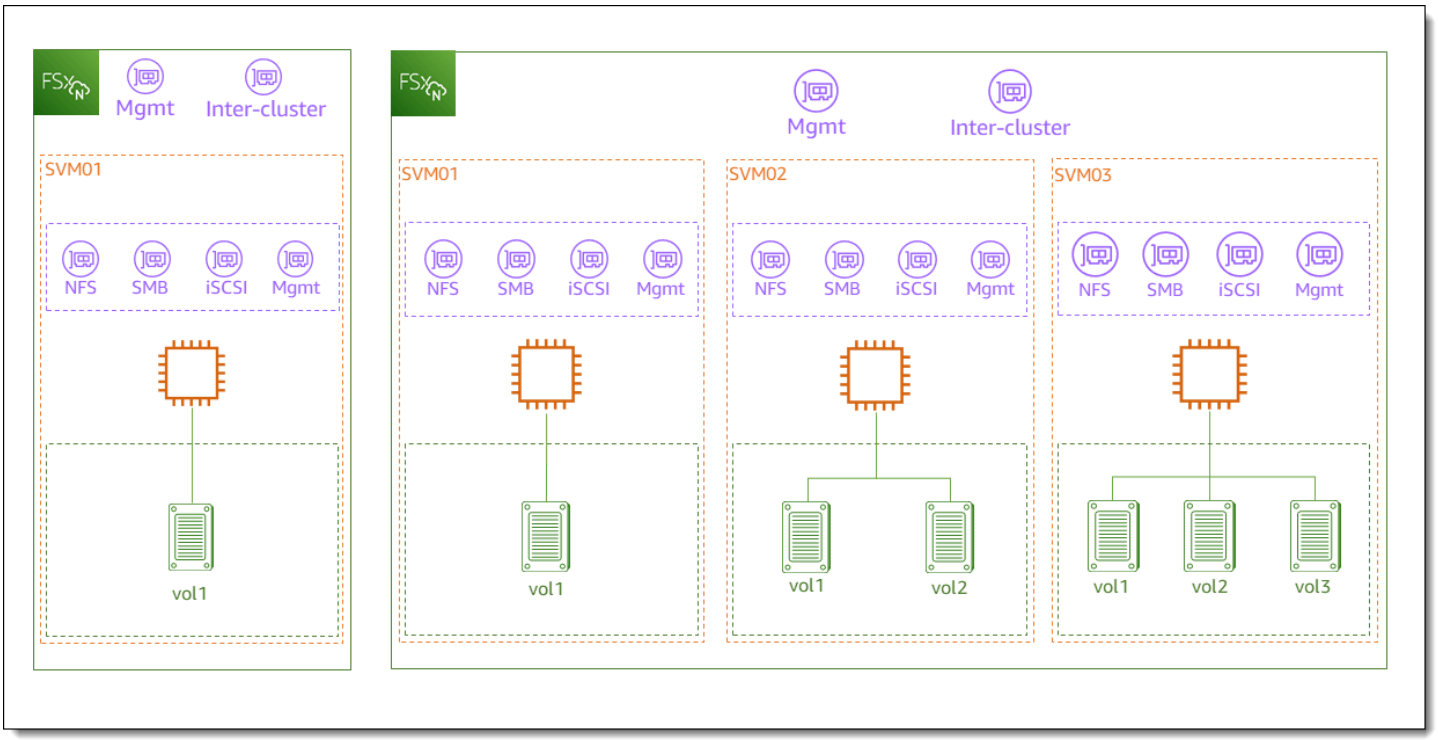
dispone di un endpoint di gestione che puoi utilizzare per gestire risorse e dati con la CLI ONTAP o l'API REST.

Risorse del file system

Un file system Amazon FSx for NetApp ONTAP è composto dalle seguenti risorse primarie:

- L'hardware fisico del file system stesso, che include i file server e i supporti di storage.
- Una o più coppie di file server ad alta disponibilità (HA), che ospitano le macchine virtuali di storage (SVM). I file system scalabili dispongono di una coppia HA e i file system con scalabilità orizzontale hanno due o più coppie HA. Ogni coppia HA ha un pool di storage chiamato aggregato. La raccolta di aggregati tra tutte le coppie HA costituisce il livello di archiviazione SSD.
- Una o più macchine virtuali di archiviazione (SVM) che ospitano i volumi del file system e dispongono di credenziali e gestione degli accessi proprie.
- Uno o più volumi che organizzano virtualmente i dati e vengono montati dai clienti.

L'immagine seguente illustra l'architettura di un file system FSx for ONTAP scalabile con una coppia HA e la relazione tra le relative risorse primarie. Il file system FSx for ONTAP sulla sinistra è il file system più semplice, con un SVM e un volume. Il file system sulla destra ha più SVM, con alcune SVM con più volumi. I file system e le SVM hanno ciascuno più endpoint di gestione e le SVM dispongono anche di endpoint di accesso ai dati.



Quando si crea un file system FSx for ONTAP, si definiscono le seguenti proprietà:

- Tipo di distribuzione: il tipo di implementazione del file system (Multi-AZ o Single-AZ). I file system Single-AZ replicano i dati e offrono il failover automatico all'interno di un'unica zona di disponibilità e offrono file system scalabili. I file system Multi-AZ offrono una maggiore resilienza replicando anche i dati e supportando il failover su più zone di disponibilità all'interno della stessa. Regione AWS
- Capacità di archiviazione: si tratta della quantità di storage SSD, fino a 192 tebibyte (TiB) per i file system scalabili verso l'alto e 1 pebibyte (PiB) per i file system con scalabilità orizzontale.
- IOPS SSD: per impostazione predefinita, ogni gigabyte di storage SSD include tre IOPS SSD (fino al massimo supportato dalla configurazione del file system). Facoltativamente, è possibile fornire ulteriori IOPS SSD in base alle esigenze.
- Capacità di trasmissione: la velocità sostenuta alla quale il file server può servire i dati.
- Rete: il VPC e le sottoreti per gli endpoint di gestione e accesso ai dati creati dal file system. Per un file system Multi-AZ, è inoltre possibile definire un intervallo di indirizzi IP e tabelle di routing.
- Crittografia: la chiave AWS Key Management Service (AWS KMS) utilizzata per crittografare i dati del file system inattivi.
- Accesso amministrativo: è possibile specificare la password per l'`fsxadmin`utente. Puoi utilizzare questo utente per amministrare il file system utilizzando la NetApp CLI ONTAP e l'API REST.

È possibile gestire i file system FSx for ONTAP utilizzando la NetApp CLI di ONTAP o l'API REST. Puoi anche configurare SnapMirror o stabilire SnapVault relazioni tra un file system Amazon FSx e un'altra implementazione ONTAP (incluso un altro file system Amazon FSx). Ogni file system FSx for ONTAP dispone dei seguenti endpoint del file system che forniscono l'accesso alle applicazioni: NetApp

- Gestione: utilizza questo endpoint per accedere alla NetApp CLI ONTAP tramite Secure Shell (SSH) o per utilizzare l'API REST NetApp ONTAP con il file system.
- Intercluster: utilizza questo endpoint per configurare la replica o la memorizzazione nella cache utilizzando. NetApp SnapMirror NetApp FlexCache

Per ulteriori informazioni, consulta Gestione delle risorse FSx for ONTAP tramite applicazioni NetApp e Replica pianificata utilizzando NetApp SnapMirror.

Coppie ad alta disponibilità (HA)

Ogni file system FSx for ONTAP è alimentato da una o più coppie di file server ad alta disponibilità (HA) in una configurazione di standby attivo. In questa configurazione, esiste un file server preferito che serve attivamente il traffico e un file server secondario che subentra se il server attivo non è disponibile. I file system scalabili FSx for ONTAP sono alimentati da una coppia HA, che offre fino a 4 GBps di capacità di throughput e 160.000 IOP SSD. I file system scalabili FSx for ONTAP sono alimentati da un massimo di 12 coppie HA, in grado di fornire fino a 72 GBps di capacità di throughput e 2.400.000 IOPS SSD (6 GBps di capacità di throughput e 200.000 IOPS SSD per coppia HA).

Quando crei il tuo file system dalla console Amazon FSx, Amazon FSx consiglia il numero di coppie HA da utilizzare in base allo storage SSD desiderato. Puoi anche scegliere manualmente il numero di coppie HA in base al carico di lavoro e ai requisiti di prestazioni. Ti consigliamo di utilizzare una singola coppia HA se i requisiti del file system sono soddisfatti da una capacità di throughput fino a 4 GBps e 160.000 IOP SSD, oltre a più coppie HA se i carichi di lavoro richiedono livelli più elevati di scalabilità delle prestazioni.

Ogni coppia HA ha un aggregato, che è un set logico di dischi fisici.

> **Note**
>
> Non è possibile aggiungere coppie HA ai file system esistenti. È invece possibile migrare i dati tra file system (con diverse coppie HA) utilizzando SnapMirror o ripristinando i dati da un backup a un nuovo file system. AWS DataSync

Creazione di FSx per i file system ONTAP

Questa sezione descrive come creare un file system FSx for ONTAP utilizzando la console Amazon FSx o AWS CLI l'API Amazon FSx. Puoi creare un file system in un cloud privato virtuale (VPC) di tua proprietà o in un VPC che un altro Account AWS ha condiviso con te. Quando si crea un file system Multi-AZ in un VPC a cui partecipi, è necessario prendere in considerazione alcune considerazioni. Queste considerazioni sono illustrate in questo argomento.

Per impostazione predefinita, quando crei un nuovo file system dalla console Amazon FSx, Amazon FSx crea automaticamente un file system con una singola macchina virtuale di storage (SVM) e un volume, che consente un accesso rapido ai dati dalle istanze Linux tramite il protocollo Network File

System (NFS). Quando si crea il file system, è possibile aggiungere facoltativamente l'SVM a un Active Directory per consentire l'accesso dai client Windows e macOS tramite il protocollo Server Message Block (SMB). Dopo aver creato il file system, è possibile creare SVM e volumi aggiuntivi in base alle esigenze.

Per creare un file system (console)

Questa procedura utilizza l'opzione di creazione Standard per creare un file system FSx for ONTAP con una configurazione personalizzata in base alle proprie esigenze. Per informazioni sull'utilizzo dell'opzione di creazione rapida per creare rapidamente un file system con un set predefinito di parametri di configurazione, vedere. Fase 1: creare un file system Amazon FSx for NetApp ONTAP

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nella dashboard, scegli Crea file system.
3. Nella pagina Seleziona il tipo di file system, per Opzioni del file system, scegli Amazon FSx for NetApp ONTAP, quindi scegli Avanti.
4. Nella sezione Metodo di creazione, scegli Creazione standard.
5. Nella sezione Dettagli del file system, fornisci le seguenti informazioni:

   - Per Nome del file system, facoltativo, immettete un nome per il file system. È più facile trovare e gestire i file system quando li si assegna un nome. È possibile utilizzare un massimo di 256 lettere Unicode, spazi bianchi e numeri, oltre ai seguenti caratteri speciali: + - =. _:/
   - Per il tipo di implementazione scegli Multi-AZ o Single-AZ.
     - I file system Multi-AZ replicano i dati e supportano il failover su più zone di disponibilità contemporaneamente. Regione AWS
     - I file system Single-AZ replicano i dati e offrono il failover automatico all'interno di un'unica zona di disponibilità.

     > **Note**
     >
     > Scegliete Single-AZ se desiderate creare un file system con due o più coppie ad alta disponibilità (HA) (fino a 12). Per ulteriori informazioni, consulta Coppie ad alta disponibilità (HA).

   Per ulteriori informazioni, consultare Disponibilità e durabilità.

- Per la capacità di archiviazione SSD, inserisci la capacità di archiviazione del tuo file system, in gibibyte (GiB). Immettere un numero intero compreso tra 1.024 e 1.048.576 GiB (fino a 1 pebibyte [PiB]).

  È possibile aumentare la capacità di archiviazione in base alle esigenze in qualsiasi momento dopo la creazione del file system. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione.

- Per Provisioned SSD IOPS, sono disponibili due opzioni per assegnare il numero di IOPS per il file system:
  - Scegli Automatico (impostazione predefinita) se desideri che Amazon FSx effettui automaticamente il provisioning di 3 IOPS per GiB di storage SSD.
  - Scegli User-provisioned se desideri specificare il numero di IOPS. È possibile effettuare il provisioning di un massimo di 200.000 IOPS SSD per file system.

  > **Note**
  >
  > È possibile aumentare gli IOPS SSD assegnati dopo aver creato il file system. Tieni presente che il livello massimo di IOPS SSD che il file system può raggiungere dipende anche dalla capacità di throughput del file system, anche in caso di provisioning di IOPS SSD aggiuntivi. Per ulteriori informazioni, consulta Impatto della capacità di throughput sulle prestazioni e Gestione della capacità di archiviazione.

- Per quanto riguarda la capacità di throughput, sono disponibili due opzioni per determinare la capacità di throughput in megabyte al secondo (MBps):
  - Scegli Capacità di throughput consigliata se desideri che Amazon FSx scelga automaticamente la capacità di throughput in base alla quantità di capacità di storage scelta.
  - Scegli Specificare la capacità di throughput se desideri specificare la quantità di capacità di throughput. Se scegli questa opzione, viene visualizzato un menu a discesa relativo alla capacità di throughput, compilato in base al tipo di distribuzione scelto. Puoi anche scegliere il numero di coppie HA (fino a 12). Per ulteriori informazioni, consulta Coppie ad alta disponibilità (HA).

  La capacità di throughput è la velocità sostenuta alla quale il file server che ospita il file system può fornire i dati. Per ulteriori informazioni, consulta Amazon FSx per NetApp prestazioni ONTAP.

6. Nella sezione Rete, fornite le seguenti informazioni:

- Per Virtual Private Cloud (VPC), scegli il VPC che desideri associare al tuo file system.
- Per i gruppi di sicurezza VPC, puoi scegliere un gruppo di sicurezza da associare all'interfaccia di rete del tuo file system. Se non ne specifichi uno, Amazon FSx assocerà il gruppo di sicurezza predefinito del VPC al tuo file system.
- Specificate una sottorete per il vostro file server. Se state creando un file system Multi-AZ, scegliete anche una sottorete Standby per il file server di standby.
- (Solo Multi-AZ) Per le tabelle di routing VPC, specifica le tabelle di routing VPC per creare gli endpoint del file system. Seleziona tutte le tabelle di routing VPC associate alle sottoreti in cui si trovano i tuoi client. Per impostazione predefinita, Amazon FSx seleziona la tabella di instradamento predefinita del tuo VPC. Per ulteriori informazioni, consulta Accesso ai dati dall'esterno del VPC di implementazione.

  > **Note**
  >
  > Amazon FSx gestisce queste tabelle di routing per file system Multi-AZ utilizzando l'autenticazione basata su tag. Queste tabelle di routing sono contrassegnate con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Quando si creano file system FSx for ONTAP Multi-AZ, si AWS CloudFormation consiglia di aggiungere il tag manualmente. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

- (Solo Multi-AZ) L'intervallo di indirizzi IP dell'endpoint specifica l'intervallo di indirizzi IP in cui vengono creati gli endpoint per accedere al file system.

  Sono disponibili tre opzioni per l'intervallo di indirizzi IP dell'endpoint:

  - Intervallo di indirizzi IP non allocati dal tuo VPC: Amazon FSx sceglie gli ultimi 64 indirizzi IP dall'intervallo CIDR primario del VPC da utilizzare come intervallo di indirizzi IP dell'endpoint per il file system. Questo intervallo è condiviso tra più file system se scegli questa opzione più volte.

    > **Note**
    >
    > Questa opzione è disattivata se uno degli ultimi 64 indirizzi IP nell'intervallo CIDR primario di un VPC è utilizzato da una sottorete. In questo caso, puoi comunque scegliere un intervallo di indirizzi in-VPC (ovvero un intervallo che non si trova alla

fine dell'intervallo CIDR primario o un intervallo che si trova in un CIDR secondario del tuo VPC) scegliendo l'opzione Inserisci un intervallo di indirizzi IP.

- Per Subnet preferita, specifica una sottorete per il tuo file server. Se state creando un file system Multi-AZ, scegliete anche una sottorete Standby per il file server di standby.
- (Solo Multi-AZ) Per le tabelle di routing VPC, specifica le tabelle di routing VPC per creare gli endpoint del file system. Seleziona tutte le tabelle di routing VPC associate alle sottoreti in cui si trovano i tuoi client. Per impostazione predefinita, Amazon FSx seleziona la tabella di instradamento predefinita del tuo VPC.
- (Solo Multi-AZ) L'intervallo di indirizzi IP dell'endpoint specifica l'intervallo di indirizzi IP in cui vengono creati gli endpoint per accedere al file system.

  Sono disponibili tre opzioni per l'intervallo di indirizzi IP dell'endpoint:

  - Intervallo di indirizzi IP non allocati dal tuo VPC: Amazon FSx sceglie gli ultimi 64 indirizzi IP dall'intervallo CIDR primario del VPC da utilizzare come intervallo di indirizzi IP dell'endpoint per il file system. Questo intervallo è condiviso tra più file system se scegli questa opzione più volte.

    > **Note**
    >
    > Questa opzione è disattivata se uno degli ultimi 64 indirizzi IP nell'intervallo CIDR primario di un VPC è utilizzato da una sottorete. In questo caso, puoi comunque scegliere un intervallo di indirizzi in-VPC (ovvero un intervallo che non si trova alla fine dell'intervallo CIDR primario o un intervallo che si trova in un CIDR secondario del tuo VPC) scegliendo l'opzione Inserisci un intervallo di indirizzi IP.

  - Intervallo di indirizzi IP fluttuante all'esterno del VPC: Amazon FSx sceglie un intervallo di indirizzi 198.19.x.0/24 che non è già utilizzato da nessun altro file system con lo stesso VPC e le stesse tabelle di routing.
  - Inserisci un intervallo di indirizzi IP: puoi fornire un intervallo CIDR a tua scelta. L'intervallo di indirizzi IP che scegli può essere interno o esterno all'intervallo di indirizzi IP del VPC, purché non si sovrapponga a nessuna sottorete.

    > **Note**
    >
    > Non scegliete alcun intervallo che rientri nei seguenti intervalli CIDR, poiché sono incompatibili con FSx for ONTAP:

- 0.0.0.0/8
- 127,0,0/8
- 19819,0,0/20
- 224,0,0/4
- 240,0,0/4
- 255,255,255,255/32

7. Nella sezione Sicurezza e crittografia, per Chiave di crittografia, scegli la chiave di crittografia AWS Key Management Service (AWS KMS) che protegge i dati del file system quando sono inattivi.
8. Per la password amministrativa del file system, inserisci una password sicura per l'`fsxadmin`utente. Conferma la password.

   È possibile utilizzare l'`fsxadmin`utente per amministrare il file system utilizzando la CLI ONTAP e l'API REST. Per ulteriori informazioni sull'`fsxadmin`utente, consulta. Gestione dei file system con la ONTAP CLI
9. Nella sezione Configurazione predefinita della macchina virtuale di archiviazione, fornisci le seguenti informazioni:

   - Nel campo Nome della macchina virtuale di archiviazione, fornire un nome per la macchina virtuale di archiviazione. È possibile utilizzare un massimo di 47 caratteri alfanumerici, più il carattere speciale di sottolineatura (_).
   - Per la password amministrativa SVM, puoi facoltativamente scegliere Specificare una password e fornire una password per l'utente dell'SVM. `vsadmin` È possibile utilizzare l'`vsadmin`utente per amministrare l'SVM utilizzando la CLI ONTAP o l'API REST. Per ulteriori informazioni sull'utente, consulta. `vsadmin` Gestione delle SVM con la CLI ONTAP

     Se scegli Non specificare una password (impostazione predefinita), puoi comunque utilizzare l'`fsxadmin`utente del file system per gestire il file system utilizzando la CLI ONTAP o l'API REST, ma non puoi usare l'utente `vsadmin` del tuo SVM per fare lo stesso.
   - Nella sezione Active Directory, puoi aggiungere un Active Directory alla SVM. Per ulteriori informazioni, consulta Utilizzo di Microsoft Active Directory in FSx for ONTAP.

     Se non vuoi aggiungere la tua SVM a un Active Directory, scegli Non partecipare a un Active Directory.

Se desideri aggiungere la tua SVM a un dominio Active Directory autogestito, scegli Iscriviti a un Active Directory e fornisci i seguenti dettagli per il tuo Active Directory:

- Il nome NetBIOS dell'oggetto computer Active Directory da creare per la SVM. Il nome NetBIOS non può superare i 15 caratteri.
- Il nome di dominio completo di Active Directory. Il nome di dominio non può superare i 255 caratteri.
- Indirizzi IP dei server DNS: gli indirizzi IPv4 dei server DNS (Domain Name System) del tuo dominio.
- Nome utente dell'account di servizio: il nome utente dell'account di servizio nell'Active Directory esistente. Non includere un prefisso o un suffisso di dominio.
- Password dell'account di servizio: la password per l'account di servizio.
- Conferma password: la password per l'account di servizio.
- (Facoltativo) Unità organizzativa (OU): il nome del percorso distinto dell'unità organizzativa a cui si desidera aggiungere il file system.
- Gruppo di amministratori di file system delegati: nome del gruppo in Active Directory che può amministrare il file system.

  Se si utilizza AWS Managed Microsoft AD, è necessario specificare un gruppo come AWS Delegated FSx Administrators AWS , Delegated Administrators o un gruppo personalizzato con autorizzazioni delegate all'unità organizzativa.

  Se ti unisci a un AD autogestito, usa il nome del gruppo nel tuo AD. Il gruppo predefinito è`Domain Admins`.

10. Nella sezione Configurazione del volume predefinito, fornite le seguenti informazioni per il volume predefinito creato con il file system:

    - Nel campo Nome del volume, fornisci un nome per il volume. È possibile utilizzare fino a 203 caratteri alfanumerici o di sottolineatura (_).
    - (Solo file system con scalabilità verticale) Per lo stile Volume, scegliete o. FlexVolFlexGroup FlexVoli volumi sono volumi generici che possono avere dimensioni fino a 300 TiB. FlexGroupi volumi sono destinati a carichi di lavoro ad alte prestazioni e possono avere dimensioni fino a 20 PiB.
    - Per Dimensione del volume, immettere un numero intero compreso tra 800 gibibyte (GiB) e 2.000 pebibyte (PiB).

- Per Tipo di volume, scegliete Read-Write (RW) per creare un volume leggibile e scrivibile o Data Protection (DP) per creare un volume di sola lettura che può essere utilizzato come destinazione di una relazione or. NetApp SnapMirror SnapVault Per ulteriori informazioni, consulta Tipi di volume.
- Per Junction path, inserite una posizione all'interno del file system in cui montare il volume. Il nome deve avere una barra iniziale, ad esempio`/vol3`.
- Per l'efficienza dello storage, scegli Enabled per abilitare le funzionalità di efficienza dello storage ONTAP (deduplicazione, compressione e compattazione). Per ulteriori informazioni, consulta FSx per l'efficienza dello storage ONTAP.
- Per lo stile di sicurezza Volume, scegli tra Unix (Linux), NTFS e Mixed per il volume. Per ulteriori informazioni, consulta Stile di sicurezza del volume.
- Per la policy Snapshot, scegli una policy di snapshot per il volume. Per ulteriori informazioni sulle politiche relative alle snapshot, vedere. Politiche relative alle istantanee

  Se si sceglie Politica personalizzata, è necessario specificare il nome della politica nel campo Custom-Policy. La politica personalizzata deve già esistere sulla SVM o nel file system. Puoi creare una policy di snapshot personalizzata con la CLI ONTAP o l'API REST. Per ulteriori informazioni, consulta Creare una policy per le istantanee nella documentazione del NetApp prodotto ONTAP.

11. Nella sezione Default Volume Storage Tiering, per la policy di storage pool di capacità su più livelli, scegli la politica di storage pool di storage tiering per il volume, che può essere Auto (impostazione predefinita), Solo snapshot, Tutti o Nessuno. Per ulteriori informazioni sulle politiche di suddivisione in più livelli del pool di capacità, vedere. Politiche di suddivisione in livelli di volume

    Per il periodo di raffreddamento delle politiche di tiering, se è stato impostato lo storage su più livelli su entrambi `Auto` e `Snapshot-only` policies.valid, i valori sono 2-183 giorni. Il periodo di raffreddamento della policy di tiering di un volume definisce il numero di giorni prima che i dati a cui non è stato effettuato l'accesso vengano contrassegnati come freddi e trasferiti nello storage con pool di capacità.

12. In Backup e manutenzione, opzionale, puoi impostare le seguenti opzioni:

    - Per Backup automatico giornaliero, scegli Abilitato per i backup giornalieri automatici. Per impostazione predefinita, questa opzione è abilitata.
    - Per Finestra di backup automatico giornaliero, imposta l'ora del giorno in UTC (Coordinated Universal Time) in cui desideri avviare la finestra di backup automatico giornaliero. La finestra

è di 30 minuti a partire dall'ora specificata. Questa finestra non può sovrapporsi alla finestra di backup settimanale per la manutenzione.

- Per Periodo di conservazione automatico dei backup, imposta un periodo compreso tra 1 e 90 giorni in cui desideri conservare i backup automatici.
- Per Finestra di manutenzione settimanale, puoi impostare l'ora della settimana in cui desideri che inizi la finestra di manutenzione. Il giorno 1 è lunedì, il 2 è martedì e così via. La finestra è di 30 minuti a partire dall'ora specificata. Questa finestra non può sovrapporsi alla finestra di backup automatico giornaliero.

13. Per i tag: facoltativo, puoi inserire una chiave e un valore per aggiungere tag al tuo file system. Un tag è una coppia chiave-valore con distinzione tra maiuscole e minuscole che consente di gestire, filtrare e cercare il file system.

    Seleziona Successivo.

14. Rivedi la configurazione del file system riportata nella pagina Crea file system. Come riferimento, prendete nota delle impostazioni del file system che potete modificare dopo la creazione del file system.
15. Scegliere Create file system (Crea file system).

Per creare un file system (CLI)

- Per creare un file system FSx for ONTAP, utilizzate il comando CLI create-file-system (o l'operazione API di CreateFilesistema equivalente), come illustrato nell'esempio seguente.

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \

    --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
    --ontap-configuration DeploymentType=MULTI_AZ_1,
        ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

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

```
{
```

```
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
                "Mode": "AUTOMATIC",
                "Iops": 3072
      },
      "PreferredSubnetId": "subnet-abcdef1234567890b",
      "RouteTableIds": [
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
      ],
      "ThroughputCapacity": 512,
      "WeeklyMaintenanceStartTime": "4:10:00"
    }
  }
}
```

> **Note**
>
> A differenza del processo di creazione di un file system nella console, il comando `create-file-system` CLI e l'operazione `CreateFileSystem` API non creano una SVM o un volume predefiniti. Per creare un SVM, vediCreazione di una macchina virtuale di archiviazione; per creare un volume, vedi. Creazione di volumi

Creazione di file system FSx per ONTAP in sottoreti condivise

La condivisione di VPC consente di Account AWS creare più risorse in cloud privati virtuali (VPC) condivisi e gestiti centralmente. In questo modello, l'account proprietario del VPC (proprietario) condivide una o più sottoreti con altri account (partecipanti) che appartengono alla stessa organizzazione di. AWS Organizations

Gli account dei partecipanti possono creare file system FSx per ONTAP Single-AZ e Multi-AZ in una sottorete VPC che l'account del proprietario ha condiviso con loro. Affinché un account partecipante possa creare un file system Multi-AZ, l'account proprietario deve inoltre concedere ad Amazon FSx l'autorizzazione a modificare le tabelle di routing nelle sottoreti condivise per conto dell'account del partecipante. Per ulteriori informazioni, consulta Gestione del supporto VPC condiviso per file system Multi-AZ.

> **Note**
>
> È responsabilità dell'account partecipante coordinarsi con il proprietario del VPC per impedire la creazione di eventuali sottoreti VPC successive che si sovrappongano al CIDR in-VPC dei file system del partecipante. Se le sottoreti si sovrappongono, il traffico verso il file system può essere interrotto.

Considerazioni e requisiti relativi alle sottoreti condivisi

Quando create i file system FSx for ONTAP in sottoreti condivise, tenete presente quanto segue:

- Il proprietario della sottorete VPC deve condividere una sottorete con un account partecipante prima che tale account possa creare un file system FSx for ONTAP al suo interno.

- Non è possibile avviare le risorse utilizzando il gruppo di sicurezza predefinito per il VPC, in quanto questo appartiene al proprietario. Inoltre, gli account dei partecipanti non possono avviare risorse utilizzando gruppi di sicurezza di proprietà di altri partecipanti o del proprietario.
- In una sottorete condivisa, il partecipante e il proprietario controllano separatamente i gruppi di sicurezza all'interno di ciascun account. L'account proprietario può vedere i gruppi di sicurezza creati dai partecipanti, ma non può eseguire alcuna azione su di essi. Se l'account proprietario desidera rimuovere o modificare questi gruppi di sicurezza, il partecipante che ha creato il gruppo di sicurezza deve intraprendere l'azione.
- Gli account dei partecipanti possono visualizzare, creare, modificare ed eliminare i file system Single-AZ e le risorse associate nelle sottoreti che l'account proprietario ha condiviso con loro.
- Gli account dei partecipanti possono creare, visualizzare, modificare ed eliminare i file system Multi-AZ e le risorse associate nelle sottoreti che l'account proprietario ha condiviso con loro. Inoltre, l'account proprietario deve concedere al servizio Amazon FSx le autorizzazioni per modificare le tabelle di routing nelle sottoreti condivise per conto dell'account del partecipante. Per ulteriori informazioni, consulta Gestione del supporto VPC condiviso per file system Multi-AZ
- Il proprietario del VPC condiviso non può visualizzare, modificare o eliminare le risorse create da un partecipante nella sottorete condivisa. Ciò si aggiunge alle risorse VPC alle quali ogni account ha un accesso diverso. Per ulteriori informazioni, consulta Responsabilità e autorizzazioni per proprietari e partecipanti nella Amazon VPC User Guide.

Per ulteriori informazioni, consulta Condividi il tuo VPC con altri account nella Amazon VPC User Guide.

Quando si condivide una sottorete VPC

Quando condividete le sottoreti con gli account dei partecipanti che creeranno i file system FSx for ONTAP nelle sottoreti condivise, dovrete fare quanto segue:

- Il proprietario del VPC deve utilizzarlo per AWS Resource Access Manager condividere in modo sicuro VPC e sottoreti con altri. Account AWS Per ulteriori informazioni, consulta Condivisione delle AWS risorse nella Guida per l'utente. AWS Resource Access Manager
- Il proprietario del VPC deve condividere uno o più VPC con un account partecipante. Per ulteriori informazioni, consulta Condividi il tuo VPC con altri account nella Amazon Virtual Private Cloud User Guide.
- Affinché gli account dei partecipanti possano creare file system FSx for ONTAP Multi-AZ, il proprietario del VPC deve inoltre concedere al servizio Amazon FSx le autorizzazioni per creare

e modificare tabelle di routing nelle sottoreti condivise per conto degli account dei partecipanti. Questo perché i file system FSx for ONTAP Multi-AZ utilizzano indirizzi IP mobili in modo che i client connessi possano passare senza problemi dai file server preferiti a quelli di standby durante un evento di failover. Quando si verifica un evento di failover, Amazon FSx aggiorna tutte le route in tutte le tabelle di route associate al file system in modo che puntino al file server attualmente attivo.

Gestione del supporto VPC condiviso per file system Multi-AZ

Gli account proprietari possono decidere se gli account dei partecipanti possono creare file system Multi-AZ FSx for ONTAP nelle sottoreti VPC che il proprietario ha condiviso con i partecipanti utilizzando l'API, e AWS Management Console AWS CLI, come descritto nelle sezioni seguenti.

Per gestire la condivisione VPC per file system Multi-AZ (console)

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

1. Nel pannello di navigazione scegli Impostazioni.
2. Individua le impostazioni del VPC condiviso Multi-AZ nella pagina Impostazioni.
   - Per abilitare la condivisione VPC per i file system Multi-AZ nelle sottoreti VPC che condividi, scegli Abilita gli aggiornamenti delle tabelle di routing dagli account dei partecipanti.
   - Per disabilitare la condivisione VPC per i file system Multi-AZ in tutti i VPC di tua proprietà, scegli Disabilita gli aggiornamenti delle tabelle di routing dagli account dei partecipanti. Viene visualizzata la schermata di conferma.

   > **Important**
   >
   > Consigliamo vivamente di eliminare i file system Multi-AZ creati dai partecipanti nel VPC condiviso prima di disabilitare questa funzionalità. Una volta disattivata la funzionalità, questi file system entreranno in uno `MISCONFIGURED` stato e rischieranno di non essere più disponibili.

3. Entra **`confirm`** e scegli Conferma per disabilitare la funzionalità.

Per gestire la condivisione VPC per i file system Multi-AZ ()AWS CLI

1. Per visualizzare l'impostazione corrente per la condivisione VPC Multi-AZ, usa il comando CLI describe-shared-vpc-configuration o il comando API equivalente, mostrato di seguito: DescribeSharedVpcConfiguration

   ```
   $ aws fsx describe-shared-vpc-configuration
   ```

   Il servizio risponde a una richiesta riuscita come segue:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
   }
   ```

2. Per gestire la configurazione VPC condivisa Multi-AZ, usa il comando CLI update-shared-vpc-configuration o il comando API equivalente. UpdateSharedVpcConfiguration L'esempio seguente abilita la condivisione VPC per file system Multi-AZ.

   ```
   $ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts true
   ```

   Il servizio risponde a una richiesta riuscita nel modo seguente:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
   }
   ```

3. Per disabilitare la funzionalità, `EnableFsxRouteTableUpdatesFromParticipantAccounts` impostate su`false`, come illustrato nell'esempio seguente.

   ```
   $ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-participant-accounts false
   ```

   Il servizio risponde a una richiesta riuscita nel modo seguente:

   ```
   {
       "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
   }
   ```

Aggiornamento di un file system

Questo argomento spiega quali proprietà di un file system esistente è possibile aggiornare e fornisce le procedure per farlo utilizzando la console e la CLI.

Puoi aggiornare le seguenti proprietà del file system FSx for ONTAP utilizzando la console Amazon FSx, e AWS CLI l'API Amazon FSx:

- Backup giornalieri automatici. Attiva o disattiva i backup giornalieri automatici, modifica la finestra di backup e il periodo di conservazione dei backup. Per ulteriori informazioni sui backup, consultare Lavorare con backup giornalieri automatici.
- Finestra di manutenzione settimanale. Imposta il giorno della settimana e l'ora in cui Amazon FSx esegue la manutenzione e gli aggiornamenti del file system. Per ulteriori informazioni sulla finestra di manutenzione, consultaOttimizzazione delle prestazioni con le finestre di manutenzione di Amazon FSx.
- Password amministrativa del file system. Modifica la password per l'`fsxadmin`utente del file system. È possibile utilizzare l'`fsxadmin`utente per amministrare il file system utilizzando la CLI ONTAP e l'API REST. Per ulteriori informazioni sull'`fsxadmin`utente, consulta. Gestione dei file system con la ONTAP CLI
- Tabelle di routing Amazon VPC. Con i file system Multi-AZ FSx for ONTAP, gli endpoint utilizzati per accedere ai dati tramite NFS o SMB e gli endpoint di gestione per accedere a CLI, API e BlueXP di ONTAP utilizzano indirizzi IP mobili nelle tabelle di routing Amazon VPC che associ al tuo file system. È possibile associare nuove tabelle di routing create ai file system Multi-AZ esistenti, in modo da configurare quali client possono accedere ai dati anche se la rete si evolve. È inoltre possibile dissociare (rimuovere) le tabelle di routing esistenti dal file system.

> **Note**
>
> Amazon FSx gestisce le tabelle di routing VPC per file system Multi-AZ utilizzando l'autenticazione basata su tag. Queste tabelle di routing sono contrassegnate con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Quando si creano o si aggiornano file system FSx for ONTAP Multi-AZ, si AWS CloudFormation consiglia di aggiungere il tag manualmente. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Per aggiornare un file system (console)

Le seguenti procedure forniscono istruzioni su come effettuare aggiornamenti a un file system FSx for ONTAP esistente utilizzando il. AWS Management Console

Per aggiornare i backup giornalieri automatici

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Per visualizzare la pagina dei dettagli del file system, nel riquadro di navigazione a sinistra, scegliete File system, quindi scegliete il file system FSx for ONTAP che desiderate aggiornare.
3. Scegliete la scheda Backup nel secondo pannello della pagina.
4. Scegli Aggiorna.
5. Modifica le impostazioni di backup giornaliero automatico per questo file system.
6. Scegliere Salva per salvare le modifiche.

Per aggiornare la finestra di manutenzione settimanale

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Per visualizzare la pagina dei dettagli del file system, nel riquadro di navigazione a sinistra, scegliete File system, quindi scegliete il file system FSx for ONTAP che desiderate aggiornare.
3. Scegliete la scheda Amministrazione nel secondo pannello della pagina.
4. Nel riquadro Manutenzione, scegli Aggiorna.
5. Modifica quando si verifica la finestra di manutenzione settimanale per questo file system.
6. Scegliere Salva per salvare le modifiche.

Per modificare la password amministrativa del file system

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Per visualizzare la pagina dei dettagli del file system, nel riquadro di navigazione a sinistra, scegliete File system, quindi scegliete il file system FSx for ONTAP che desiderate aggiornare.
3. Scegliete la scheda Amministrazione.
4. Nel riquadro di amministrazione ONTAP, scegli Aggiorna sotto la password dell'amministratore ONTAP.
5. Nella finestra di dialogo Aggiorna le credenziali dell'amministratore ONTAP, inserisci una nuova password nel campo della password amministrativa ONTAP.

6. Utilizza il campo Conferma password per confermare la password.
7. Scegli Aggiorna credenziali per salvare le modifiche.

> **Note**
>
> Se viene visualizzato un errore che indica che la nuova password non soddisfa i requisiti di password, è possibile utilizzare il comando `security login role config show`ONTAPCLI per visualizzare le impostazioni dei requisiti relativi alla password nel file system. Per ulteriori informazioni, incluse le istruzioni su come modificare l'impostazione della password, vedere. L'aggiornamento della password `fsxadmin` dell'account non riesce

Per aggiornare le tabelle di routing VPC sui file system Multi-AZ

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Per visualizzare la pagina dei dettagli del file system, nel riquadro di navigazione a sinistra, scegliete File system, quindi scegliete il file system FSx for ONTAP che desiderate aggiornare.
3. Per Azioni, scegliete Gestisci le tabelle dei percorsi. Questa opzione è disponibile solo per i file system Multi-AZ.
4. Nella finestra di dialogo Gestisci le tabelle degli itinerari, effettuate una delle seguenti operazioni:
   - Per associare una nuova tabella di routing VPC, seleziona una tabella di routing dall'elenco a discesa Associa nuove tabelle di routing, quindi scegli Associa.
   - Per dissociare una tabella di routing VPC esistente, seleziona una tabella di routing dal riquadro Tabelle di routing correnti, quindi scegli Dissocia.
5. Scegli Chiudi.

Per aggiornare un file system (CLI)

La procedura seguente illustra come effettuare aggiornamenti a un file system FSx for ONTAP esistente utilizzando. AWS CLI

1. Per aggiornare la configurazione di un file system FSx for ONTAP, utilizzate il comando CLI update-file-system (o l'operazione API di UpdateFilesistema equivalente), come illustrato nell'esempio seguente.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
      FsxAdminPassword=new-fsx-admin-password
```

2. Per disabilitare i backup giornalieri automatici, impostate la proprietà su 0. `AutomaticBackupRetentionDays`

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

Cancellazione di un file system

Puoi eliminare un file system FSx for ONTAP utilizzando la console Amazon FSx, l'API e AWS CLI gli SDK di Amazon FSx.

Per eliminare un file system:

- Utilizzo della console: seguire la procedura descritta inFase 3: Eliminazione delle risorse.
- Utilizzo della CLI o dell'API: per prima cosa elimina tutti i volumi e le SVM sul file system. Quindi utilizza il comando CLI delete-file-system o l'operazione System API. DeleteFile

Visualizzazione dei dettagli del file system

Puoi visualizzare informazioni di configurazione dettagliate per il tuo file system FSx for ONTAP utilizzando la console Amazon FSx AWS CLI, l'API e gli SDK supportati. AWS

Per visualizzare informazioni dettagliate sul file system:

- Utilizzo della console: scegli un file system per visualizzare la pagina dei dettagli dei file system. Il pannello Riepilogo mostra l'ID del file system, lo stato del ciclo di vita, il tipo di implementazione, la capacità di archiviazione SSD, la capacità di throughput, gli IOPS assegnati, le zone di disponibilità e l'ora di creazione.

Le seguenti schede forniscono informazioni dettagliate sulla configurazione e sulla modifica delle proprietà che possono essere modificate:

- Rete e sicurezza
- Monitoraggio e prestazioni: visualizza gli CloudWatch allarmi che hai creato e le metriche e gli avvisi per le seguenti categorie:
  - Riepilogo: riepilogo di alto livello delle metriche di attività del file system
  - Capacità di archiviazione del file system
  - Prestazioni del file server e del disco

  Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.
- Amministrazione: visualizza le seguenti informazioni di amministrazione del file system:
  - I DNS nomi e IP gli indirizzi degli endpoint di gestione del file system e intercluster.
  - Il ONTAP nome utente dell'amministratore.
  - L'opzione per aggiornare la password ONTAP dell'amministratore.
- Elenco delle SVM del file system
- Elenco dei volumi del file system
- Impostazioni di backup: modifica l'impostazione di backup giornaliero automatico del file system.
- Aggiornamenti: mostra lo stato degli aggiornamenti avviati dall'utente e apportati alla configurazione del file system.
- Tag: visualizza, modifica, aggiungi e rimuovi coppie di tag Key:Value.

- Utilizzo della CLI o dell'API: utilizza il comando CLI describe-file-systems o l'operazione Systems API. DescribeFile

Stato del file system FSx for ONTAP

Puoi visualizzare lo stato di un file system Amazon FSx utilizzando la console Amazon FSx, il AWS CLI comando describe-file-systems o i sistemi operativi API. DescribeFile

Stato del file system	Descrizione
DISPONIBILE	Il file system è stato creato correttamente ed è disponibile per l'uso.

Stato del file system	Descrizione
CREAZIONE IN CORSO	Amazon FSx sta creando un nuovo file system.
ELIMINAZIONE IN CORSO	Amazon FSx sta eliminando un file system esistente.
CONFIGURATO MALE	Il file system è in uno stato configurato in modo errato ma ripristinabile.
Non riuscito	1. Il file system è guasto e Amazon FSx non è in grado di ripristinarlo. 2. Durante la creazione di un nuovo file system, Amazon FSx non è stato in grado di creare un nuovo file system.

Gestione delle macchine virtuali di storage FSx for ONTAP

In FSx for ONTAP, i volumi sono ospitati su file server virtuali denominati Storage Virtual Machine (SVM). Un SVM è un file server isolato con le proprie credenziali amministrative ed endpoint per l'amministrazione e l'accesso ai dati. Quando si accede ai dati in FSx for ONTAP, i client e le workstation montano un volume, una condivisione SMB o un LUN iSCSI ospitato da una SVM utilizzando l'endpoint (indirizzo IP) dell'SVM.

Amazon FSx crea automaticamente una SVM predefinita sul tuo file system quando crei un file system utilizzando. AWS Management Console Puoi creare SVM aggiuntive sul tuo file system in qualsiasi momento utilizzando la console o l'API e gli AWS CLI SDK di Amazon FSx. Non è possibile creare SVM utilizzando la CLI ONTAP o l'API REST.

Puoi unire le tue SVM a Microsoft Active Directory per l'autenticazione e l'autorizzazione dell'accesso ai file. Per ulteriori informazioni, consulta Utilizzo di Microsoft Active Directory in FSx for ONTAP.

Numero massimo di SVM per file system

La tabella seguente elenca il numero massimo di SVM che è possibile creare per un file system. Il numero massimo di SVM dipende dalla quantità di capacità di throughput fornita in megabyte al secondo (MBps).

Il tipo di distribuzione	Quantità di capacità di trasmissione (MBps)	Numero massimo di SVM per file system
Single-AZ (scale-up) e Multi-AZ (scale-up)	128	6
	256	6
	512	14
	1,024	14
	2.048	24
	4,096	24
Single-AZ (scalabilità orizzontale)	Qualsiasi	5

Argomenti

Creazione di una macchina virtuale di archiviazione

È possibile creare un SVM FSx for ONTAP utilizzando l'API AWS Management Console, AWS CLI e.

Il numero massimo di SVM che è possibile creare per un file system dipende dal tipo di implementazione del file system e dalla quantità di capacità di throughput fornita. Per ulteriori informazioni, consulta Numero massimo di SVM per file system.

Proprietà SVM

Quando si crea un SVM, si definiscono le seguenti proprietà:

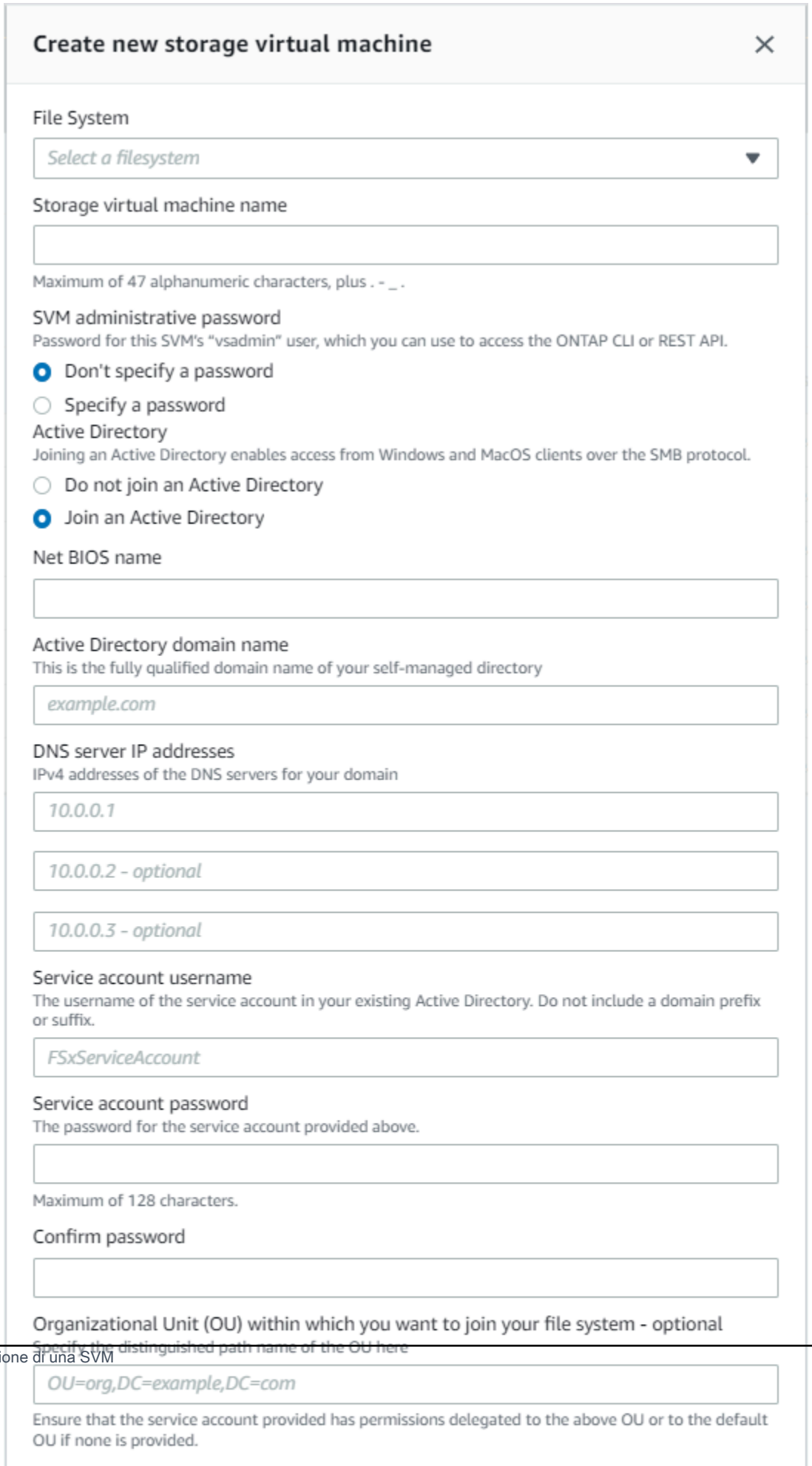
- Il file system FSx for ONTAP a cui appartiene.

- La configurazione di Microsoft Active Directory (AD): puoi facoltativamente aggiungere il tuo SVM a un AD autogestito per l'autenticazione e il controllo degli accessi dei client Windows e macOS. Per ulteriori informazioni, consulta Utilizzo di Microsoft Active Directory in FSx for ONTAP.
- Lo stile di sicurezza del volume root: imposta lo stile di sicurezza del volume root (Unix, NTFS o Mixed) per allinearlo al tipo di client che stai utilizzando per accedere ai tuoi dati all'interno dell'SVM. Per ulteriori informazioni, consulta Stile di sicurezza del volume.
- La password amministrativa SVM: puoi facoltativamente impostare la password per l'utente dell'SVM. `vsadmin` Per ulteriori informazioni, consulta Gestione delle SVM con la CLI ONTAP.

Per creare una macchina virtuale di archiviazione (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli Storage virtual machines.
3. Scegli Crea nuova macchina virtuale di archiviazione.

   Viene visualizzata la finestra di dialogo Crea nuova macchina virtuale di archiviazione.


Create new storage virtual machine
File System
Select a filesystem
Storage virtual machine name
Maximum of 47 alphanumeric characters, plus . - _ .
SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.
Don't specify a password
Specify a password
Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.
Do not join an Active Directory
Join an Active Directory
Net BIOS name
Active Directory domain name
This is the fully qualified domain name of your self-managed directory
example.com
DNS server IP addresses
IPv4 addresses of the DNS servers for your domain
10.0.0.1
10.0.0.2 - optional
10.0.0.3 - optional
Service account username
The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
FSxServiceAccount
Service account password
The password for the service account provided above.
Maximum of 128 characters.
Confirm password
Organizational Unit (OU) within which you want to join your file system - optional
Specify the distinguished path name of the OU here
OU=org,DC=example,DC=com
Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

4. Per File system, scegli il file system su cui creare la macchina virtuale di archiviazione.
5. Nel campo Nome macchina virtuale di archiviazione, fornisci un nome per la macchina virtuale di archiviazione. È possibile utilizzare un massimo di 47 caratteri alfanumerici, più il carattere speciale di sottolineatura (_).
6. Per la password amministrativa SVM, puoi facoltativamente scegliere Specificare una password e fornire una password per l'utente di questo SVM. `vsadmin` È possibile utilizzare l'`vsadmin`utente per amministrare l'SVM utilizzando la CLI ONTAP o l'API REST. Per ulteriori informazioni sull'utente, consulta. `vsadmin` Gestione delle SVM con la CLI ONTAP

   Se scegli Non specificare una password (impostazione predefinita), puoi comunque utilizzare l'`fsxadmin`utente del file system per gestire il file system utilizzando la CLI ONTAP o l'API REST, ma non puoi usare l'utente `vsadmin` del tuo SVM per fare lo stesso.
7. Per Active Directory, sono disponibili le seguenti opzioni:

   - Se non state unendo il vostro file system a un Active Directory (AD), scegliete Non iscrivervi ad Active Directory.
   - Se stai aggiungendo il tuo SVM a un dominio AD autogestito, scegli Iscriviti a un Active Directory e fornisci i seguenti dettagli per il tuo AD. Per ulteriori informazioni, consulta Prerequisiti per aggiungere una SVM a un Microsoft AD autogestito.
     - Il nome NetBIOS dell'oggetto computer Active Directory da creare per la SVM. Il nome NetBIOS non può superare i 15 caratteri. Questo è il nome di questa SVM in Active Directory.
     - Il nome di dominio completo (FQDN) del tuo Active Directory. Il nome di dominio completo non può superare i 255 caratteri.
     - Indirizzi IP dei server DNS: gli indirizzi IPv4 dei server DNS del dominio.
     - Nome utente dell'account di servizio: il nome utente dell'account di servizio nell'Active Directory esistente. Non includere un prefisso o un suffisso di dominio. Per `EXAMPLE\ADMIN`, utilizza `ADMIN`.
     - Password dell'account di servizio: la password per l'account di servizio.
     - Conferma password: la password per l'account di servizio.
     - (Facoltativo) Unità organizzativa (OU): il nome del percorso distinto dell'unità organizzativa a cui si desidera aggiungere il file system.
     - Gruppo di amministratori di file system delegati: il nome del gruppo dell'AD che può amministrare il file system.

Se si utilizza AWS Managed Microsoft AD, è necessario specificare un gruppo come AWS Delegated FSx Administrators AWS , Delegated Administrators o un gruppo personalizzato con autorizzazioni delegate all'unità organizzativa.

Se ti unisci a un AD autogestito, usa il nome del gruppo nel tuo AD. Il gruppo predefinito è`Domain Admins`.

8. Per lo stile di sicurezza del volume root SVM, scegliete lo stile di sicurezza per l'SVM in base al tipo di client che accedono ai dati. Scegliete Unix (Linux) se accedete ai dati principalmente tramite client Linux; scegliete NTFS se accedete principalmente ai dati tramite client Windows. Per ulteriori informazioni, consulta Stile di sicurezza del volume.
9. Scegli Conferma per creare la macchina virtuale di archiviazione.

È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system, nella colonna Stato del riquadro Storage virtual machines. La macchina virtuale di archiviazione è pronta per l'uso quando il suo stato è Creato.

Per creare una macchina virtuale di archiviazione (CLI)

- Per creare una macchina virtuale di archiviazione (SVM) FSx for ONTAP, utilizzate il comando create-storage-virtual-machineCLI (o l'operazione CreateStorageVirtualMachineAPI equivalente), come illustrato nell'esempio seguente.

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name svm1 \
    --svm-admin-password password \
    --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

Dopo aver creato correttamente la macchina virtuale di storage, Amazon FSx ne restituisce la descrizione in formato JSON, come illustrato nell'esempio seguente.

```
{
```

```
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
```

```
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Aggiornamento di una macchina virtuale di storage

Puoi aggiornare le seguenti proprietà di configurazione della macchina virtuale di storage (SVM) utilizzando la console AWS CLI Amazon FSx e l'API Amazon FSx:

- Password dell'account amministrativo SVM.
- Configurazione SVM Active Directory (AD): è possibile aggiungere una SVM a un AD o modificare la configurazione AD di una SVM già aggiunta a un AD. Per ulteriori informazioni, consulta Gestione delle configurazioni SVM Active Directory.

Per aggiornare le credenziali dell'account amministratore SVM (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli la SVM da aggiornare come segue:
   - Nel riquadro di navigazione a sinistra, scegliete File system, quindi scegliete il file system ONTAP per il quale desiderate aggiornare un SVM.
   - Scegli la scheda Storage virtual machines.

     —Oppure—
   - Per visualizzare un elenco di tutte le SVM attualmente disponibili Regione AWS, Account AWS espandi ONTAP e scegli Storage virtual machines.
3. Scegli la macchina virtuale di archiviazione che desideri aggiornare.
4. Scegli Azioni > Aggiorna la password dell'amministratore. Viene visualizzata la finestra Aggiorna credenziali amministrative SVM.
5. Immettere la nuova password per l'`vsadmin`utente e confermarla.
6. Scegli Aggiorna credenziali per salvare la nuova password.

Per aggiornare le credenziali dell'account amministratore SVM (CLI)

- Per aggiornare la configurazione di un FSx for ONTAP SVM, utilizzate il comando update-storage-virtual-machineCLI (o l'operazione UpdateStorageVirtualMachineAPI equivalente), come illustrato nell'esempio seguente.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

Dopo aver creato correttamente la macchina virtuale di storage, Amazon FSx ne restituisce la descrizione in formato JSON, come illustrato nell'esempio seguente.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
```

```
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
    "StorageVirtualMachineId": "svm-abcdef01234567890",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

Eliminazione di una macchina virtuale di archiviazione (SVM)

Puoi eliminare una SVM FSx for ONTAP solo utilizzando la console Amazon FSx, l'API e l'API. AWS CLI Prima di poter eliminare una SVM, è necessario eliminare prima tutti i volumi non root collegati alla SVM.

> **Important**
>
> Non è possibile eliminare una SVM utilizzando la NetApp CLI o l'API ONTAP.

> **Note**
>
> Prima di eliminare una macchina virtuale di archiviazione, assicuratevi che nessuna applicazione stia accedendo ai dati nella SVM e di aver eliminato tutti i volumi non root collegati alla SVM.

Per eliminare una macchina virtuale di archiviazione (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli la SVM che desideri eliminare come segue:

   - Nel riquadro di navigazione a sinistra, scegliete File system, quindi scegliete il file system ONTAP per il quale desiderate eliminare un SVM.
   - Scegli la scheda Storage virtual machines.

   —Oppure—

   - Per visualizzare un elenco di tutte le SVM disponibili, espandi ONTAP e scegli Storage virtual machines.

   Seleziona la SVM che desideri eliminare dall'elenco.
3. Nella scheda Volumi, visualizza l'elenco dei volumi collegati alla SVM. Se sono presenti volumi non root collegati alla SVM, è necessario eliminarli prima di poter eliminare la SVM. Per ulteriori informazioni, consulta Eliminazione di un volume.
4. Scegli Elimina macchina virtuale di archiviazione dal menu Azioni.
5. Nella finestra di dialogo di conferma dell'eliminazione, scegli Elimina macchina virtuale di archiviazione.

Per eliminare una macchina virtuale di archiviazione (CLI)

- Per eliminare una macchina virtuale di archiviazione FSx for ONTAP, utilizzate il comando delete-storage-virtual-machineCLI (o l'operazione DeleteStorageVirtualMachineAPI equivalente), come illustrato nell'esempio seguente.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

Visualizzazione dei dettagli di configurazione della macchina virtuale di storage

Puoi visualizzare le macchine virtuali di storage FSx for ONTAP attualmente presenti sul tuo file system utilizzando la console Amazon FSx, AWS CLI l'API Amazon FSx.

Per visualizzare una macchina virtuale di storage sul tuo file system:

- Utilizzo della console: scegli un file system per visualizzarne la pagina di dettaglio dei file system. Per elencare tutte le macchine virtuali di archiviazione sul file system, scegli la scheda Macchine virtuali di archiviazione, quindi scegli la macchina virtuale di archiviazione che desideri visualizzare.
- Utilizzo della CLI o dell'API: utilizza il comando describe-storage-virtual-machinesCLI o l'operazione API. DescribeStorageVirtualMachines

  La risposta del sistema è un elenco di descrizioni complete di tutte le SVM presenti nel tuo account. Regione AWS

Gestione dei volumi FSx for ONTAP

Ogni macchina virtuale di storage (SVM) su un file system FSx for ONTAP può avere uno o più volumi. Un volume è un contenitore di dati isolato per file, directory o unità logiche di storage (LUN) iSCSI. I volumi sono dotati di thin provisioning, il che significa che consumano la capacità di storage solo per i dati in essi contenuti.

È possibile accedere a un volume da client Linux, Windows o macOS tramite il protocollo Network File System (NFS), il protocollo Server Message Block (SMB) o tramite il protocollo Internet Small Computer Systems Interface (iSCSI) creando un LUN iSCSI (storage a blocchi condiviso). FSx for ONTAP supporta anche l'accesso multiprotocollo (accesso NFS e SMB simultaneo) allo stesso volume.

Puoi creare volumi utilizzando AWS Management Console, AWS CLI, l'API Amazon FSX o NetApp BlueXP. Puoi anche utilizzare l'endpoint amministrativo del tuo file system o SVM per creare, aggiornare ed eliminare volumi utilizzando la CLI NetApp ONTAP o l'API REST.

> **Note**
>
> È possibile creare 500 volumi per coppia HA, fino a 1.000 volumi per tutte le coppie HA. FlexGroupi volumi costituenti vengono conteggiati ai fini di questo limite. Per impostazione predefinita, ci sono otto volumi costituenti per aggregato, per. FlexGroup

Quando si crea un volume, si definiscono le seguenti proprietà:

- Stile del volume: lo stile del volume può essere uno FlexVol oFlexGroup.

- Nome del volume: il nome del volume.
- Tipo di volume: il tipo di volume può essere Read-Write (RW) o Data protection (DP). I volumi DP sono di sola lettura e vengono utilizzati come destinazione in una relazione or. NetApp SnapMirror SnapVault
- Dimensione del volume: si tratta della quantità massima di dati che il volume può archiviare, indipendentemente dal livello di storage.
- Percorso di giunzione: questa è la posizione nello spazio dei nomi di SVM in cui viene montato il volume.
- Efficienza dello storage: le funzionalità di efficienza dello storage, tra cui la compattazione, la compressione e la deduplicazione dei dati, offrono un risparmio di storage tipico del 65% per carichi di lavoro di condivisione di file generici.
- Stile di sicurezza del volume (Unix, NTFS o misto): determina il tipo di autorizzazioni utilizzate per l'accesso ai dati sul volume durante l'autorizzazione degli utenti.
- Suddivisione dei dati su più livelli: la politica di suddivisione in più livelli definisce quali dati vengono archiviati nel livello del pool di capacità a costi contenuti.
- Periodo di raffreddamento della politica di suddivisione in più livelli: definisce quando i dati vengono contrassegnati come freddi e trasferiti in un pool di storage con pool di capacità.
- Politica relativa alle istantanee: le policy relative alle istantanee definiscono il modo in cui il sistema crea le istantanee per un volume. Puoi scegliere tra tre politiche predefinite o utilizzare una politica personalizzata creata utilizzando l'ONTAP CLI o l'API REST.
- Copia i tag nei backup: Amazon FSx copierà automaticamente tutti i tag dai volumi ai backup utilizzando questa opzione. Puoi impostare questa opzione utilizzando l'API AWS CLI o Amazon FSx.

Argomenti

- Stili di volume
- Tipi di volume
- Stile di sicurezza del volume
- Creazione di volumi
- Aggiornamento di un volume
- Eliminazione di un volume
- Visualizzazione di un volume

Stili di volume

FSx for ONTAP offre due stili di volumi che è possibile utilizzare per scopi diversi. Puoi creare uno FlexVol o più FlexGroup volumi utilizzando la console Amazon FSx AWS CLI, e l'API Amazon FSx.

- FlexVoli volumi offrono l'esperienza più semplice per i file system con una coppia ad alta disponibilità (HA) e sono lo stile di volume predefinito per i file system con scalabilità verticale. La dimensione minima di un FlexVol volume è 20 mebibyte (MiB) e la dimensione massima è 314.572.800 MiB.
- FlexGroupi volumi sono composti da più volumi costituenti, il che consente loro di offrire prestazioni e scalabilità di archiviazione più elevate rispetto ai FlexVol volumi per file system con più coppie HA. FlexVol FlexGroupi volumi sono lo stile di volume predefinito per i file system con scalabilità orizzontale. La dimensione minima di un FlexGroup volume è di 100 gibibyte (GiB) per costituente e la dimensione massima è di 20 pebibyte (PiB).

Puoi convertire un volume con lo FlexVol stile nello FlexGroup stile con la ONTAP CLI, che crea un volume FlexGroup con un singolo componente. Tuttavia, si consiglia di AWS DataSync utilizzare lo spostamento dei dati tra un FlexVol volume e un nuovo FlexGroup volume per garantire che i dati siano distribuiti uniformemente tra i componenti. FlexGroup's Per ulteriori informazioni, consulta FlexGroupcostituenti.

> **Note**
>
> Se desideri utilizzare la ONTAP CLI per convertire un FlexVol volume in un FlexGroup volume, assicurati di eliminare tutti i backup del FlexVol volume prima di convertirlo. ONTAPnon ribilancia automaticamente i dati come parte della conversione, pertanto i dati potrebbero essere squilibrati tra i componenti. FlexGroup

FlexGroupcostituenti

Un FlexGroup volume è composto da componenti, che sono volumi. FlexVol Per impostazione predefinita, FSx for ONTAP assegna otto componenti a un volume per coppia HA. FlexGroup

Quando create il FlexGroup volume, la sua dimensione viene divisa equamente tra i suoi componenti. Ad esempio, se create un FlexGroup volume da 800 gigabyte (GB) con otto componenti, ogni costituente avrà una dimensione di 100 GB. Un FlexGroup volume può avere una dimensione

compresa tra 100 GB e 20 PiB, ma la dimensione totale dipende dalla dimensione dei componenti. Ogni componente ha una dimensione minima di 100 GB e una dimensione massima di 300 TiB. Ad esempio, un FlexGroup volume con otto componenti ha una dimensione minima di 800 GB e una dimensione massima di 20 PiB.

ONTAP distribuisce i dati a livello di file tra i componenti. Puoi archiviare fino a due miliardi di file in ogni componente del tuo volume. FlexGroup

Quando aggiorni la dimensione del FlexGroup volume, la nuova dimensione viene distribuita uniformemente tra i componenti esistenti.

Puoi anche aggiungere altri componenti al tuo FlexGroup volume utilizzando la ONTAP CLI o l'API REST. Tuttavia, ti consigliamo di farlo solo se hai bisogno di capacità di archiviazione aggiuntiva e tutti i tuoi componenti hanno già raggiunto la dimensione massima (300 TiB per componente). L'aggiunta di componenti può portare a uno squilibrio di dati e I/O tra i componenti. Finché i componenti non saranno bilanciati, è possibile che la velocità di scrittura sia inferiore del 5-10% rispetto a un volume bilanciato. FlexGroup Quando vengono scritti nuovi dati sul FlexGroup volume, ONTAP dà la priorità alla loro distribuzione tra i nuovi componenti fino al bilanciamento dei componenti. Se aggiungi nuovi componenti, ti consigliamo di scegliere un numero pari e di non superare gli otto per aggregato.

> **Note**
>
> Se aggiungi nuovi componenti, le istantanee esistenti diventano istantanee parziali; pertanto, non possono essere utilizzate per ripristinare completamente il volume allo stato precedente. FlexGroup Le istantanee precedenti non possono offrire un' point-in-time immagine completa del FlexGroup volume perché i nuovi componenti non esistevano ancora. Tuttavia, le istantanee parziali possono essere utilizzate per ripristinare singoli file e directory, per creare un nuovo volume o per eseguire la replica. SnapMirror

Tipi di volume

FSx for ONTAP offre due tipi di volumi che è possibile creare utilizzando la console Amazon FSx, e AWS CLI l'API Amazon FSx.

- I volumi di lettura-scrittura (RW) vengono utilizzati nella maggior parte dei casi. Come indica il nome, sono leggibili e scrivibili.

- I volumi di protezione dei dati (DP) sono volumi di sola lettura che vengono utilizzati come destinazione di una relazione or. NetApp SnapMirror SnapVault È consigliabile utilizzare i volumi DP quando si desidera migrare o proteggere i dati di un singolo volume.

FlexVole FlexGroup i volumi possono essere RW o DP.

> **Note**
>
> Non è possibile aggiornare il tipo di un volume dopo la creazione del volume.

Stile di sicurezza del volume

FSx for ONTAP supporta 3 diversi stili di sicurezza dei volumi: Unix, NTFS e misto. Ogni stile di sicurezza ha un effetto diverso sul modo in cui vengono gestite le autorizzazioni per i dati. È necessario comprendere i diversi effetti per assicurarsi di selezionare lo stile di sicurezza appropriato per i propri scopi.

È importante comprendere che gli stili di sicurezza non determinano quali tipi di client possono o non possono accedere ai dati. Gli stili di sicurezza determinano solo il tipo di autorizzazioni utilizzate da FSx for ONTAP per controllare l'accesso ai dati e il tipo di client che può modificare tali autorizzazioni.

I due fattori utilizzati per determinare lo stile di sicurezza di un volume sono il tipo di amministratori che gestiscono il file system e il tipo di utenti o servizi che accedono ai dati sul volume.

Quando si crea un volume nella console Amazon FSx, nella CLI e nell'API, lo stile di sicurezza viene impostato automaticamente sullo stile di sicurezza del volume root. Puoi modificare lo stile di sicurezza di un volume utilizzando l'API AWS CLI o. È possibile modificare questa impostazione dopo la creazione del volume. Per ulteriori informazioni, consulta Aggiornamento di un volume.

Quando configuri lo stile di sicurezza su un volume, considera le esigenze del tuo ambiente per assicurarti di selezionare lo stile di sicurezza migliore al fine di evitare problemi con la gestione delle autorizzazioni. Tieni presente che lo stile di sicurezza non determina quali tipi di client possono accedere ai dati. Lo stile di sicurezza determina le autorizzazioni utilizzate per consentire l'accesso ai dati e i tipi di client che possono modificare tali autorizzazioni. Di seguito sono riportate alcune considerazioni che possono aiutarti a decidere quale stile di sicurezza scegliere per un volume:

- Unix (Linux): scegliete questo stile di sicurezza se il file system è gestito da un amministratore Unix, la maggior parte degli utenti sono client NFS e un'applicazione che accede ai dati utilizza un

utente Unix come account di servizio. Solo i client Linux possono modificare le autorizzazioni con lo stile di sicurezza Unix e i tipi di permessi usati su file e directory sono mode-bit o ACL NFS v4.x.

- NTFS: scegli questo stile di sicurezza se il file system è gestito da un amministratore di Windows, la maggior parte degli utenti sono client SMB e un'applicazione che accede ai dati utilizza un utente Windows come account di servizio. Se è richiesto l'accesso di Windows a un volume, si consiglia di utilizzare lo stile di sicurezza NTFS. Solo i client Windows possono modificare le autorizzazioni con lo stile di sicurezza NTFS e i tipi di autorizzazioni utilizzati su file e directory sono gli ACL NTFS.
- Mista: si tratta di un'impostazione avanzata. Per ulteriori informazioni, consulta l'argomento Quali sono gli stili di sicurezza e i relativi effetti nel NetApp Documentation Center.

Creazione di volumi

Puoi creare un FSx for ONTAP FlexVol o un FlexGroup volume utilizzando la console Amazon FSx, l'API Amazon FSx, oltre AWS CLI all'interfaccia a riga di NetApp comando (CLI) ONTAP e all'API REST.

Per creare un volume (console) FlexVol

> **Note**
>
> Lo stile di sicurezza del volume viene impostato automaticamente sullo stile di sicurezza del volume principale.

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli Volumes.
3. Selezionare Create volume (Crea volume).
4. Per il tipo di file system, scegli Amazon FSx for NetApp ONTAP.
5. Nella sezione Dettagli del file system, fornisci le seguenti informazioni:
   - Per File system, scegli il file system su cui creare il volume.
   - Per Macchina virtuale di archiviazione, scegli la macchina virtuale di archiviazione (SVM) su cui creare il volume.
6. Nella sezione Stile del volume, scegli FlexVol.
7. Nella sezione Dettagli del volume, fornisci le seguenti informazioni:

- Nel campo Nome del volume, fornisci un nome per il volume. È possibile utilizzare fino a 203 caratteri alfanumerici o di sottolineatura (_).
- Per Dimensione del volume, immettete un numero intero compreso tra 20 e 314572800 per specificare la dimensione in mebibyte (MiB).
- Per Tipo di volume, scegliete Read-Write (RW) per creare un volume leggibile e scrivibile o Data Protection (DP) per creare un volume di sola lettura che può essere utilizzato come destinazione di una relazione or. NetApp SnapMirror SnapVault Per ulteriori informazioni, consulta Tipi di volume.
- Per Junction path, inserite una posizione all'interno del file system in cui montare il volume. Il nome deve avere una barra iniziale, ad esempio `/vol3`.
- Per l'efficienza dello storage, scegli Enabled per abilitare le funzionalità di efficienza dello storage ONTAP (deduplicazione, compressione e compattazione). Per ulteriori informazioni, consulta FSx per l'efficienza dello storage ONTAP.
- Per lo stile di sicurezza Volume, scegli tra Unix (Linux), NTFS e Mixed per il volume. Per ulteriori informazioni, consulta Stile di sicurezza del volume.
- Per la policy Snapshot, scegli una policy di snapshot per il volume. Per ulteriori informazioni sulle politiche relative alle snapshot, vedere. Politiche relative alle istantanee

  Se si sceglie Politica personalizzata, è necessario specificare il nome della politica nel campo Custom-Policy. La politica personalizzata deve già esistere sulla SVM o nel file system. Puoi creare una policy di snapshot personalizzata con la CLI ONTAP o l'API REST. Per ulteriori informazioni, consulta Creare una policy per le istantanee nella documentazione del NetApp prodotto ONTAP.

8. Nella sezione Storage tiering, fornisci le seguenti informazioni:

   - Per la politica di suddivisione in più livelli del pool di capacità, scegli la politica di suddivisione in più livelli del pool di storage per il volume, che può essere Auto (impostazione predefinita), Solo snapshot, Tutti o Nessuno. Per ulteriori informazioni, consulta Politiche di suddivisione in livelli di volume.
   - Se si sceglie Auto o Solo snapshot, è possibile impostare il periodo di raffreddamento della politica di tiering per definire il numero di giorni prima che i dati a cui non è stato effettuato l'accesso vengano contrassegnati come freddi e trasferiti nello storage del pool di capacità. È possibile fornire un valore compreso tra 2 e 183 giorni. L'impostazione predefinita è 31 giorni.

9. Nella sezione Avanzate, per SnapLockConfigurazione, scegli tra Abilitato e Disabilitato. Per ulteriori informazioni sulla configurazione di un volume SnapLock Compliance o di un volume

SnapLock Enterprise, consulta Creazione di un volume di SnapLock conformità eCreazione di un volume SnapLock Enterprise. Per ulteriori informazioni su SnapLock, consulta Proteggi i tuoi dati con SnapLock.

10. Scegli Conferma per creare il volume.

È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system, nella colonna Stato del riquadro Volumi. Il volume è pronto per l'uso quando viene impostato lo stato Creato.

Per creare un FlexGroup volume (console)

> **Note**
>
> Puoi creare FlexGroup volumi per file system con scalabilità orizzontale solo utilizzando la console Amazon FSx. Per creare FlexVol volumi per i tuoi file system con scalabilità orizzontale, usa l'API AWS CLI Amazon FSx o gli strumenti di gestione. NetApp

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli Volumes.
3. Selezionare Create volume (Crea volume).
4. Per il tipo di file system, scegli Amazon FSx for NetApp ONTAP.
5. Nella sezione Dettagli del file system, fornisci le seguenti informazioni:
   - Per File system, scegli il file system su cui creare il volume.
   - Per Macchina virtuale di archiviazione, scegli la macchina virtuale di archiviazione (SVM) su cui creare il volume.
6. Nella sezione Stile del volume, scegli FlexGroup.
7. Nella sezione Dettagli del volume, fornisci le seguenti informazioni:
   - Nel campo Nome del volume, fornisci un nome per il volume. È possibile utilizzare fino a 203 caratteri alfanumerici o di sottolineatura (_).
   - Per Dimensione del volume, immettere un numero intero compreso tra 800 gibibyte (GiB) e 2.000 pebibyte (PiB).
   - Per Tipo di volume, scegliete Read-Write (RW) per creare un volume leggibile e scrivibile o Data Protection (DP) per creare un volume di sola lettura che può essere utilizzato come

destinazione di una relazione or. NetApp SnapMirror SnapVault Per ulteriori informazioni, consulta Tipi di volume.

- Per Junction path, inserite una posizione all'interno del file system in cui montare il volume. Il nome deve avere una barra iniziale, ad esempio `/vol3`.
- Per l'efficienza dello storage, scegli Enabled per abilitare le funzionalità di efficienza dello storage ONTAP (deduplicazione, compressione e compattazione). Per ulteriori informazioni, consulta FSx per l'efficienza dello storage ONTAP.
- Per lo stile di sicurezza Volume, scegli tra Unix (Linux), NTFS e Mixed per il volume. Per ulteriori informazioni, consulta Stile di sicurezza del volume.

> **Note**
>
> Lo stile di sicurezza del volume viene impostato automaticamente sullo stile di sicurezza del volume principale.

- Per la policy Snapshot, scegli una policy di snapshot per il volume. Per ulteriori informazioni sulle politiche relative alle snapshot, vedere. Politiche relative alle istantanee

  Se si sceglie Politica personalizzata, è necessario specificare il nome della politica nel campo Custom-Policy. La politica personalizzata deve già esistere sulla SVM o nel file system. Puoi creare una policy di snapshot personalizzata con la CLI ONTAP o l'API REST. Per ulteriori informazioni, consulta Creare una policy per le istantanee nella documentazione del NetApp prodotto ONTAP.

8. Nella sezione Storage tiering, fornisci le seguenti informazioni:

   - Per la politica di suddivisione in più livelli del pool di capacità, scegli la politica di suddivisione in più livelli del pool di storage per il volume, che può essere Auto (impostazione predefinita), Solo snapshot, Tutti o Nessuno. Per ulteriori informazioni, consulta Politiche di suddivisione in livelli di volume.
   - Se si sceglie Auto o Solo snapshot, è possibile impostare il periodo di raffreddamento della politica di tiering per definire il numero di giorni prima che i dati a cui non è stato effettuato l'accesso vengano contrassegnati come freddi e trasferiti nello storage del pool di capacità. È possibile fornire un valore compreso tra 2 e 183 giorni. L'impostazione predefinita è 31 giorni.

9. Nella sezione Avanzate, per SnapLockConfigurazione, scegli tra Abilitato e Disabilitato. Per ulteriori informazioni sulla configurazione di un volume SnapLock Compliance o di un volume SnapLock Enterprise, consulta Creazione di un volume di SnapLock conformità eCreazione di un

volume SnapLock Enterprise. Per ulteriori informazioni su SnapLock, consulta Proteggi i tuoi dati con SnapLock.

10. Scegli Conferma per creare il volume.

È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system, nella colonna Stato del riquadro Volumi. Il volume è pronto per l'uso quando viene impostato lo stato Creato.

Per creare un volume (CLI)

- Per creare un volume FSx for ONTAP, utilizzate il comando create-volume CLI (o l'operazione CreateVolumeAPI equivalente), come illustrato nell'esempio seguente.

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
          SizeInMegabytes=1024,SnapshotPolicy=default, \
          StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
          StorageEfficiencyEnabled=true
```

Dopo aver creato correttamente il volume, Amazon FSx restituisce la sua descrizione in formato JSON, come mostrato nell'esempio seguente.

```
{
    "Volume": {
        "CreationTime": "2022-08-12T13:03:37.625000-04:00",
        "FileSystemId": "fs-abcdef0123456789c",
        "Lifecycle": "CREATING",
        "Name": "vol1",
        "OntapConfiguration": {
            "CopyTagsToBackups": true,
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "NTFS",
            "SizeInMegabytes": 1024,
            "SnapshotPolicy": "default",
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abcdef0123456789a",
```

```
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "NONE"
            },
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
        "VolumeId": "fsvol-abcdef0123456789b",
        "VolumeType": "ONTAP"


    }
}
```

Puoi anche creare un nuovo volume ripristinando un backup di un volume su un nuovo volume. Per ulteriori informazioni, consulta Ripristino dei backup su un nuovo volume.

Aggiornamento di un volume

Puoi aggiornare la configurazione di un volume FSx for ONTAP utilizzando la console Amazon FSx, l'API Amazon FSx, oltre AWS CLI all'interfaccia a riga di NetApp comando (CLI) e all'API REST di ONTAP. È possibile modificare le seguenti proprietà di un volume FSx for ONTAP esistente:

- Nome del volume
- Percorso di giunzione
- Volume size (Dimensione dei volumi)
- Efficienza di archiviazione
- Politica di suddivisione in più livelli del pool di capacità
- Stile di sicurezza del volume
- Politica sulle istantanee
- Periodo di raffreddamento della politica di tiering
- Copia i tag nei backup (utilizzando l'API AWS CLI Amazon FSx)

Per ulteriori informazioni, consulta Gestione dei volumi FSx for ONTAP.

Per aggiornare la configurazione di un volume (console)

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

2. Passa a File system e scegli il file system ONTAP per cui desideri aggiornare un volume.
3. Scegli la scheda Volumi.
4. Scegli il volume che desideri aggiornare.
5. Per Azioni, scegli Aggiorna volume.

   Viene visualizzata la finestra di dialogo Aggiorna volume con le impostazioni correnti del volume.
6. Per Junction path, inserite una posizione esistente all'interno del file system per montare il volume. Il nome deve avere una barra iniziale, ad esempio`/vol15`.
7. Per le dimensioni del volume, puoi aumentare o diminuire le dimensioni del volume all'interno dell'intervallo specificato nella console Amazon FSx. Per FlexVol i volumi, la dimensione massima è di 300 TiB. Per FlexGroup i volumi, la dimensione massima è 300 TiB moltiplicata per il numero totale di volumi costituenti di cui FlexGroup dispone, fino a un massimo di 20 PiB.
8. Per l'efficienza dello storage, scegli Abilitato per abilitare le funzionalità di efficienza dello storage ONTAP (deduplicazione, compressione e compattazione) oppure scegli Disabilitato per disabilitarle.
9. Per la politica di suddivisione in più livelli del pool di capacità, scegli una nuova politica di suddivisione in più livelli del pool di storage per il volume, che può essere Auto (impostazione predefinita), Solo snapshot, Tutti o Nessuno. Per ulteriori informazioni sulle politiche di suddivisione in più livelli del pool di capacità, vedere. Politiche di suddivisione in livelli di volume
10. Per lo stile di sicurezza Volume, scegli Unix (Linux), NTFS o Mixed. Lo stile di sicurezza di un volume determina se dare la preferenza agli ACL NTFS o UNIX per l'accesso multiprotocollo. La modalità MIXED non è richiesta per l'accesso multiprotocollo ed è consigliata solo per utenti esperti.
11. Per la policy Snapshot, scegli una policy di snapshot per il volume. Per ulteriori informazioni sulle politiche relative alle snapshot, vedere. Politiche relative alle istantanee

    Se si sceglie Politica personalizzata, è necessario specificare il nome della politica nel campo Custom-Policy. La politica personalizzata deve già esistere sulla SVM o nel file system. Puoi creare una policy di snapshot personalizzata con la CLI ONTAP o l'API REST. Per ulteriori informazioni, consulta Creare una policy per le istantanee nella documentazione del NetApp prodotto ONTAP.
12. Per il periodo di raffreddamento della politica di tiering, i valori validi sono 2-183 giorni. Il periodo di raffreddamento della politica di tiering di un volume definisce il numero di giorni prima che i dati a cui non è stato effettuato l'accesso vengano contrassegnati come freddi e trasferiti nello

storage con pool di capacità. Questa impostazione influisce solo sulle `Snapshot-only` politiche `Auto` and.

13. Scegli Aggiorna per aggiornare il volume.

Per aggiornare la configurazione di un volume (CLI)

- Per aggiornare la configurazione di un volume FSx for ONTAP, utilizzate il comando CLI update-volume (o l'operazione UpdateVolumeAPI equivalente), come illustrato nell'esempio seguente.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

Eliminazione di un volume

Puoi eliminare un volume FSx for ONTAP utilizzando la console Amazon FSx, l'API Amazon FSx, oltre AWS CLI all'interfaccia a riga di NetApp comando (CLI) ONTAP e all'API REST.

> **Important**
>
> Puoi eliminare i volumi utilizzando la console, l'API o la CLI di Amazon FSx solo se sul volume sono abilitati i backup Amazon FSx.

> **Important**
>
> Quando elimini un volume utilizzando la console Amazon FSx, hai la possibilità di eseguire un backup finale del volume. Puoi creare nuovi volumi dai backup. Si consiglia di scegliere di eseguire un backup finale come procedura consigliata. Se ritieni di non averne bisogno dopo un certo periodo di tempo, puoi eliminare questo e altri backup di volume creati manualmente. Quando elimini un volume utilizzando il comando `delete-volume` CLI, Amazon FSx esegue un backup finale per impostazione predefinita.

Prima di eliminare un volume, assicurati che nessuna applicazione acceda ai dati del volume che desideri eliminare.

Per eliminare un volume (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli File system, quindi scegli il file system ONTAP da cui desideri eliminare un volume.
3. Scegli la scheda Volumi.
4. Scegli il volume che desideri eliminare.
5. Per Azioni, scegli Elimina volume.
6. Nella finestra di dialogo di conferma, per Crea backup finale, sono disponibili due opzioni:
   - Scegli Sì per eseguire un backup finale del volume. Viene visualizzato il nome del backup finale.
   - Scegli No se non desideri un backup finale del volume. Ti viene chiesto di confermare che, una volta eliminato il volume, i backup automatici non sono più disponibili.
7. Conferma l'eliminazione del volume inserendo delete nel campo Conferma eliminazione.
8. Scegli Elimina volume/i.

Per eliminare un volume (CLI)

- Per eliminare un volume FSx for ONTAP, utilizzate il comando delete-volume CLI (o l'operazione DeleteVolumeAPI equivalente), come illustrato nell'esempio seguente.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Visualizzazione di un volume

Puoi visualizzare i volumi FSx for ONTAP attualmente presenti sul tuo file system utilizzando la console Amazon FSx, l'API e AWS CLI gli SDK di Amazon FSx.

Per visualizzare i volumi sul tuo file system:

- Utilizzo della console: scegli un file system per visualizzare la pagina dei dettagli dei file system. Scegli la scheda Volumi per elencare tutti i volumi del file system, quindi scegli il volume che desideri visualizzare.
- Utilizzo della CLI o dell'API: utilizza il comando CLI describe-volumes o l'operazione API. DescribeVolumes

Creazione di un LUN iSCSI

Questo processo descrive come creare un LUN iSCSI su un file system scalabile Amazon FSx for NetApp ONTAP utilizzando il comando ONTAP CLI. NetApp lun create Per ulteriori informazioni, consulta il Centro di documentazione ONTAP. lun create NetApp

> **Note**
>
> Il protocollo iSCSI non è supportato per i file system con scalabilità orizzontale.

Questo processo presuppone che sul file system sia già stato creato un volume. Per ulteriori informazioni, consulta Creazione di volumi.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.
2. Creare un LUN utilizzando il comando lun create NetApp CLI, sostituendo i seguenti valori:

   - ***`svm_name`***- Il nome della macchina virtuale di archiviazione (SVM) che fornisce la destinazione iSCSI. L'host utilizza questo valore per raggiungere il LUN.
   - ***`vol_name`***- Il nome del volume che ospita il LUN.
   - ***`lun_name`***- Il nome che si desidera assegnare al LUN.
   - ***`size`***- La dimensione, in byte, del LUN. La dimensione massima del LUN che è possibile creare è di 128 TB.

> **Note**
>
> Si consiglia di utilizzare un volume almeno del 5% più grande della dimensione del LUN. Questo margine lascia spazio per le istantanee del volume.

- ***ostype***- Il sistema operativo dell'host, o`windows_2008`. `linux` Utilizzabile `windows_2008` per tutte le versioni di Windows; ciò garantisce che il LUN abbia un offset di blocco adeguato per il sistema operativo e ottimizza le prestazioni.

> **Note**
>
> Si consiglia di abilitare l'allocazione dello spazio sul LUN. Con l'allocazione dello spazio abilitata, ONTAP può informare l'host quando la capacità del LUN è esaurita e può recuperare spazio quando si eliminano i dati dal LUN.

Per ulteriori informazioni, consulta la `lun create`documentazione della CLI di NetApp ONTAP.

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
ostype ostype -space-allocation enabled
```

```
Created a LUN of size 10g (10737418240)
```

3. Conferma che il LUN sia stato creato, online e mappato.

```
> lun show
```

Il sistema risponde con il seguente output:

```
Vserver   Path                            State   Mapped   Type         Size
--------- ------------------------------- ------- -------- ------------ --------
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

Passaggi successivi

Dopo aver creato un LUN iSCSI, il passaggio successivo del processo di utilizzo di un LUN iSCSI come storage a blocchi consiste nel mappare il LUN su un. `igroup` Per ulteriori informazioni, consulta Montaggio di LUN iSCSI su un client Linux o Montaggio di LUN iSCSI su un client Windows.

Gestione delle condivisioni SMB

Per gestire le condivisioni di file SMB sul tuo file system Amazon FSx, puoi utilizzare l'interfaccia grafica delle cartelle condivise di Microsoft Windows. L'interfaccia grafica delle cartelle condivise fornisce una posizione centrale per la gestione di tutte le cartelle condivise nella macchina virtuale di storage (SVM). Le seguenti procedure descrivono in dettaglio come creare, aggiornare e rimuovere le condivisioni di file.

> **Note**
>
> È inoltre possibile gestire le condivisioni di file SMB utilizzando NetApp System Manager. Per ulteriori informazioni, consulta Utilizzo di NetApp System Manager con BlueXP.

Per connettere cartelle condivise al tuo file system Amazon FSx

1. Avvia l'istanza Amazon EC2 e collegala a Microsoft Active Directory a cui è collegato il file system Amazon FSx. A tale scopo, scegli una delle seguenti procedure dalla Guida all'AWS Directory Service amministrazione:
   - Unisciti senza problemi a un'istanza Windows EC2
   - Unisciti manualmente a un'istanza Windows
2. Connect alla propria istanza come utente membro del gruppo di amministratori del file system. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
3. Apri il menu Start ed esegui fsmgmt.msc utilizzando Esegui come amministratore. In questo modo si apre lo strumento GUI delle cartelle condivise.
4. Per Azione, scegli Connetti a un altro computer.
5. Per un altro computer, inserisci il nome DNS della tua macchina virtuale di archiviazione (SVM), ad esempio. **`netbios_name.corp.example.com`**

Per trovare il nome DNS della tua SVM sulla console Amazon FSx, scegli Storage virtual machines, scegli la tua SVM, quindi scorri verso il basso fino a Endpoints fino a trovare il nome DNS SMB. Puoi anche ottenere il nome DNS nella risposta dell'operazione API. DescribeStorageVirtualMachines

6. Scegli OK. Viene quindi visualizzata una voce relativa al file system Amazon FSx nell'elenco dello strumento Cartelle condivise.

Ora che Shared Folders è connesso al tuo file system Amazon FSx, puoi gestire le condivisioni di file Windows sul file system con le seguenti azioni:

> **Note**
>
> Ti consigliamo di localizzare le tue condivisioni SMB su un volume diverso dal volume root.

- Crea una nuova condivisione di file: nello strumento Cartelle condivise, scegli Condivisioni nel riquadro a sinistra per visualizzare le condivisioni attive per il tuo file system Amazon FSx. I volumi vengono visualizzati montati sul percorso scelto durante la creazione del volume. Scegli Nuova condivisione e completa la procedura guidata Crea una cartella condivisa.

  È necessario creare la cartella locale prima di creare la nuova condivisione di file. È possibile eseguire questa operazione nel modo seguente:

  - Utilizzando lo strumento Cartelle condivise: scegli Sfoglia quando specifichi il percorso di una cartella locale, scegli Crea nuova cartella per creare la cartella locale.
  - Utilizzando la riga di comando:

    ```
    New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
    $volume_path\MyNewFolder
    ```

- Modifica una condivisione di file: nello strumento Cartelle condivise, apri il menu contestuale (fai clic con il pulsante destro del mouse) per la condivisione di file che desideri modificare nel riquadro destro e scegli Proprietà. Modificate le proprietà e scegliete OK.
- Rimuovi una condivisione di file: nello strumento Cartelle condivise, apri il menu contestuale (fai clic con il pulsante destro del mouse) relativo alla condivisione di file che desideri rimuovere nel riquadro di destra, quindi scegli Interrompi condivisione.

> **Note**
>
> La rimozione delle condivisioni di file dalla GUI è possibile solo se ti sei connesso a fsmgmt.msc utilizzando il nome DNS del file system Amazon FSx. Se ti sei connesso utilizzando l'indirizzo IP o il nome alias DNS del file system, l'opzione Stop Sharing non funzionerà e la condivisione di file non verrà rimossa.

Audit dell'accesso ai file

Amazon FSx per NetApp ONTAP supporta il controllo degli accessi degli utenti finali a file e directory in una macchina virtuale di archiviazione (SVM).

Argomenti

Panoramica del controllo dell'accesso ai file

Il controllo dell'accesso ai file consente di registrare gli accessi degli utenti finali a singoli file e directory in base alle politiche di controllo definite dall'utente. Il controllo dell'accesso ai file può aiutarti a migliorare la sicurezza del sistema e ridurre il rischio di accesso non autorizzato ai dati di sistema. Il controllo dell'accesso ai file aiuta le organizzazioni a mantenere la conformità ai requisiti di protezione dei dati, a identificare tempestivamente le potenziali minacce e a ridurre il rischio di violazione dei dati.

In tutti gli accessi a file e directory, Amazon FSx supporta la registrazione dei tentativi riusciti (ad esempio un utente con autorizzazioni sufficienti che accede con successo a un file), dei tentativi falliti o di entrambi. Puoi anche disattivare il controllo dell'accesso ai file in qualsiasi momento.

Per impostazione predefinita, i registri degli eventi di controllo sono archiviati nel formato diEVTX file, che consente di visualizzarli utilizzando Microsoft Event Viewer.

Eventi di accesso SMB che possono essere controllati

La tabella seguente elenca gli eventi di accesso ai file e alle cartelle SMB che possono essere controllati.

ID evento (EVT/EVTX)	Evento	Descrizione	Categoria
560/4656	Apri oggetto/Crea oggetto	ACCESSO ALL'OGGETTO: oggetto (file o directory) aperto	Accesso ai file
563/4659	Apri oggetto con l'intento di eliminarlo	ACCESSO ALL'OGGETTO: è stato richiesto un handle di un oggetto (file o directory) con l'intento di eliminare	Accesso ai file
564/4660	Eliminazione dell'oggetto	ACCESSO ALL'OGGETTO: Elimina oggetto (file o directory). ONTAP genera questo evento quando un client Windows tenta di eliminare l'oggetto (file o directory)	Accesso ai file
567/4663	Leggi oggetto/Scrivi oggetto/Ottieni attributi dell'oggetto/Imposta gli attributi dell'oggetto	ACCESSO ALL'OGGETTO: tentativo di accesso all'oggetto (lettura, scrittura, acquisizione dell'attributo, impostazione dell'attributo).	Accesso ai file

ID evento (EVT/EVTX)	Evento	Descrizione	Categoria
		Note Per questo evento, ONTAP controlla solo la prima operazione di lettura e scrittura SMB (riuscita o fallita) su un oggetto. Ciò impedisce a ONTAP di creare un numero eccessivo di voci di registro quando un singolo client apre un oggetto ed esegue molte operazioni di lettura o scrittura successive sullo stesso oggetto.	

ID evento (EVT/EVTX)	Evento	Descrizione	Categoria
N/A/4664	Collegamento fisso	ACCESSO ALL'OGGETTO: è stato effettuato un tentativo di creare un collegamento fisico	Accesso ai file
N/A/N/A ID evento ONTAP 9999	Rinominare un oggetto	ACCESSO ALL'OGGETTO: oggetto rinominato. Questo è un evento ONTAP. Attualmente non è supportato da Windows come evento singolo.	Accesso ai file
N/A/N/A ID evento ONTAP 9998	Oggetto Unlink	ACCESSO ALL'OGGETTO: oggetto non collegato. Questo è un evento ONTAP. Attualmente non è supportato da Windows come evento singolo.	Accesso ai file

Eventi di accesso NFS che possono essere controllati

È possibile controllare i seguenti eventi di accesso a file e cartelle NFS.

- READ
- OPEN
- CLOSE
- LEGGI LA DIR
- WRITE

- SETATTR
- CREATE
- COLLEGAMENTO
- APRI ATTR
- REMOVE
- GETATTR
- VERIFICARE
- N VERIFICA
- RENAME

Panoramica delle attività per l'impostazione del controllo dell'accesso ai file

La configurazione di FSx for ONTAP per il controllo dell'accesso ai file comporta le seguenti attività di alto livello:

1. Acquisisci familiarità con i requisiti e le considerazioni relative al controllo dell'accesso ai file.
2. Crea una configurazione di controllo su un SVM specifico.
3. Abilita il controllo su quella SVM.
4. Configura le politiche di controllo sui tuoi file e directory.
5. Visualizza i registri degli eventi di audit dopo che FSx for ONTAP li ha emessi.

I dettagli delle attività sono forniti nelle seguenti procedure.

Ripeti le operazioni per qualsiasi altra SVM sul tuo file system per cui desideri abilitare il controllo degli accessi ai file.

Requisiti di audit

Prima di configurare e abilitare il audit su una SVM, è importante considerare i seguenti requisiti e tenere presente quanto riportato di seguito.

- Il controllo NFS supporta l'audit delle voci di controllo degli accessi (ACE) designate come tipou, che generano una voce del registro di controllo quando si tenta di accedere all'oggetto. Per il controllo NFS, non esiste una mappatura tra i bit di modalità e gli ACE di controllo. Quando si

convertono gli ACL in bit di modalità, gli ACE di controllo vengono ignorati. Quando si convertono i bit di modalità in ACL, gli ACE di controllo non vengono generati.

- Il controllo dipende dalla disponibilità di spazio nei volumi di staging. (Un volume di staging è un volume dedicato creato da ONTAP per archiviare i file di staging, che sono file binari intermedi su singoli nodi in cui vengono archiviati i record di controllo prima della conversione in un formato di file EVTX o XML.) È necessario assicurarsi che vi sia spazio sufficiente per i volumi di gestione temporanea in aggregati che contengono volumi controllati.
- Il controllo dipende dalla disponibilità di spazio nel volume contenente la directory in cui sono archiviati i registri degli eventi di controllo convertiti. È necessario assicurarsi che vi sia spazio sufficiente nei volumi utilizzati per archiviare i registri degli eventi. È possibile specificare il numero di registri di controllo da conservare nella directory di controllo utilizzando il `-rotate-limit` parametro durante la creazione di una configurazione di controllo, che può aiutare a garantire che lo spazio disponibile per i registri di controllo nel volume sia sufficiente.

Creazione di configurazioni di controllo su SVM

Prima di poter iniziare a controllare gli eventi di file e directory, è necessario creare una configurazione di controllo sulla Storage Virtual Machine (SVM). Dopo aver creato la configurazione di audit, devi abilitarla nella SVM.

Prima di utilizzare il `vserver audit create` comando per creare la configurazione di controllo, assicuratevi di aver creato una directory da utilizzare come destinazione per i registri e che la directory non contenga collegamenti simbolici. Si specifica la directory di destinazione con il `-destination` parametro.

È possibile creare una configurazione di controllo che ruoti i registri di controllo in base alle dimensioni del registro o a una pianificazione, come segue:

- Per ruotare i registri di controllo in base alla dimensione del registro, usa questo comando:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

  L'esempio seguente crea una configurazione di controllo per l'SVM denominato `svm1` che controlla le operazioni sui file e gli eventi di accesso e disconnessione CIFS (SMB) (impostazione predefinita) utilizzando la rotazione basata sulle dimensioni. Il formato del registro è `EVTX`

(predefinito), i registri sono archiviati nella`/audit_log` directory e avrai un singolo file di registro alla volta (fino a 200 MB di dimensione).

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- Per ruotare i registri di controllo in base a una pianificazione, usa questo comando:

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]
       [-rotate-limit integer] [-rotate-schedule-month chron_month]
       [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-
day chron_dayofmonth]
       [-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

Il`-rotate-schedule-minute` parametro è obbligatorio se si configura la rotazione del registro di controllo basata sul tempo.

L'esempio seguente crea una configurazione di controllo per la SVM denominata`svm2` utilizzando la rotazione basata sul tempo. Il formato del registro è`EVTX` (predefinito) e i registri di controllo vengono ruotati mensilmente, alle 12:30 in tutti i giorni della settimana.

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB  -
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -
rotate-schedule-minute 30
```

È possibile utilizzare il`-format` parametro per specificare se i registri di controllo vengono creati nel`EVTX` formato convertito (predefinito) o nel formato di`XML` file. Il`EVTX` formato consente di visualizzare i file di registro con Microsoft Event Viewer.

Per impostazione predefinita, le categorie di eventi da controllare sono gli eventi di accesso ai file (sia SMB che NFS), gli eventi di accesso e disconnessione CIFS (SMB) e gli eventi di modifica dei criteri di autorizzazione. È possibile avere un maggiore controllo sugli eventi da registrare tramite il`-events` parametro, che ha il seguente formato:

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-
account|authorization-policy-change|security-group}
```

Ad esempio, l'utilizzo`-events file-share` consente il controllo degli eventi di condivisione di file.

Per ulteriori informazioni sul`vserver audit create` comando, vedere Creare una configurazione di controllo.

Abilitare il controllo su una SVM

Dopo aver completato l'impostazione della configurazione di controllo, è necessario abilitare il controllo sulla SVM. A tale scopo, utilizza il seguente comando:

```
vserver audit enable -vserver svm_name
```

Ad esempio, utilizza il seguente comando per abilitare il audit sulla SVM denominata`svm1`.

```
vserver audit enable -vserver svm1
```

Puoi disabilitare il controllo dell'accesso in qualsiasi momento. Ad esempio, utilizzate il seguente comando per disattivare il controllo sulla SVM denominata`svm4`.

```
vserver audit disable -vserver svm4
```

Quando si disabilita il controllo, la configurazione di audit non viene eliminata sull'SVM, il che significa che è possibile riattivare il controllo su tale SVM in qualsiasi momento.

Configurazione delle politiche di controllo di file e cartelle

È necessario configurare le politiche di controllo sui file e sulle cartelle che si desidera vengano controllati per i tentativi di accesso degli utenti. È possibile configurare le politiche di controllo per monitorare i tentativi di accesso riusciti e falliti.

È possibile configurare le politiche di controllo SMB e NFS. Le politiche di audit SMB e NFS hanno requisiti di configurazione e capacità di audit diversi in base allo stile di sicurezza del volume.

Politiche di controllo su file e directory in stile sicurezza NTFS

È possibile configurare le politiche di controllo NTFS utilizzando la scheda Sicurezza di Windows o l'interfaccia a riga di comando di ONTAP.

Per configurare i criteri di controllo NTFS (scheda Sicurezza di Windows)

È possibile configurare le politiche di controllo NTFS aggiungendo voci ai SACL NTFS associati a un descrittore di sicurezza NTFS. Il descrittore di sicurezza viene quindi applicato ai file e alle

directory NTFS. Queste attività vengono gestite automaticamente dalla GUI di Windows. Il descrittore di sicurezza può contenere liste di controllo degli accessi (DACL) discrezionali per l'applicazione delle autorizzazioni di accesso a file e cartelle, SACL per il controllo di file e cartelle o sia SACL che DACL.

1. Dal menu Strumenti di Windows Explorer, seleziona Mappa unità di rete.
2. Completa la casella Map Network Drive:

   a. Scegli una lettera Drive.

   b. Nella casella Cartella, digitare il nome del server SMB (CIFS) che contiene la condivisione, i dati che si desidera controllare e il nome della condivisione.

   c. Scegli Finish (Fine).

   L'unità selezionata è montata e pronta con la finestra di Windows Explorer che mostra i file e le cartelle contenuti nella condivisione.
3. Selezionate il file o la directory per la quale si desidera abilitare l'accesso di audit.
4. Fate clic con il pulsante destro del mouse sul file o sulla directory, quindi scegliete Proprietà.
5. Scegliere la scheda Sicurezza .
6. Fai clic su Avanzate.
7. Scegliete la scheda Controllo.
8. Esegui le azioni desiderate:

Se vuoi...	Esegui queste operazioni
Configurare il controllo per un nuovo utente o gruppo	1. Scegli Add (Aggiungi). 2. Nella casella Inserisci il nome dell'oggetto da selezionare, digita il nome dell'utente o del gruppo che desideri aggiungere. 3. Scegli OK.
Rimozione del audit da un utente o un gruppo	1. Nella casella Inserisci il nome dell'oggetto da selezionare, seleziona l'utente o il gruppo che desideri rimuovere. 2. Scegliere Remove (Rimuovi). 3. Scegli OK. 4. Salta il resto di questa procedura.

Se vuoi...	Esegui queste operazioni
Controllo delle modifiche per un utente o un gruppo	1. Nella casella Inserisci il nome dell'oggetto da selezionare, scegli l'utente o il gruppo che desideri modificare. 2. Scegliere Edit (Modifica). 3. Scegli OK.

Se si sta configurando il controllo su un utente o un gruppo o modificando il controllo su un utente o un gruppo esistente, viene visualizzata la casella Voce di controllo per ***l'oggetto***.

9. Nella casella Applica a, selezionate come applicare questa voce di controllo.

   Se si sta configurando il controllo su un singolo file, la casella Applica a non è attiva, poiché l'impostazione predefinita è Solo questo oggetto.

10. Nella casella Accesso, selezionare ciò che si desidera verificare e se si desidera controllare gli eventi riusciti, gli eventi di fallimento o entrambi.

    - Per controllare gli eventi che hanno avuto successo, scegli la casella Successo.
    - Per controllare gli eventi di errore, selezionare la casella Fallimento.

    Scegli le azioni da monitorare per soddisfare i tuoi requisiti di sicurezza. Per ulteriori informazioni su questi eventi verificabili, consulta la documentazione di Windows. Puoi tenere presente quanto riportato di seguito:

    - Controllo completo
    - Cartella Traverse/ esegui file
    - Cartella di elenco/leggi i dati
    - Leggi gli attributi
    - Leggi gli attributi estesi
    - Crea file/scrivi dati
    - Crea cartelle/ aggiungi dati
    - Scrittura di attributi
    - Scrittura di attributi estesi
    - Eliminare sottocartelle e file

- Delete
- Autorizzazioni di lettura
- Modifica delle autorizzazioni
- Assumere la responsabilità

11. Se non desiderate che l'impostazione di controllo si propaghi ai file e alle cartelle successivi del contenitore originale, selezionate la casella Applica queste voci di controllo solo agli oggetti e/o ai contenitori all'interno di questo contenitore.
12. Seleziona Apply (Applica).
13. Dopo aver aggiunto, rimosso o modificato le voci di controllo, scegli OK.

    La casella Voce di controllo per ***l'oggetto*** si chiude.
14. Nella casella Controllo, scegli le impostazioni di ereditarietà per questa cartella. Scegli solo il livello minimo che fornisce gli eventi di controllo che soddisfano i tuoi requisiti di sicurezza.

    È possibile scegliere una delle seguenti opzioni:

    - Scegliete la casella Includi voci di controllo ereditabili dalla casella principale di questo oggetto.
    - Scegliete la casella Sostituisci tutte le voci di controllo ereditabili esistenti su tutti i discendenti con voci di controllo ereditabili da questo oggetto.
    - Scegli entrambe le scatole.
    - Non scegli nessuna delle due scatole.

    Se si impostano i SACL su un singolo file, la casella Sostituisci tutte le voci di controllo ereditabili esistenti su tutti i discendenti con le voci di controllo ereditabili di questo oggetto non è presente nella casella Controllo.
15. Scegli OK.

Per configurare le politiche di controllo NTFS (ONTAP CLI)

Utilizzando l'interfaccia a riga di comando di ONTAP, è possibile configurare le politiche di controllo NTFS senza la necessità di connettersi ai dati utilizzando una condivisione SMB su un client Windows.

- È possibile configurare le politiche di controllo NTFS utilizzando la famiglia di comandi vserver security file-directory.

Ad esempio, il comando seguente applica una politica di sicurezza denominata`p1` alla SVM denominata`vs0`.

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

Politiche di controllo su file e directory in stile sicurezza UNIX

È possibile configurare il controllo per file e directory in stile di sicurezza UNIX aggiungendo ACE di controllo di accesso (espressioni di controllo degli accessi) agli ACL di NFS v4.x (elenchi di controllo degli accessi). Ciò consente di monitorare determinati eventi di accesso a file e directory NFS per motivi di sicurezza.

> **Note**
>
> Per NFS v4.x, sia gli ACE discrezionali che quelli di sistema sono archiviati nello stesso ACL. Pertanto, è necessario prestare attenzione quando si aggiungono ACE di controllo a un ACL esistente per evitare di sovrascrivere e perdere un ACL esistente. L'ordine in cui si aggiungono gli ACE di controllo a un ACL esistente non ha importanza.

Per configurare le politiche di controllo UNIX

1. Recupera l'ACL esistente per il file o la directory utilizzando il comando`nfs4_getfacl` o equivalente.
2. Aggiungi gli ACE di controllo desiderati.
3. Applica l'ACL aggiornato al file o alla directory utilizzando il comando`nfs4_setfacl` o equivalente.

   Questo esempio utilizza l'`-a`opzione per assegnare a un utente (denominato`testuser`) le autorizzazioni di lettura per il file denominato`file1`.

   ```
   nfs4_setfacl -a "A::testuser@example.com:R" file1
   ```

Visualizzazione dei log di eventi di audit

È possibile visualizzare i registri degli eventi di controllo salvati nei formati di`XML` file`EVTX` o.

- `EVTX`formato file: è possibile aprire i registri degli eventi di`EVTX` controllo convertiti come file salvati utilizzando Microsoft Event Viewer.

  Esistono due opzioni che è possibile utilizzare per visualizzare i registri degli eventi utilizzando Event Viewer:

  - Vista generale: le informazioni comuni a tutti gli eventi vengono visualizzate per il record dell'evento. I dati specifici dell'evento per il record dell'evento non vengono visualizzati. È possibile utilizzare la vista dettagliata per visualizzare dati specifici dell'evento.
  - Vista dettagliata: sono disponibili una visualizzazione intuitiva e una visualizzazione XML. La visualizzazione intuitiva e la visualizzazione XML mostrano sia le informazioni comuni a tutti gli eventi sia i dati specifici dell'evento per il record dell'evento.
- `XML`formato file: è possibile visualizzare ed elaborare i registri degli eventi di controllo XML su applicazioni di terze parti che supportano il formato di file XML. Gli strumenti di visualizzazione XML possono essere utilizzati per visualizzare i log di controllo a condizione che si disponga dello schema XML e delle informazioni sulle definizioni dei campi XML.

Scalabilità della capacità di archiviazione SSD e provisioning degli IOPS

Quando hai bisogno di spazio di archiviazione aggiuntivo per la parte attiva del tuo set di dati, puoi aumentare la capacità di storage su unità a stato solido (SSD) del tuo file system Amazon FSx NetApp for ONTAP. Puoi farlo utilizzando la console Amazon FSx, l'API Amazon FSx o (). AWS Command Line Interface AWS CLI

Puoi anche modificare gli IOPS SSD assegnati per il tuo file system, sia quando aumenti la capacità di archiviazione SSD principale sia come azione indipendente. Per ulteriori informazioni sulla scalabilità della capacità di archiviazione SSD principale di un file system e sulla quantità di IOPS assegnati, consulta. Aggiornamento dello storage SSD e degli IOPS del file system

Gestione della capacità di throughput

FSx for ONTAP configura la capacità di throughput quando si crea il file system. È possibile modificare la capacità di trasmissione del file system con scalabilità verticale in qualsiasi momento, ma non è possibile modificare la capacità di trasmissione del file system con scalabilità orizzontale. Tieni presente che il file system richiede una configurazione specifica per raggiungere la massima capacità di throughput. Ad esempio, per fornire 4 GBps di capacità di throughput per un file system

scalabile verso l'alto, il file system richiede una configurazione con un minimo di 5.120 GiB di capacità di archiviazione SSD e 160.000 IOPS SSD. Per ulteriori informazioni, consulta Impatto della capacità di throughput sulle prestazioni.

La capacità di throughput è un fattore che determina la velocità alla quale il file server che ospita il file system può servire i dati del file. Livelli più elevati di capacità di throughput sono associati a livelli più elevati di rete, operazioni di I/O di lettura del disco (IOPS) e capacità di memorizzazione nella cache dei dati sul file server. Per ulteriori informazioni, consulta Prestazioni.

Quando modifichi la capacità di throughput del file system, Amazon FSx disattiva il file server che alimenta il file system. Sia i file system Single-AZ che Multi-AZ subiscono un failover e un failback automatici durante questo processo, che in genere richiede alcuni minuti per essere completato. I processi di failover e failback sono trasparenti per i client NFS (Network File Sharing), SMB (Server Message Block) e iSCSI (Internet Small Computer Systems Interface), permettendo ai carichi di lavoro di continuare a funzionare senza interruzioni o interventi manuali. Ti verrà addebitata la nuova quantità di capacità di throughput non appena sarà disponibile per il tuo file system.

> **Note**
>
> Per garantire l'integrità dei dati durante le attività di manutenzione, FSx for ONTAP chiude tutti i blocchi opportunistici e completa tutte le operazioni di scrittura in sospeso sui volumi di storage sottostanti che ospitano il file system prima dell'inizio della manutenzione. Durante una finestra di manutenzione pianificata del file system, le modifiche al sistema (come le modifiche alla capacità di throughput) potrebbero subire ritardi. La manutenzione del sistema può far sì che queste modifiche rimangano in coda fino a quando non vengono elaborate. Per ulteriori informazioni, consulta the section called “Finestre di manutenzione”.

Argomenti

Quando modificare la capacità di throughput

Amazon FSx si integra con Amazon CloudWatch, che ti aiuta a monitorare i livelli di utilizzo del throughput continuo del file system. Il throughput e le prestazioni IOPS che è possibile ottenere attraverso il file system dipendono dalle caratteristiche specifiche del carico di lavoro, oltre che dalla capacità di throughput del file system. Di norma, è necessario fornire una capacità di throughput sufficiente a supportare il throughput di lettura del carico di lavoro più il doppio del throughput di scrittura del carico di lavoro. È possibile utilizzare le CloudWatch metriche per determinare quali di queste dimensioni modificare per migliorare le prestazioni. Per ulteriori informazioni, consulta the section called “Come usare FSx per le metriche ONTAP CloudWatch”.

> **Note**
>
> Non è possibile modificare la capacità di throughput per i file system con scalabilità orizzontale.

Come vengono gestite le richieste simultanee di throughput e scalabilità dello storage

È possibile richiedere un aggiornamento della capacità di throughput appena prima dell'inizio del flusso di lavoro di aggiornamento della capacità di archiviazione SSD e dell'IOPS assegnato o mentre è in corso. La sequenza di gestione delle due richieste da parte di Amazon FSx è la seguente:

- Se invii contemporaneamente un aggiornamento SSD/IOPS e un aggiornamento della capacità di throughput, entrambe le richieste vengono accettate. L'aggiornamento SSD/IOPS ha la priorità prima dell'aggiornamento della capacità di throughput.
- Se si invia un aggiornamento della capacità di throughput mentre è in corso un aggiornamento SSD/IOPS, la richiesta di aggiornamento della capacità di throughput viene accettata e messa in coda dopo l'aggiornamento SSD/IOPS. L'aggiornamento della capacità di throughput inizia dopo l'aggiornamento dell'SSD/IOPS (sono disponibili nuovi valori) e durante la fase di ottimizzazione. Questa operazione richiede in genere meno di 10 minuti.
- Se si invia un aggiornamento SSD/IOPS mentre è in corso un aggiornamento della capacità di throughput, la richiesta di aggiornamento dello storage SSD/IOPS viene accettata e messa in coda per iniziare una volta completato l'aggiornamento della capacità di throughput (è disponibile una nuova capacità di throughput). Questa operazione richiede in genere 20 minuti.

Per ulteriori informazioni sullo storage SSD e sugli aggiornamenti IOPS forniti, vedere. Gestione della capacità di archiviazione

Come modificare la capacità di throughput

Puoi modificare la capacità di throughput di un file system utilizzando la console Amazon FSx, AWS CLI () o AWS Command Line Interface l'API Amazon FSx.

Per modificare la capacità di throughput di un file system (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il file system ONTAP per cui desideri aumentare la capacità di throughput.
3. Per Azioni, scegli Aggiorna la capacità di trasmissione. Oppure, nel pannello Riepilogo, scegliete Aggiorna accanto alla capacità di throughput del file system.
4. Scegliete il nuovo valore per la capacità di trasmissione dall'elenco.

   > **Note**
   >
   > È possibile modificare la capacità di throughput per qualsiasi file system FSx for ONTAP. Tuttavia, solo i file system creati a partire dal 9 dicembre 2021 possono supportare una capacità di throughput di 128 MB/s o 256 MB/s.

5. Scegliete Aggiorna per avviare l'aggiornamento della capacità di throughput.
6. È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system, nella scheda Aggiornamenti.

   Puoi monitorare lo stato di avanzamento dell'aggiornamento utilizzando la console Amazon FSxAWS CLI, e l'API. Per ulteriori informazioni, consulta Monitoraggio delle variazioni della capacità di throughput.

Per modificare la capacità di throughput (CLI) di un file system

Per modificare la capacità di throughput di un file system, utilizzate il comando. AWS CLI update-file-system Imposta i seguenti parametri:

- `--file-system-id`dall'ID del file system che state aggiornando.

- `ThroughputCapacity`al valore desiderato a cui aggiornare il file system.

Puoi monitorare lo stato di avanzamento dell'aggiornamento utilizzando la console Amazon FSxAWS CLI, e l'API. Per ulteriori informazioni, consulta Monitoraggio delle variazioni della capacità di throughput.

Monitoraggio delle variazioni della capacità di throughput

Puoi monitorare lo stato di avanzamento di una modifica della capacità di throughput utilizzando la console Amazon FSx, l'API e il. AWS CLI

Monitoraggio delle variazioni della capacità di throughput nella console

Nella scheda Aggiornamenti della finestra 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

I tipi supportati sono la capacità di throughput, la capacità di archiviazione e l'ottimizzazione dello storage.

Target value (Valore target)

Il valore desiderato su cui modificare la capacità di throughput del file system.

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.
- Completato: l'aggiornamento della capacità di throughput è stato completato correttamente.
- 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 delle modifiche con l'API AWS CLI and

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 una capacità di trasmissione di 128 MB/s e una capacità di trasmissione di destinazione di 256 MB/s.

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

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 `ThroughputCapacity` proprietà. Ciò è illustrato nel seguente estratto di risposta di un comando CLIdescribe-file-systems.

```
.
.
```

```
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Se la modifica della capacità di throughput non riesce, lo stato cambia e la `FailureDetails` proprietà fornisce informazioni sull'errore. `FAILED`

Ottimizzazione delle prestazioni con le finestre di manutenzione di Amazon FSx

Essendo un servizio completamente gestito, FSx for ONTAP esegue regolarmente la manutenzione e gli aggiornamenti del file system. Questa manutenzione non ha alcun impatto sulla maggior parte dei carichi di lavoro. Per i carichi di lavoro sensibili alle prestazioni, in rare occasioni potresti notare un breve impatto (<60 secondi) sulle prestazioni durante la manutenzione; Amazon FSx ti consente di utilizzare la finestra di manutenzione per controllare quando si verifica una potenziale attività di manutenzione di questo tipo.

L'applicazione delle patch avviene raramente, in genere una volta ogni diverse settimane. Per i file system con scalabilità verticale, l'applicazione delle patch richiede in genere solo 30 minuti dall'inizio della finestra di manutenzione. Per i file system con scalabilità orizzontale, l'applicazione delle patch richiede fino a 90 minuti dall'inizio della finestra di manutenzione. Durante questi pochi minuti, i file system eseguono automaticamente il failover e il failback. È possibile scegliere la finestra di manutenzione durante la creazione del file system. Se non si ha alcuna preferenza oraria, viene assegnata un'ora di inizio di 30 minuti.

FSx for ONTAP consente di regolare la finestra di manutenzione secondo necessità per soddisfare il carico di lavoro e i requisiti operativi. È possibile spostare la finestra di manutenzione con la frequenza richiesta, a condizione che una finestra di manutenzione si verifichi almeno una volta

ogni 14 giorni. Se viene rilasciata una patch e non si verifica una finestra di manutenzione entro 14 giorni, FSx for ONTAP procederà alla manutenzione del file system per garantirne la sicurezza e l'affidabilità.

> **Note**
>
> Per garantire l'integrità dei dati durante le attività di manutenzione, FSx for ONTAP chiude tutti i blocchi opportunistici e completa tutte le operazioni di scrittura in sospeso sui volumi di storage sottostanti che ospitano il file system prima dell'inizio della manutenzione.

Puoi utilizzare la console di gestione Amazon FSx AWS CLI, l' AWS API o uno degli AWS SDK per modificare la finestra di manutenzione per i tuoi file system.

Per modificare la finestra di manutenzione settimanale (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli File system nella colonna di navigazione a sinistra.
3. Scegli il file system per cui desideri modificare la finestra di manutenzione settimanale. Viene visualizzata la pagina di riepilogo dei dettagli del file system.
4. Scegliete Amministrazione per visualizzare il pannello Impostazioni di amministrazione del file system.
5. Scegli Aggiorna per visualizzare la finestra Modifica manutenzione.
6. Inserisci il nuovo giorno e l'ora in cui desideri che inizi la finestra di manutenzione settimanale.
7. Scegliere Salva per salvare le modifiche. La nuova ora di inizio della manutenzione viene visualizzata nel pannello Impostazioni di amministrazione del file system.

Per modificare la finestra di manutenzione settimanale utilizzando il comando update-file-systemCLI, vedere. Per aggiornare un file system (CLI)

Tagging delle risorse Amazon FSx.

Per semplificare la gestione delle risorse Amazon FSx, è possibile assegnare metadati personalizzati a ciascuna risorsa sotto forma di tag. Con i tag puoi categorizzare le AWS risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Questa categorizzazione è 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 assegni a una AWS risorsa. Ogni tag è composto da due parti che definisci:

- Una chiave del tag (ad esempio, `CostCenter`, `Environment` o `Project`). Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.
- Un valore di tag (ad esempio, `111122223333` oppure `Production`). Analogamente alle chiavi dei tag, i valori dei tag prevedono una distinzione tra lettere maiuscole e minuscole. I valori dei tag sono opzionali.

Puoi usare i tag per categorizzare AWS le 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 del tuo account e monitorare così ogni proprietario dell'istanza e il livello dello stack.

Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Tramite un set di chiavi di tag coerente la gestione delle risorse risulta notevolmente semplificata. Puoi cercare e filtrare le risorse in base ai tag che aggiungi. Per ulteriori informazioni su come implementare una strategia efficace di applicazione di tag alle risorse, consulta tagging AWS delle risorse nella. Riferimenti generali di AWS

Cose da tenere a mente quando si aggiungono tag:

- I tag non hanno alcun significato semantico per Amazon FSx e vengono interpretati rigorosamente come una stringa di caratteri.

- 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, il AWS Command Line Interface (AWS CLI) o un AWS SDK, puoi fare quanto segue:
  - Puoi utilizzare l'operazione `TagResource` API per applicare tag a risorse esistenti.
  - Per alcune operazioni per la creazione di risorse, puoi specificare tag per una risorsa durante la sua creazione. Il tagging delle risorse in fase di creazione ti permette di evitare di eseguire script di tagging personalizzati dopo la creazione delle risorse.

    Se i tag non possono essere applicati durante la creazione della risorsa, Amazon FSx esegue il rollback del processo di creazione della risorsa. Questo comportamento aiuta a garantire che le risorse vengano create con i tag oppure che non vengano create affatto, nonché che nessuna risorsa sia mai sprovvista di tag.

    > **Note**
    >
    > Alcune autorizzazioni AWS Identity and Access Management (IAM) sono necessarie agli utenti affinché possano aggiungere tag alle risorse durante la creazione. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

Tagging delle risorse

Puoi assegnare tag alle risorse Amazon FSx esistenti nel tuo account. Se utilizzi la console Amazon FSx, puoi applicare tag alle risorse utilizzando la scheda Tag nella schermata della risorsa interessata. Quando crei risorse, puoi applicare la chiave Nome con un valore e puoi applicare i tag di tua scelta quando crei un nuovo file system. Tuttavia, anche se la console organizza le risorse in base alla chiave Name, questa chiave non ha un significato semantico per il servizio Amazon FSx.

Per implementare un controllo granulare sugli utenti e sui gruppi che associano tag alle risorse durante la creazione, puoi applicare autorizzazioni basate su tag a livello di risorsa nelle policy IAM

alle operazioni dell'API Amazon FSx che supportano il tagging in fase di creazione. Utilizzando tali autorizzazioni nelle policy, ottieni i seguenti vantaggi:

- Le risorse vengono adeguatamente protette a partire dal momento della creazione.
- Poiché i tag vengono applicati subito alle risorse, 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.

Per controllare quali chiavi e valori di tag sono impostati sulle risorse esistenti, puoi applicare autorizzazioni a livello di risorsa alle operazioni `TagResource` e dell'API `UntagResource` Amazon FSx nelle policy IAM.

Per ulteriori informazioni sulle autorizzazioni necessarie per taggare le risorse Amazon FSx durante la 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 risorse Amazon FSx nelle policy IAM, consultaUtilizzo dei tag per controllare l'accesso alle risorse Amazon FSx.

Per informazioni sul tagging delle risorse per la fatturazione, consulta Utilizzo di tag per l'allocazione dei costi nella Guida per l'AWS Billingutente di.

Copia di tag nei backup

Quando crei o aggiorni un volume nell'API Amazon FSx oppureAWS CLI, puoi `CopyTagsToBackups` abilitare la copia automatica di qualsiasi tag dai tuoi volumi ai backup.

> **Note**
>
> Se specifichi i tag durante la creazione di un backup avviato dall'utente (incluso il tag con il nome quando crei un backup utilizzando la console Amazon FSx), i tag non vengono copiati dal volume anche se li hai abilitati. `CopyTagsToBackups`

Per ulteriori informazioni sui backup, consultare Utilizzo dei backup. Per ulteriori informazioni sull'attivazione`CopyTagsToBackups`, consulta Per creare un volume (CLI) la Guida per l'utente

di Amazon FSx for NetApp ONTAP o CreateVolumela Guida di riferimento dell'UpdateVolumeAPI Amazon FSx for NetApp ONTAP. Per aggiornare la configurazione di un volume (CLI)

Limitazioni applicate ai tag

Ai tag si applicano le seguenti limitazioni di base:

- Il numero massimo di tag per risorsa è 50.
- La lunghezza massima delle chiavi è 128 caratteri Unicode in UTF-8.
- Il valore massimo è 256 caratteri Unicode in UTF-8.
- I caratteri consentiti sono lettere, numeri e spazi rappresentabili in formato UTF-8, oltre ai seguenti caratteri: `+ - ` (trattino) (trattino basso). `= . _ : / @`
- Per ciascuna risorsa, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.
- i valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole;
- Il prefisso `aws:` è riservato per l'uso di 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 puoi eliminare una risorsa solo sulla base dei relativi tag. Devi specificare il relativo identificatore. Ad esempio, per eliminare un file system associato a una chiave di tag denominata`DeleteMe`, devi utilizzare l'`DeleteFileSystem`operazione con l'identificatore della risorsa del file system, ad esempio`fs-1234567890abcdef0`.

Quando si aggiungono tag a risorse pubbliche o condivise, i tag assegnati sono disponibili solo per le Account AWS risorse che assegni. Account AWS Per il controllo degli accessi 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 taggare le risorse Amazon FSx durante la 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 risorse Amazon FSx nelle policy IAM, consultaUtilizzo dei tag per controllare l'accesso alle risorse Amazon FSx.

Gestione delle risorse FSx for ONTAP tramite applicazioni NetApp

Oltre alle AWS API e agli SDK AWS Management Console AWS CLI, è possibile utilizzare anche questi strumenti e applicazioni di NetApp gestione per gestire le risorse FSx for ONTAP:

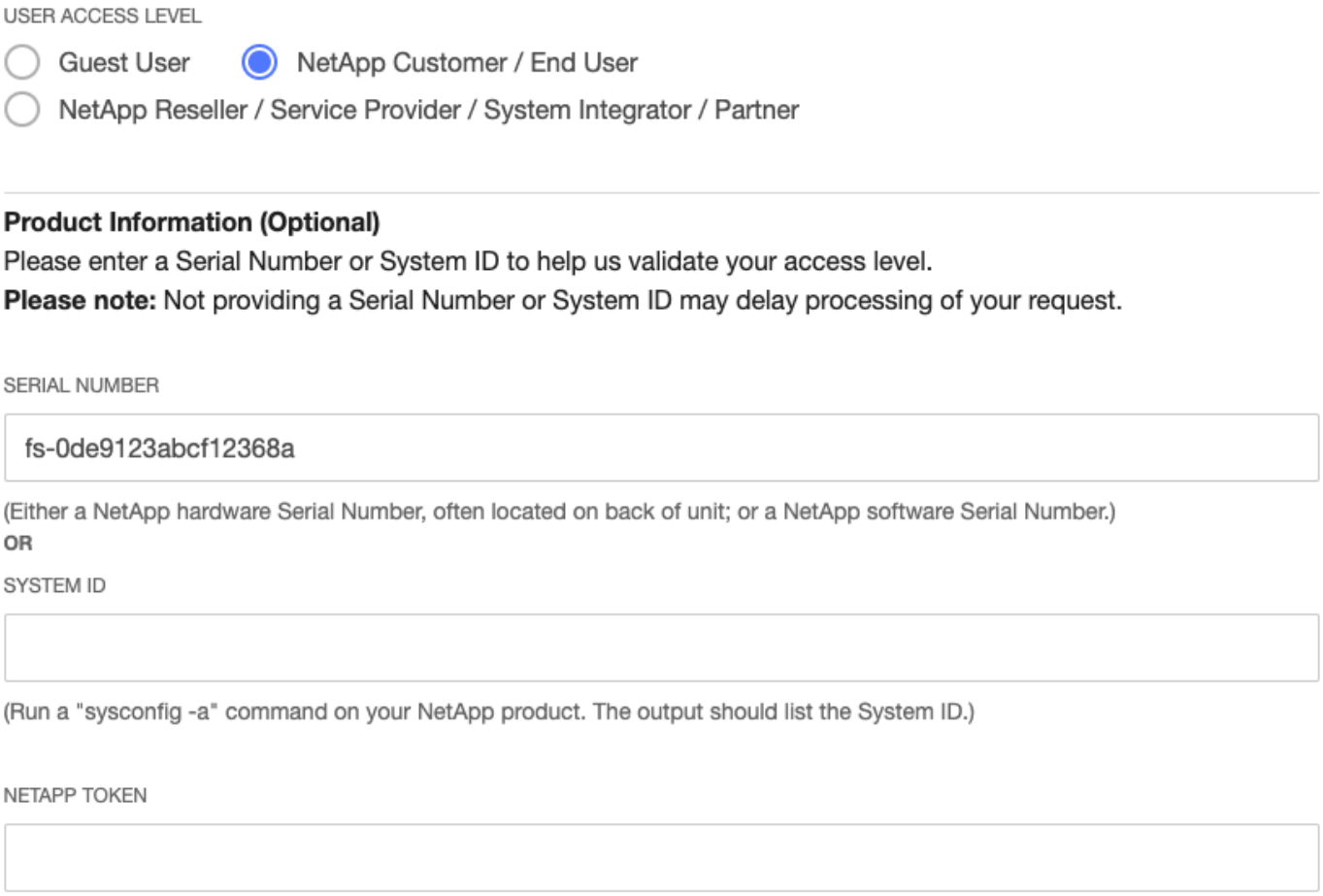
Argomenti

> **Important**
>
> Amazon FSx si sincronizza periodicamente con ONTAP per garantire la coerenza. Se crei o modifichi volumi utilizzando NetApp applicazioni, potrebbero essere necessari alcuni minuti prima che queste modifiche si riflettano nell'API AWS Management Console AWS CLI, e negli SDK.

Registrazione di un account NetApp

Per scaricare alcuni NetApp software, ad esempio BlueXPSnapCenter, e il connettore ONTAP Antivirus, è necessario disporre di un NetApp account. Per creare un NetApp account, procedi nel seguente modo:

1. Vai alla pagina di registrazione NetApp utente e registrati per creare un nuovo account NetApp utente.
2. Completa il modulo o i moduli con le tue informazioni. Assicurati di selezionare il livello di accesso NetAppCliente/Utente finale. Nel campo NUMERO DI SERIE, copia e incolla l'ID del file system per il file system FSx for ONTAP. Fai riferimento al file di esempio seguente:



Cosa aspettarsi dopo la registrazione

I clienti con NetApp prodotti esistenti avranno il livello di accesso al livello di cliente dal loro account NSS entro un giorno lavorativo. L'onboarding dei nuovi clienti NetApp verrà effettuato utilizzando le procedure commerciali standard, oltre ad avere il loro account NSS aggiornato al livello di accesso Customer Level. Fornire l'ID del file system aiuta ad accelerare questo processo. Puoi controllare lo stato del tuo account NSS accedendo a mysupport.netapp.com e accedendo alla pagina di benvenuto. Il livello di accesso del tuo account deve essere Accesso clienti.

Uso di NetApp BlueXP

NetApp BlueXP è un piano di controllo unificato che semplifica le esperienze di gestione dei servizi di archiviazione e dati in ambienti locali e cloud. BlueXP fornisce un'interfaccia utente centralizzata per gestire, monitorare e automatizzare le implementazioni ONTAP in sede e in sede. AWS Per ulteriori

informazioni, consulta la documentazione di NetApp BlueXP e la documentazione di NetApp BlueXP for Amazon FSX for ONTAP. NetApp

> **Note**
>
> NetApp BlueXPnon è supportato per i file system con scalabilità orizzontale.

Utilizzo di NetApp System Manager con BlueXP

Puoi gestire i tuoi file system Amazon FSx for NetApp ONTAP utilizzando System Manager direttamente da. BlueXP BlueXPti consente di utilizzare la stessa interfaccia di System Manager a cui sei abituato, in modo da poter gestire la tua infrastruttura ibrida multi-cloud da un unico piano di controllo. Hai anche accesso alle altre funzionalità di BlueXP. Per ulteriori informazioni, consultate l'argomento Integrazione di System Manager con BlueXP nella documentazione ONTAP. NetApp

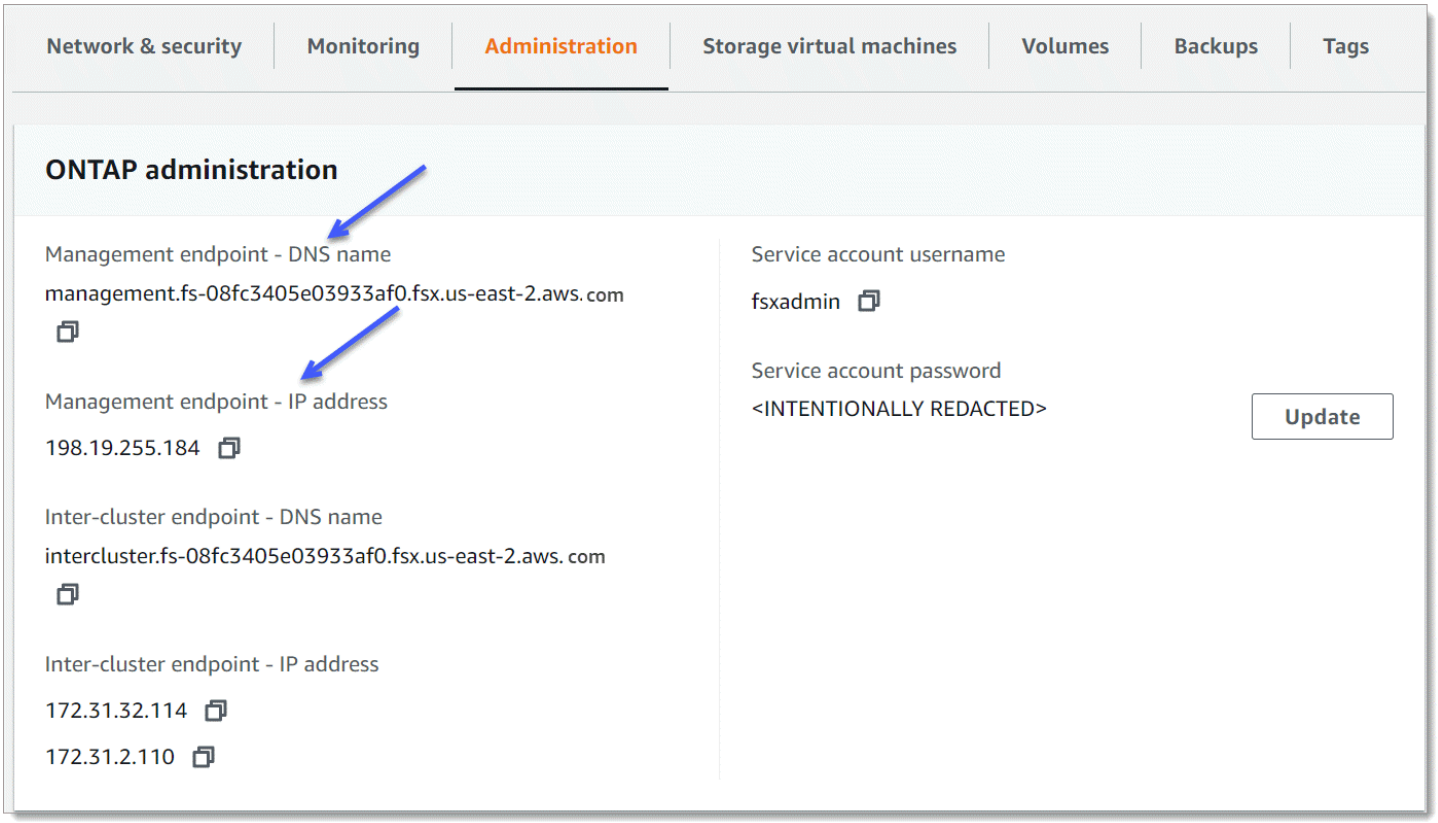
> **Note**
>
> NetApp System Manager non è supportato per i file system con scalabilità orizzontale.

Utilizzo della CLI NetApp ONTAP

Puoi gestire le tue risorse Amazon FSx for NetApp ONTAP utilizzando la CLI. NetApp ONTAP Puoi gestire le risorse a livello di file system (analogo al cluster NetApp ONTAP) e a livello SVM.

Gestione dei file system con la ONTAP CLI

È possibile eseguire comandi ONTAP CLI sul file system FSx for ONTAP, analogamente all'esecuzione su un cluster. NetApp ONTAP Puoi accedere alla ONTAP CLI sul tuo file system stabilendo una connessione Secure Shell (SSH) all'endpoint di gestione del file system, accedendo con nome utente e password. `fsxadmin` È possibile impostare la password quando si crea il file system utilizzando il flusso di creazione personalizzato o utilizzando il. AWS CLI Se hai creato il file system utilizzando l'opzione Creazione rapida, la `fsxadmin` password non è stata impostata, quindi dovrai impostarne una per accedere alla CLI di ONTAP. Per ulteriori informazioni, consulta Aggiornamento di un file system. Puoi trovare il nome DNS e l'indirizzo IP dell'endpoint di gestione del tuo file system nella console Amazon FSx, nella scheda Amministrazione della pagina dei dettagli del file system FSx for ONTAP, mostrata nel grafico seguente.



Per connetterti all'endpoint di gestione del file system con SSH, usa l'utente e la password. `fsxadmin` È possibile accedere tramite SSH all'indirizzo IP o al nome DNS dell'endpoint di gestione del file system da un client che si trova nello stesso VPC del file system, come negli esempi seguenti.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

Il comando SSH con valori di esempio:

```
ssh fsxadmin@198.51.100.0
```

Il comando SSH che utilizza il nome DNS dell'endpoint di gestione:

```
ssh fsxadmin@file-system-management-endpoint-dns-name
```

Il comando SSH che utilizza un nome DNS di esempio:

```
$ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin-password

This is your first recorded login.
```

```
FsxId0abcdef123456789::>
```

Ambito di comandi ONTAP CLI disponibili per **`fsxadmin`**

La visualizzazione amministrativa `fsxadmin` è a livello di file system, che include tutte le SVM e i volumi del file system. Il `fsxadmin` ruolo svolge il ruolo di amministratore del ONTAP cluster. Poiché i file system Amazon FSx for NetApp ONTAP sono completamente gestiti, il `fsxadmin` ruolo può eseguire un sottoinsieme dei comandi CLI disponibili. ONTAP

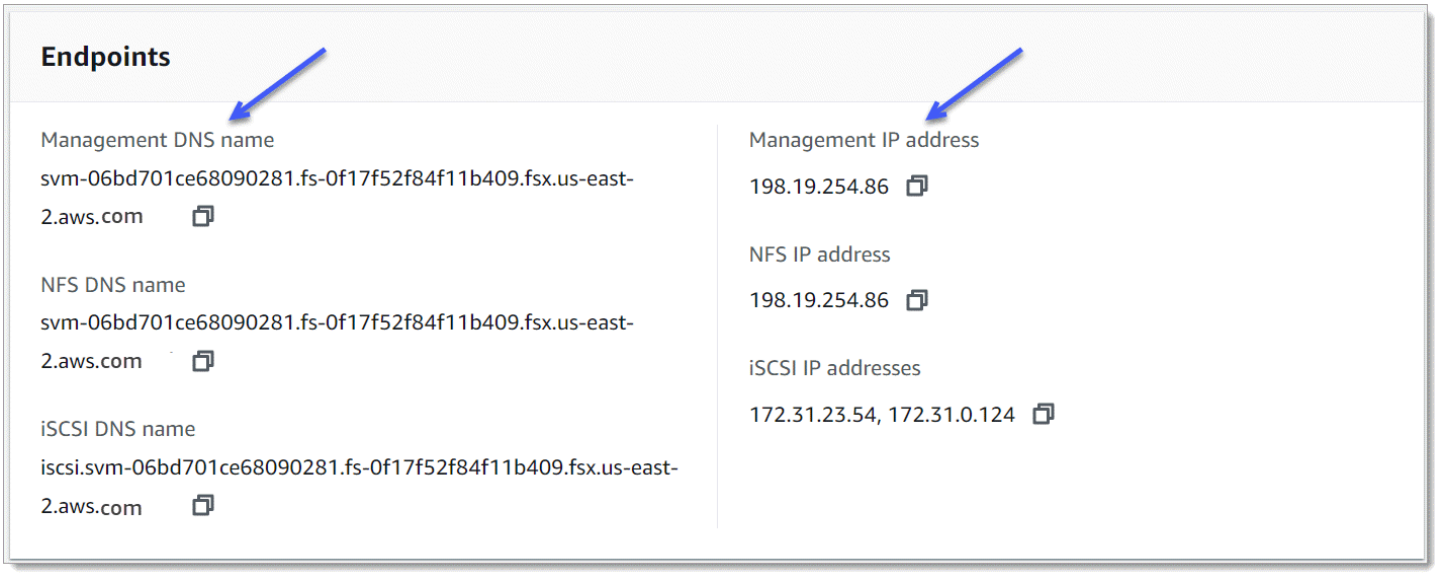
Per visualizzare un elenco dei comandi che `fsxadmin` possono essere eseguiti, utilizza il seguente comando `security login role show`ONTAPCLI:

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
           Role          Command/                                    Access
Vserver    Name          Directory                             Query Level
---------- ------------- --------- ----------------------------------- --------
FsxId0abcdef123456789
           fsxadmin      application                                   all
                         cluster application-record                    all
                         cluster date show                             readonly
                         cluster ha modify                             readonly
                         cluster ha show                               readonly
                         cluster identity modify                       readonly
                         cluster identity show                         readonly
                         cluster log-forwarding           -port !55555 all
                         cluster modify                                readonly
                         cluster peer                                  all
                         cluster show                                  readonly
                         cluster statistics show                       readonly
                         cluster time-service ntp server create        readonly
                         cluster time-service ntp server delete        readonly
                         cluster time-service ntp server modify        readonly
                         cluster time-service ntp server show          readonly
                         debug network tcpdump       -ipspace !Cluster all
                         debug san lun                                 all
                         df         -vserver !FsxId* -vserver !Cluster readonly
                         echo                                          all
                         event catalog show                            readonly
                         event config                                  all
.
.
.
```

```
363 entries were displayed.
```

Gestione delle SVM con la CLI ONTAP

È possibile accedere alla ONTAP CLI sulla SVM stabilendo una connessione Secure Shell (SSH) all'endpoint di gestione dell'SVM utilizzando `fsxadmin` o il nome utente e la password. `vsadmin` Puoi trovare il nome DNS e l'indirizzo IP dell'endpoint di gestione SVM nella console Amazon FSx, nel pannello Endpoints della pagina dei dettagli delle macchine virtuali di storage, mostrata nel grafico seguente.



Per connetterti all'endpoint di gestione dell'SVM con SSH, puoi utilizzare il nome utente e la password. `vsadmin` `fsxadmin` Se non avete impostato una password per l'`vsadmin`utente al momento della creazione dell'SVM, potete impostarla in qualsiasi momento. `vsadmin` Per ulteriori informazioni, consulta Aggiornamento di una macchina virtuale di storage. È possibile accedere alla SVM tramite SSH da un client che si trova nello stesso VPC del file system, utilizzando l'indirizzo IP o il nome DNS dell'endpoint di gestione.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

Il comando con valori di esempio:

```
ssh vsadmin@198.51.100.10
```

Il comando SSH che utilizza il nome DNS dell'endpoint di gestione:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

Il comando SSH che utilizza un nome DNS di esempio:

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Amazon FSx for NetApp ONTAP supporta i comandi NetApp ONTAP CLI.

Per un riferimento completo dei comandi NetApp ONTAP CLI, consulta la sezione Comandi ONTAP: manuale di riferimento alla pagina.

Utilizzo dell'API REST di ONTAP

Quando accedete al file system FSx for ONTAP utilizzando l'API ONTAP REST utilizzando le `fsxadmin` credenziali, effettuate una delle seguenti operazioni:

- Disabilita la convalida TLS.

  Or
- Considera attendibili le autorità di AWS certificazione (CA): il pacchetto di certificati per le CA di ciascuna regione è disponibile ai seguenti URL:
  - https://fsx-aws-certificates.s3.amazonaws.com/bundle - *`aws-region .pem`* per pubblico Regioni AWS
  - https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle - *`aws-region .pem`* per le regioni AWS GovCloud
  - https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle - *`aws-region .pem`* per le regioni cinesi AWS

Per un riferimento completo dei comandi dell'API NetApp ONTAP REST, consulta il riferimento online all'API NetApp ONTAPREST.

Sicurezza in Amazon FSx per ONTAP NetApp

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 aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per informazioni sui programmi di conformità applicabili ad Amazon FSx for NetApp ONTAP, consulta AWS Services in Scope by Compliance Program 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 ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon FSx. I seguenti argomenti mostrano come configurare Amazon FSx per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon FSx.

Argomenti

- Ruoli e utenti in Amazon FSx for ONTAP NetApp

Protezione dei dati in Amazon FSx for ONTAP NetApp

Il modello di responsabilità AWS condivisa Modello si applica alla protezione dei dati in Amazon FSx for NetApp ONTAP. 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
- 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 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente 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, l'API o AWS gli AWS CLI SDK. 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.

Crittografia dei dati in FSx for ONTAP

Amazon FSx for NetApp ONTAP supporta la crittografia dei dati inattivi e la crittografia dei dati in transito. La crittografia dei dati inattivi viene abilitata automaticamente durante la creazione di un file system Amazon FSx. Amazon FSx for NetApp ONTAP supporta la crittografia basata su Kerberos in transito sui protocolli NFS e SMB se accedi ai dati in una Storage Virtual Machine (SVM) unita a un Active Directory o a un dominio utilizzando il Lightweight Directory Access Protocol (LDAP).

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, i dati vengono automaticamente crittografati quando sono inattivi. Si consiglia inoltre di abilitare la crittografia dei dati in transito installando il file system utilizzando la crittografia dei dati in transito.

Per ulteriori informazioni sulla crittografia dei dati con Amazon FSx for NetApp ONTAP, consulta e. Crittografia dei dati a riposo Crittografia dei dati in transito

Crittografia dei dati a riposo

Tutti i file system Amazon FSx for NetApp ONTAP sono crittografati quando sono inattivi con chiavi gestite tramite AWS Key Management Service ().AWS KMS I dati vengono crittografati automaticamente prima di essere scritti nel file system e decrittografati automaticamente durante la lettura. Questi processi sono gestiti in modo trasparente da Amazon FSx, quindi non è necessario modificare le applicazioni.

Amazon FSx utilizza un algoritmo di crittografia AES-256 standard di settore per crittografare dati e metadati Amazon FSx a riposo. Per ulteriori informazioni, consulta Elementi di base di crittografia nella Guida per sviluppatori di AWS Key Management Service .

> **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.

Come utilizza Amazon FSx AWS KMS

Amazon FSx si integra con AWS KMS per la gestione delle chiavi. Amazon FSx utilizza le chiavi KMS per crittografare il file system. Scegli la chiave KMS utilizzata per crittografare e decrittografare i file system (dati e metadati). Puoi abilitare, disabilitare o revocare le concessioni su questa chiave KMS. Questa chiave KMS può essere di uno dei due tipi seguenti:

- AWS-chiave KMS gestita: questa è la chiave KMS predefinita ed è gratuita.
- Chiave KMS gestita dal cliente: questa è la chiave KMS più flessibile da utilizzare, poiché è possibile configurarne le politiche e le concessioni principali per più utenti o servizi. Per ulteriori informazioni sulla creazione di chiavi KMS, consulta Creating Keys nella Developer Guide. AWS Key Management Service

> **Important**
>
> Amazon FSx accetta solo chiavi KMS con crittografia simmetrica. Non puoi usare chiavi KMS asimmetriche con Amazon FSx.

Se utilizzi una chiave KMS gestita dal cliente come chiave KMS per la crittografia e la decrittografia dei dati dei file, puoi abilitare la rotazione delle chiavi. Quando si abilita la rotazione delle chiavi, AWS KMS fa ruotare automaticamente la chiave una volta all'anno. Inoltre, con una chiave KMS gestita dal cliente, puoi scegliere quando disabilitare, riattivare, eliminare o revocare l'accesso alla tua chiave KMS in qualsiasi momento. Per ulteriori informazioni, consulta Rotazione AWS KMS keys e attivazione e disattivazione delle chiavi nella Guida per gli sviluppatori.AWS Key Management Service

Politiche chiave di Amazon FSx 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 testo semplice che è stato precedentemente crittografato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

- kms: ReEncrypt — (Facoltativo) Crittografa i dati sul lato server con uno nuovo AWS KMS key, 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: GenerateData KeyWithout Plaintext — (Obbligatorio) Restituisce una chiave di crittografia dei dati crittografata con una chiave KMS. Questa autorizzazione è inclusa nella politica delle chiavi predefinita in kms: Key*. GenerateData
- 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 autorizzazioni, consulta Utilizzo delle autorizzazioni nella Guida per gli sviluppatori di 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 delle chiavi 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

Questo argomento spiega le diverse opzioni disponibili per crittografare i dati dei file mentre sono in transito tra un file system FSx for ONTAP e i client connessi. Fornisce inoltre indicazioni per aiutarvi a scegliere il metodo di crittografia più adatto al vostro flusso di lavoro.

Tutti i dati che fluiscono attraverso la Regioni AWS rete AWS globale vengono automaticamente crittografati a livello fisico prima di lasciare le strutture AWS protette. Tutto il traffico tra le zone di disponibilità è crittografato. I livelli di crittografia aggiuntivi, inclusi quelli elencati in questa sezione, forniscono protezioni aggiuntive. Per ulteriori informazioni su come AWS fornisce protezione per il flusso di dati tra Regioni AWS zone disponibili e istanze, consulta Encryption in transit nella Amazon Elastic Compute Cloud User Guide for Linux Instances.

Amazon FSx for NetApp ONTAP supporta i seguenti metodi per crittografare i dati in transito tra i file system FSx for ONTAP e i client connessi:

- Crittografia automatica basata su Nitro su tutti i protocolli e client supportati in esecuzione su tipi di istanze Amazon EC2 Linux e Windows supportati.
- Crittografia basata su Kerberos su protocolli NFS e SMB.

- Crittografia basata su IPSec su protocolli NFS, iSCSI e SMB

Tutti i metodi supportati per la crittografia dei dati in transito utilizzano algoritmi crittografici AES-256 standard del settore che forniscono una crittografia avanzata di livello aziendale.

Argomenti

Scelta di un metodo per crittografare i dati in transito

Questa sezione fornisce informazioni che possono aiutarti a decidere quale dei metodi di crittografia supportati nei metodi di transito è più adatto al tuo flusso di lavoro. Fai riferimento a questa sezione per esplorare le opzioni supportate descritte in dettaglio nelle sezioni che seguono.

Esistono diversi fattori da considerare nella scelta del modo in cui crittografare i dati in transito tra il file system FSx for ONTAP e i client connessi. Questi fattori includono:

- Il Regione AWS file system FSx for ONTAP su cui è in esecuzione.
- Il tipo di istanza su cui è in esecuzione il client.
- La posizione del client che accede al file system.
- Requisiti prestazionali della rete.
- Il protocollo di dati che desideri crittografare.
- Se si utilizza Microsoft Active Directory.

Regione AWS

Il sistema in Regione AWS cui è in esecuzione il file system determina se è possibile utilizzare o meno la crittografia basata su Amazon Nitro. La crittografia basata su Nitro è disponibile nelle seguenti versioni: Regioni AWS

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- US West (Oregon)
- Europa (Irlanda)

Inoltre, la crittografia basata su Nitro è disponibile per i file system con scalabilità orizzontale nella regione Asia-Pacifico (Sydney). Regione AWS

Tipo di istanza del client

Puoi utilizzare la crittografia basata su Amazon Nitro se il client che accede al tuo file system è in esecuzione su uno dei tipi di istanza Amazon EC2 per Mac, Linux o Windows supportati e il tuo flusso di lavoro soddisfa tutti gli altri requisiti per l'utilizzo della crittografia basata su Nitro. Non esistono requisiti relativi al tipo di istanza client per l'utilizzo della crittografia Kerberos o IPSec.

Client location (Posizione del client)

La posizione del client che accede ai dati rispetto alla posizione del file system influisce sui metodi di crittografia in transito disponibili per l'uso. Puoi utilizzare uno qualsiasi dei metodi di crittografia supportati se il client e il file system si trovano nello stesso VPC. Lo stesso vale se il client e il file system si trovano in VPC peer, purché il traffico non passi attraverso un dispositivo o un servizio di rete virtuale, come un gateway di transito. La crittografia basata su Nitro non è un'opzione disponibile se il client non si trova nello stesso VPC o in un VPC peerizzato o se il traffico passa attraverso un dispositivo o un servizio di rete virtuale.

Prestazioni di rete

L'uso della crittografia basata su Amazon Nitro non ha alcun impatto sulle prestazioni di rete. Questo perché le istanze Amazon EC2 supportate utilizzano le funzionalità di offload dell'hardware Nitro System sottostante per crittografare automaticamente il traffico in transito tra le istanze.

L'utilizzo della crittografia Kerberos o IPSec ha un impatto sulle prestazioni della rete. Questo perché entrambi questi metodi di crittografia sono basati su software, il che richiede al client e al server di utilizzare risorse di elaborazione per crittografare e decrittografare il traffico in transito.

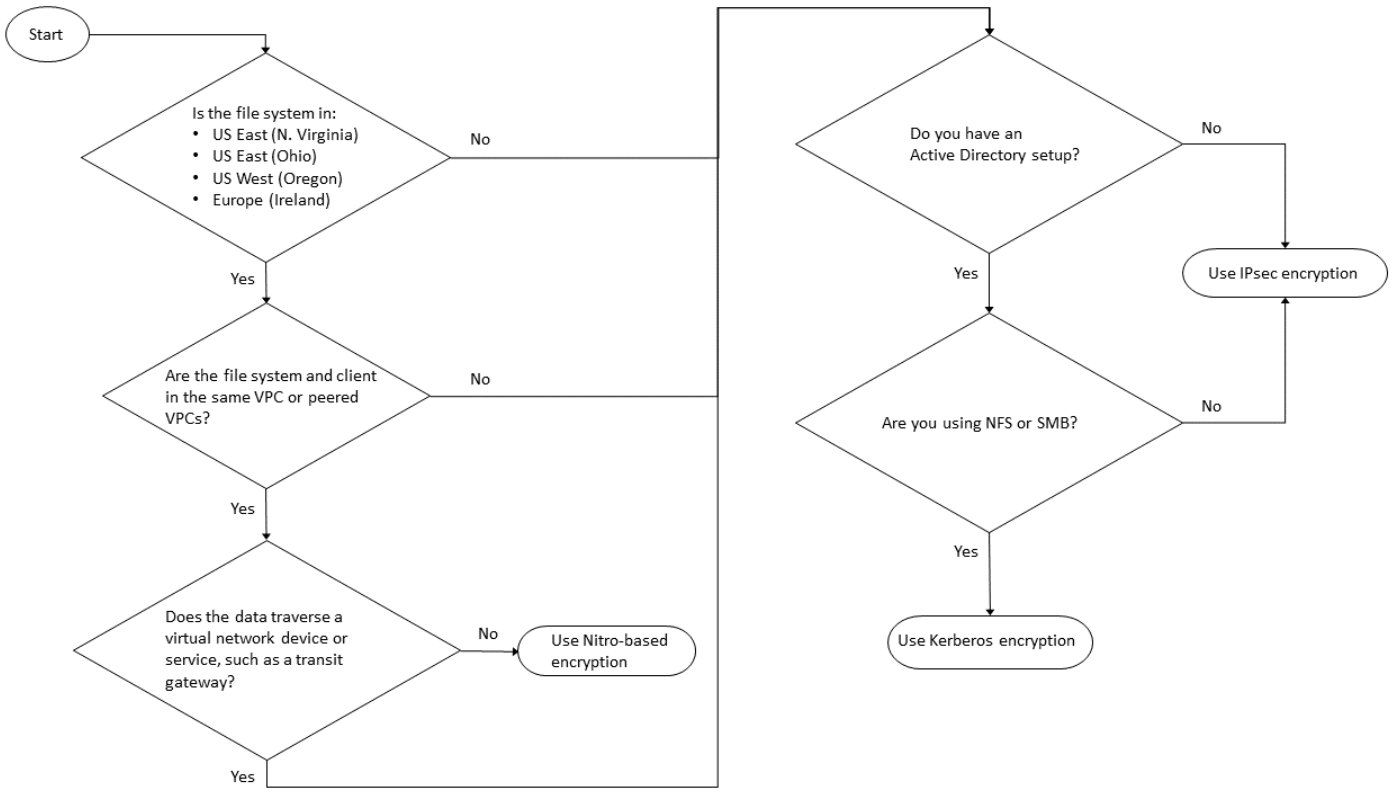
Protocollo dati

Puoi utilizzare la crittografia basata su Amazon Nitro e la crittografia IPSec con tutti i protocolli supportati: NFS, SMB e iSCSI. Puoi utilizzare la crittografia Kerberos con i protocolli NFS e SMB (con Active Directory).

Active Directory

Se si utilizza Microsoft Active Directory, è possibile utilizzare la crittografia Kerberos sui protocolli NFS e SMB.

Utilizzate il seguente diagramma per decidere quale metodo di crittografia in transito utilizzare.



La crittografia IPSec è l'unica opzione disponibile quando tutte le seguenti condizioni si applicano al flusso di lavoro:

- Stai utilizzando il protocollo NFS, SMB o iSCSI.
- Il tuo flusso di lavoro non supporta l'uso della crittografia basata su Amazon Nitro.
- Non stai utilizzando un dominio Microsoft Active Directory.

Crittografia dei dati in transito con AWS Nitro System

Con la crittografia basata su Nitro, i dati in transito vengono crittografati automaticamente quando i client che accedono ai tuoi file system sono in esecuzione su tipi di istanze Linux o Windows supportati di Amazon EC2.

L'uso della crittografia basata su Amazon Nitro non ha alcun impatto sulle prestazioni di rete. Questo perché le istanze Amazon EC2 supportate utilizzano le funzionalità di offload dell'hardware Nitro System sottostante per crittografare automaticamente il traffico in transito tra le istanze.

La crittografia basata su Nitro viene abilitata automaticamente quando i tipi di istanze client supportati si trovano nello stesso Regione AWS e nello stesso VPC o in un VPC peerizzato con il VPC del file system. Inoltre, se il client si trova in un VPC con peering, i dati non possono attraversare un dispositivo o un servizio di rete virtuale (come un gateway di transito) per abilitare automaticamente la crittografia basata su Nitro. Per ulteriori informazioni sulla crittografia basata su Nitro, consulta la sezione Encryption in transit della Amazon EC2 User Guide per i tipi di istanze Linux o Windows.

La crittografia in transito basata su Nitro è disponibile per i file system creati dopo il 28 novembre 2022 nei seguenti paesi: Regioni AWS

- Stati Uniti orientali (Virginia settentrionale)
- Stati Uniti orientali (Ohio)
- US West (Oregon)
- Europa (Irlanda)

Inoltre, la crittografia basata su Nitro è disponibile per i file system a scalabilità orizzontale nell'Asia Pacifico (Sydney). Regione AWS

Per ulteriori informazioni sui paesi Regioni AWS in cui è disponibile FSx for ONTAP, consulta i prezzi di Amazon FSx for ONTAP. NetApp

Per ulteriori informazioni sulle specifiche prestazionali per i file system FSx for ONTAP, vedere. Impatto della capacità di throughput sulle prestazioni

Crittografia dei dati in transito con la crittografia basata su Kerberos

Se si utilizza Microsoft Active Directory, è possibile utilizzare la crittografia basata su Kerberos sui protocolli NFS e SMB per crittografare i dati in transito per i volumi figlio di SVM uniti a Microsoft Active Directory.

Crittografia dei dati in transito su NFS utilizzando Kerberos

La crittografia dei dati in transito tramite Kerberos è supportata per i protocolli NFSv3 e NFSv4. Per abilitare la crittografia in transito utilizzando Kerberos per il protocollo NFS, vedi Uso di Kerberos con NFS per una sicurezza avanzata nel Documentation Center. NetApp ONTAP

Crittografia dei dati in transito su SMB utilizzando Kerberos

La crittografia dei dati in transito tramite il protocollo SMB è supportata sulle condivisioni di file mappate su un'istanza di calcolo che supporta il protocollo SMB 3.0 o versione successiva. Sono incluse tutte Microsoft Windows le versioni di Microsoft Windows Server 2012 e versioni successive e Microsoft Windows 8 e versioni successive. Se abilitato, FSx for ONTAP crittografa automaticamente i dati in transito utilizzando la crittografia SMB quando si accede al file system senza la necessità di modificare le applicazioni.

FSx for ONTAP SMB supporta la crittografia a 128 e 256 bit, determinata dalla richiesta di sessione del client. Per le descrizioni dei diversi livelli di crittografia, consulta la sezione Impostazione del livello minimo di sicurezza di autenticazione del server SMB di Gestire SMB con la CLI nel Documentation Center. NetApp ONTAP

> **Note**
>
> Il client determina l'algoritmo di crittografia. Sia l'autenticazione NTLM che quella Kerberos funzionano con la crittografia a 128 e 256 bit. Il server SMB FSx for ONTAP accetta tutte le richieste standard dei client Windows e i controlli granulari sono gestiti dalle impostazioni dei criteri di gruppo o del registro di Microsoft.

Utilizzi la ONTAP CLI per gestire la crittografia nelle impostazioni di transito su SVM e volumi FSx for ONTAP. Per accedere alla NetApp ONTAP CLI, stabilite una sessione SSH sulla SVM su cui state effettuando la crittografia nelle impostazioni di transito, come descritto in. Gestione delle SVM con la CLI ONTAP

Per istruzioni su come abilitare la crittografia SMB su un SVM o un volume, consulta. Abilita la crittografia SMB dei dati in transito

Crittografia dei dati in transito con crittografia IPSec

FSx for ONTAP supporta l'utilizzo del protocollo IPSec in modalità di trasporto per garantire che i dati siano continuamente sicuri e crittografati durante il transito. IPSec offre end-to-end la crittografia dei dati in transito tra client e file system FSx for ONTAP per tutto il traffico IP supportato: protocolli NFS, iSCSI e SMB. Con la crittografia IPSec, si stabilisce un tunnel IPSec tra un SVM FSx for ONTAP configurato con IPSec abilitato e un client IPSec in esecuzione sul client connesso che accede ai dati.

Si consiglia di utilizzare IPSec per crittografare i dati in transito tramite i protocolli NFS, SMB e iSCSI quando si accede ai dati da client che non supportano la crittografia basata su Nitro e se il client e

le SVM non sono uniti a un Active Directory, necessario per la crittografia basata su Kerberos. La crittografia IPSec è l'unica opzione disponibile per crittografare i dati in transito per il traffico iSCSI quando il client iSCSI non supporta la crittografia basata su Nitro.

Per l'autenticazione IPSec, è possibile utilizzare chiavi precondivise (PSK) o certificati. Se si utilizza un PSK, il client IPSec utilizzato deve supportare Internet Key Exchange versione 2 (IKEv2) con un PSK. I passaggi di alto livello per configurare la crittografia IPSec sia su FSx for ONTAP che sul client sono i seguenti:

1. Abilita e configura IPSec sul tuo file system.
2. Installa e configura IPSec sul tuo client
3. Configura IPSec per l'accesso a più client

Per ulteriori informazioni su come configurare IPSec utilizzando PSK, vedere Configurare la sicurezza IP (IPSec) tramite crittografia via cavo nel centro documentazione. NetApp ONTAP

Per ulteriori informazioni su come configurare IPSec utilizzando i certificati, vedere. Configurazione di IPSec utilizzando l'autenticazione dei certificati

Abilita la crittografia SMB dei dati in transito

Per impostazione predefinita, quando si crea una SVM, la crittografia SMB è disattivata. È possibile abilitare la crittografia SMB richiesta su singole condivisioni o su una SVM, che la attiva per tutte le condivisioni di quella SVM.

> **Note**
>
> Quando la crittografia SMB richiesta è abilitata su una SVM o una condivisione, i client SMB che non supportano la crittografia non possono connettersi a tale SVM o condivisione.

Per richiedere la crittografia SMB per il traffico SMB in entrata su una SVM

Utilizzare la procedura seguente per richiedere la crittografia SMB su una SVM utilizzando la CLINetApp ONTAP.

1. Per connetterti all'endpoint di gestione SVM con SSH, usa il nome utente `vsadmin` e la password vsadmin che hai impostato quando hai creato l'SVM. Se non avete impostato una

password vsadmin, utilizzate il nome utente e la password fsxadmin. `fsxadmin` È possibile accedere alla SVM tramite SSH da un client che si trova nello stesso VPC del file system, utilizzando l'indirizzo IP o il nome DNS dell'endpoint di gestione.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

Il comando con valori di esempio:

```
ssh vsadmin@198.51.100.10
```

Il comando SSH che utilizza il nome DNS dell'endpoint di gestione:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

Il comando SSH che utilizza un nome DNS di esempio:

```
ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-
east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxIdabcdef01234567892::>
```

2. Utilizzate il comando `vserver cifs security modify`NetApp ONTAPCLI per richiedere la crittografia SMB per il traffico SMB in entrata verso SVM.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
```

3. Per interrompere la richiesta della crittografia SMB per il traffico SMB in entrata, utilizzate il seguente comando.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required
 false
```

4. Per vedere l'`is-smb-encryption-required`impostazione corrente su una SVM, usa il comando `vserver cifs security show`NetApp ONTAPCLI:

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required
```

```
vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

Per ulteriori informazioni sulla gestione della crittografia SMB su una SVM, vedere Configurazione della crittografia SMB richiesta sui server SMB per i trasferimenti di dati tramite SMB nel Documentation Center. NetApp ONTAP

Per abilitare la crittografia SMB su un volume

Utilizzare la procedura seguente per abilitare la crittografia SMB su una condivisione utilizzando la NetApp ONTAP CLI.

1. Stabilire una connessione Secure Shell (SSH) all'endpoint di gestione dell'SVM come descritto in. Gestione delle SVM con la CLI ONTAP
2. Utilizza il seguente comando NetApp ONTAP CLI per creare una nuova condivisione SMB e richiedere la crittografia SMB per accedere a questa condivisione.

   ```
   vserver cifs share create -vserver vserver_name -share-name share_name -
   path share_path -share-properties encrypt-data
   ```

   Per ulteriori informazioni, consultate `vserver cifs share create`le pagine man del comando NetApp ONTAP CLI.
3. Per richiedere la crittografia SMB su una condivisione SMB esistente, utilizzare il comando seguente.

   ```
   vserver cifs share properties add -vserver vserver_name -share-name share_name -
   share-properties encrypt-data
   ```

   Per ulteriori informazioni, consultate `vserver cifs share create`le pagine man del comando NetApp ONTAP CLI.
4. Per disattivare la crittografia SMB su una condivisione SMB esistente, utilizzare il comando seguente.

   ```
   vserver cifs share properties remove -vserver vserver_name -share-name share_name -
   share-properties encrypt-data
   ```

Per ulteriori informazioni, consultate `vserver cifs share properties remove`le pagine man del comando NetApp ONTAP CLI.

5. Per visualizzare l'`is-smb-encryption-required`impostazione corrente su una condivisione SMB, usa il seguente comando NetApp ONTAP CLI:

```
vserver cifs share properties show -vserver vserver_name -share-name share_name -
fields share-properties
```

Se una delle proprietà restituite dal comando è la `encrypt-data` proprietà, tale proprietà specifica che è necessario utilizzare la crittografia SMB per accedere a questa condivisione.

Per ulteriori informazioni, consultate `vserver cifs share properties show`le pagine man del comando NetApp ONTAP CLI.

Configurazione di IPSec utilizzando l'autenticazione PSK

Se si utilizza PSK per l'autenticazione, i passaggi per configurare la crittografia IPSec sia su FSx for ONTAP che sul client sono i seguenti:

1. Abilita e configura IPSec sul tuo file system.
2. Installa e configura IPSec sul tuo client
3. Configura IPSec per l'accesso a più client

Per i dettagli sulla configurazione di IPSec utilizzando PSK, consulta Configurare la sicurezza IP (IPSec) tramite crittografia cablata nel centro di documentazione. NetApp ONTAP

Configurazione di IPSec utilizzando l'autenticazione dei certificati

I seguenti argomenti forniscono istruzioni per configurare la crittografia IPSec utilizzando l'autenticazione dei certificati su un file system FSx for ONTAP e un client che esegue Libreswan IPSec. Questa soluzione utilizza AWS Certificate Manager e AWS Private Certificate Authority per creare un'autorità di certificazione privata e per generare i certificati.

I passaggi di alto livello per configurare la crittografia IPSec utilizzando l'autenticazione dei certificati sui file system FSx for ONTAP e sui client connessi sono i seguenti:

1. Disponete di un'autorità di certificazione per il rilascio dei certificati.

2. Genera ed esporta certificati CA per il file system e il client.
3. Installa il certificato e configura IPSec sull'istanza del client.
4. Installa il certificato e configura IPSec sul tuo file system.
5. Definire il database delle politiche di sicurezza (SPD).
6. Configurare IPSec per l'accesso a più client.

Creazione e installazione di certificati CA

Per l'autenticazione dei certificati, è necessario generare e installare certificati da un'autorità di certificazione sul file system FSx for ONTAP e sui client che accederanno ai dati sul file system. L'esempio seguente utilizza AWS Private Certificate Authority la configurazione di un'autorità di certificazione privata e la generazione dei certificati da installare sul file system e sul client. Utilizzando AWS Private Certificate Authority, è possibile creare una gerarchia interamente AWS ospitata di autorità di certificazione (CA) principali e subordinate per uso interno da parte dell'organizzazione. Questo processo prevede cinque fasi:

1. Crea un'autorità di certificazione (CA) privata utilizzando AWS Private CA
2. Emetti e installa il certificato principale sulla CA privata
3. Richiedi un certificato privato AWS Certificate Manager per il tuo file system e i tuoi client
4. Esporta il certificato per il file system e i client.

Per ulteriori informazioni, consulta la sezione Amministrazione privata della CA nella Guida AWS Private Certificate Authority per l'utente.

Per creare la CA privata principale

1. Quando si crea una CA, è necessario specificare la configurazione della CA in un file fornito dall'utente. Il comando seguente utilizza l'editor di testo Nano per creare il `ca_config.txt` file, che specifica le seguenti informazioni:

   - Il nome dell'algoritmo
   - L'algoritmo di firma utilizzato dalla CA per firmare
   - Informazioni sull'oggetto X.500

```
$ > nano ca_config.txt
```

Viene visualizzato l'editor di testo.

2. Modifica il file con le specifiche della tua CA.

```
{
   "KeyAlgorithm":"RSA_2048",
   "SigningAlgorithm":"SHA256WITHRSA",
   "Subject":{
      "Country":"US",
      "Organization":"Example Corp",
      "OrganizationalUnit":"Sales",
      "State":"WA",
      "Locality":"Seattle",
      "CommonName":"*.ec2.internal"
   }
}
```

3. Salvate e chiudete il file, uscendo dall'editor di testo. Per ulteriori informazioni, vedere Procedura per la creazione di una CA nella Guida per l' AWS Private Certificate Authority utente.

4. Utilizza il comando AWS Private CA CLI create-certificate-authority per creare una CA privata.

```
~/home > aws acm-pca create-certificate-authority \
     --certificate-authority-configuration file://ca_config.txt \
     --certificate-authority-type "ROOT" \
     --idempotency-token 01234567 --region aws-region
```

In caso di successo, questo comando genera l'Amazon Resource Name (ARN) della CA.

```
{
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

Per creare e installare un certificato per la tua CA root privata ()AWS CLI

1. Genera una richiesta di firma del certificato (CSR) utilizzando il comando `get-certificate-authority-csr` AWS CLI.

```
$ aws acm-pca get-certificate-authority-csr \
```

```
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --output text \
    --endpoint https://acm-pca.aws-region.amazonaws.com \
    --region eu-west-1 > ca.csr
```

Il file risultante`ca.csr`, un file PEM codificato in formato base64, ha il seguente aspetto.

```
-----BEGIN CERTIFICATE-----
 MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
 VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
 BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
 MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
 VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
 b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
 YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
 21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
 rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
 Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
 nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
 FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
 NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
 -----END CERTIFICATE-----
```

Per ulteriori informazioni, vedere Installazione di un certificato CA root nella Guida per l'utente. AWS Private Certificate Authority

2. Usa il `issue-certificate` AWS CLI comando per emettere e installare il certificato root sulla tua CA privata.

```
$ aws acm-pca issue-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --csr file://ca.csr \
    --signing-algorithm SHA256WITHRSA \
    --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
    --validity Value=3650,Type=DAYS --region aws-region
```

3. Scarica il certificato principale utilizzando il `get-certificate` AWS CLI comando.

```
$ aws acm-pca get-certificate \
```

```
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
    --output text --region aws-region > rootCA.pem
```

4. Installa il certificato root sulla tua CA privata utilizzando il `import-certificate-authority-certificate` AWS CLI comando.

```
$ aws acm-pca import-certificate-authority-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --certificate file://rootCA.pem --region aws-region
```

Genera ed esporta il file system e il certificato client

1. Utilizzate il `request-certificate` AWS CLI comando per richiedere un AWS Certificate Manager certificato da utilizzare sul file system e sui client.

```
$ aws acm request-certificate \
    --domain-name *.ec2.internal \
    --idempotency-token 12345 \
    --region aws-region \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

   Se la richiesta ha esito positivo, viene restituito l'ARN del certificato emesso.

2. Per motivi di sicurezza, è necessario assegnare una passphrase per la chiave privata durante l'esportazione. Create una passphrase e memorizzatela in un file denominato `passphrase.txt`

3. Usa il `export-certificate` AWS CLI comando per esportare il certificato privato emesso in precedenza. Il file esportato contiene il certificato, la catena di certificati e la chiave RSA privata crittografata a 2048 bit associata alla chiave pubblica incorporata nel certificato. Per motivi di sicurezza, è necessario assegnare una passphrase per la chiave privata durante l'esportazione. L'esempio seguente riguarda un'istanza Linux EC2.

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
```

```
    --passphrase $(cat passphrase.txt | base64)) --region aws-region >
 exported_cert.json
```

4. Usa i seguenti `jq` comandi per estrarre la chiave privata e il certificato dalla risposta JSON.

```
$ cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

5. Usa il `openssl` comando seguente per decrittografare la chiave privata dalla risposta JSON. Dopo aver immesso il comando, viene richiesta la passphrase.

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

Installazione e configurazione di Libreswan IPSec su un client Amazon Linux 2

Le seguenti sezioni forniscono istruzioni per l'installazione e la configurazione di Libreswan IPSec su un'istanza Amazon EC2 che esegue Amazon Linux 2.

Per installare e configurare Libreswan

1. Connect alla tua istanza EC2 tramite SSH. Per istruzioni specifiche su come eseguire questa operazione, consulta Connect alla tua istanza Linux utilizzando un client SSH nella Amazon Elastic Compute Cloud User Guide for Linux Instances.
2. Esegui il seguente comando per l'installazione: `libreswan`

```
$ sudo yum install libreswan
```

3. (Facoltativo) Durante la verifica di IPSec in un passaggio successivo, queste proprietà potrebbero essere contrassegnate senza queste impostazioni. Ti consigliamo di testare prima la configurazione senza queste impostazioni. Se la connessione presenta problemi, torna a questo passaggio e apporta le seguenti modifiche.

   Al termine dell'installazione, utilizzate l'editor di testo preferito per aggiungere le seguenti voci al `/etc/sysctl.conf` file.

```
net.ipv4.ip_forward=1
net.ipv4.conf.all.accept_redirects = 0
net.ipv4.conf.all.secure_redirects = 0
```

```
net.ipv4.conf.all.send_redirects = 0
net.ipv4.conf.default.accept_redirects = 0
net.ipv4.conf.default.send_redirects = 0
net.ipv4.conf.lo.accept_redirects = 0
net.ipv4.conf.lo.send_redirects = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
```

Salvate le modifiche e uscite dall'editor di testo.

4. Applica le modifiche.

```
$ sudo sysctl -p
```

5. Verificare la configurazione IPSec.

```
$ sudo ipsec verify
```

Verifica che la versione installata `Libreswan` sia in esecuzione.

6. Inizializza il database IPSec NSS.

```
$ sudo ipsec checknss
```

Per installare il certificato sul client

1. Copia il certificato che hai generato per il client nella directory di lavoro sull'istanza EC2. Utente corrente
2. Esporta il certificato generato in precedenza in un formato compatibile con`libreswan`.

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \
    -certfile rootCA.pem -out certkey.p12 -name fsx
```

3. Importa la chiave riformattata, fornendo la passphrase quando richiesta.

```
$ sudo ipsec import certkey.p12
```

4. Crea un file di configurazione IPSec utilizzando l'editor di testo preferito.

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

Aggiungere le seguenti voci al file di configurazione:

```
conn fsxn
    authby=rsasig
    left=172.31.77.6
    right=198.19.254.13
    auto=start
    type=transport
    ikev2=insist
    keyexchange=ike
    ike=aes256-sha2_384;dh20
    esp=aes_gcm_c256
    leftcert=fsx
    leftrsasigkey=%cert
    leftid=%fromcert
    rightid=%fromcert
    rightrsasigkey=%cert
```

Avvierai IPSec sul client dopo aver configurato IPSec sul tuo file system.

Configurazione di IPSec sul file system

Questa sezione fornisce istruzioni sull'installazione del certificato sul file system FSx for ONTAP e sulla configurazione di IPSec.

Per installare il certificato sul file system

1. Copia i file del certificato principale (`rootCA.pem`), del certificato client (`cert.pem`) e della chiave decrittografata (`decrypted.key`) nel file system. Dovrai conoscere la passphrase del certificato.
2. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

3. Utilizzatelo cat su un client (non sul file system in uso) per elencare il contenuto dei `decrypted.key` file `cert.pem` `erootCA.pem`, in modo da copiare l'output di ogni file e incollarlo quando richiesto nei passaggi seguenti.

```
$ > cat cert.pem
```

Copia il contenuto del certificato.

4. È necessario installare tutti i certificati CA utilizzati durante l'autenticazione reciproca, incluse le CA lato ONTAP e lato client, per la gestione dei ONTAP certificati, a meno che non siano già installati (come nel caso di una ROOT-CA autofirmata ONTAP).

Utilizzate il comando `security certificate install` NetApp CLI come segue per installare il certificato client:

```
FSxID123:: > security certificate install -vserver dr -type client -cert-name
 ipsec-client-cert
```

```
Please enter Certificate: Press <Enter> when done
```

Incolla il contenuto del `cert.pem` file che hai copiato in precedenza e premi Invio.

```
Please enter Private Key: Press <Enter> when done
```

Incolla il contenuto del `decrypted.key` file e premi invio.

```
Do you want to continue entering root and/or intermediate certificates {y|n}:
```

Invio n per completare l'immissione del certificato client.

5. Crea e installa un certificato da utilizzare da parte della SVM. La CA emittente di questo certificato deve essere già installata ONTAP e aggiunta a IPSec.

Utilizzare il comando seguente per installare il certificato principale.

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
 ipsec-ca-cert
```

```
Please enter Certificate: Press <Enter> when done
```

Incolla il contenuto del `rootCA.pem` file e premi invio.

6. Per garantire che la CA installata rientri nel percorso di ricerca CA IPSec durante l'autenticazione, aggiungi le CA di gestione dei ONTAP certificati al modulo IPSec utilizzando il comando «security ipsec ca-certificate add».

   Immettere il comando seguente per aggiungere il certificato root.

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. Immettere il comando seguente per creare la politica IPSec richiesta nel database delle politiche di sicurezza (SPD).

```
security ipsec policy create -vserver dr -name policy-name -local-ip-
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
 ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
 "CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. Utilizzare il comando seguente per mostrare la politica IPSec per la conferma del file system.

```
FSxID123:: > security ipsec policy show -vserver dr -instance

                                 Vserver: dr
                             Policy Name: promise
                          Local IP Subnets: 198.19.254.13/32
                         Remote IP Subnets: 172.31.0.0/16
                               Local Ports: 0-0
                              Remote Ports: 0-0
                                 Protocols: any
                                    Action: ESP_TRA
                              Cipher Suite: SUITEB_GCM256
          IKE Security Association Lifetime: 86400
        IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
                         Is Policy Enabled: true
                            Local Identity: CN=*.ec2.internal
                           Remote Identity: CN=*.ec2.internal
                    Authentication Method: PKI
             Certificate for Local Identity: ipsec-client-cert
```

Avviare IPSec sul client

Ora IPSec è configurato sia sul file system FSx for ONTAP che sul client, è possibile avviare IPSec sul client.

1. Connect al sistema client tramite SSH.
2. Avvia IPSec.

```
$ sudo ipsec start
```

3. Controlla lo stato di IPSec.

```
$ sudo ipsec status
```

4. Monta un volume sul tuo file system.

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. Verificate la configurazione IPSec mostrando la connessione crittografata sul file system FSx for ONTAP.

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ---------------- -----------
dr          policy-name
                   198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                   198.19.254.38   172.31.65.193   4fd3f22c993e60c5 ESTABLISHED
2 entries were displayed.
```

Configurazione di IPSec per più client

Quando un numero limitato di client deve sfruttare IPSec, è sufficiente utilizzare una singola voce SPD per ogni client. Tuttavia, quando centinaia o addirittura migliaia di client devono sfruttare IPSec, si consiglia di utilizzare la configurazione IPSec con più client.

FSx for ONTAP supporta la connessione di più client su più reti a un singolo indirizzo IP SVM con IPSec abilitato. È possibile eseguire questa operazione utilizzando la `subnet` configurazione o la `Allow all clients` configurazione, illustrate nelle seguenti procedure:

Per configurare IPSec per più client utilizzando una configurazione di sottorete

Per consentire a tutti i client su una particolare sottorete (ad esempio 192.168.134.0/24) di connettersi a un singolo indirizzo IP SVM utilizzando una singola voce di policy SPD, è necessario specificare la voce in subnet. `remote-ip-subnets` Inoltre, è necessario specificare il campo con l'identità lato client corretta. `remote-identity`

> **Important**
>
> Quando si utilizza l'autenticazione tramite certificato, ogni client può utilizzare il proprio certificato univoco o un certificato condiviso per l'autenticazione. FSx for ONTAP IPSec verifica la validità del certificato in base alle CA installate nel suo trust store locale. FSx for ONTAP supporta anche il controllo della lista di revoca dei certificati (CRL).

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Utilizzate il comando `security ipsec policy create` NetApp ONTAP CLI come segue, sostituendo i valori di *`esempio`* con i vostri valori specifici.

   ```
   FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
     -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
     -local-ports 2049 -protocols tcp -auth-method PSK \
     -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
     -remote-identity client_side_identity
   ```

Per configurare IPSec per più client utilizzando una configurazione che consente l'accesso a tutti i client

Per consentire a qualsiasi client, indipendentemente dall'indirizzo IP di origine, di connettersi all'indirizzo IP SVM abilitato per IPSec, utilizzate la `0.0.0.0/0` wild card quando specificate il campo. `remote-ip-subnets`

Inoltre, è necessario specificare il `remote-identity` campo con l'identità lato client corretta. Per l'autenticazione del certificato, puoi inserire`ANYTHING`.

Inoltre, quando si utilizza la wild card 0.0.0.0/0, è necessario configurare un numero di porta locale o remota specifico da utilizzare. Ad esempio, la porta NFS 2049.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Utilizzate il comando `security ipsec policy create` NetApp ONTAP CLI come segue, sostituendo i valori di *`esempio`* con i vostri valori specifici.

   ```
   FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
     -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
     -local-ports 2049 -protocols tcp -auth-method PSK \
     -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
     -local-ports 2049 -remote-identity client_side_identity
   ```

Gestione delle identità e degli accessi per Amazon FSx for ONTAP NetApp

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS 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 strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

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 servizio Amazon FSx per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Amazon FSx 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, consulta. Risoluzione dei problemi di identità e accesso ad Amazon FSx for NetApp ONTAP

Amministratore del servizio: se sei responsabile delle risorse Amazon FSx della tua azienda, probabilmente hai pieno accesso ad Amazon FSx. È tuo compito determinare a quali funzionalità e risorse di Amazon FSx 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, consulta. Come funziona Amazon FSx for NetApp ONTAP 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 basate

sull'identità di Amazon FSx che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Amazon FSx for ONTAP NetApp

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 sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

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) in AWSnella 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, è possibile avere un gruppo denominato IAMAdmins e concedere a tale 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 Quando creare un utente IAM (invece di un ruolo) 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. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. 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 Creazione di un ruolo per un provider di identità di terza parte 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 Differenza tra i ruoli IAM e le policy basate su risorse 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 comune che tale 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 diretto (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 azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni 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 Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella 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'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

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 azioni 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 su 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 azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM 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 su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su 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 azioni 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 (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

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 dei servizi (SCP): le SCP 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 Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- 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 una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon FSx for NetApp ONTAP 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 ONTAP NetApp

Funzionalità IAM	Supporto per Amazon FSx
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
Liste di controllo degli accessi (ACL)	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 AWS altri servizi funzionano con la maggior parte delle funzionalità IAM, AWS consulta i servizi che funzionano con IAM nella IAM User Guide.

Policy 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 azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM 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 policy basate sull'identità di Amazon FSx, consulta. Esempi di policy basate sull'identità per Amazon FSx for ONTAP NetApp

Policy 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	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni 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 azioni 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 azioni Amazon FSx, consulta Actions defined by Amazon FSx 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 policy basate sull'identità di Amazon FSx, consulta. Esempi di policy basate sull'identità per Amazon FSx for ONTAP NetApp

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. Cioè, 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).

Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni 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 risorse Amazon FSx e dei relativi ARN, consulta Resources defined by Amazon FSx nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon FSx.

Per visualizzare esempi di policy basate sull'identità di Amazon FSx, consulta. Esempi di policy basate sull'identità per Amazon FSx for ONTAP NetApp

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. Cioè, quale principale può eseguire azioni 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. Puoi 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.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi 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 condizione di Amazon FSx, consulta Condition keys for Amazon FSx nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon FSx.

Per visualizzare esempi di policy basate sull'identità di Amazon FSx, consulta. Esempi di policy basate sull'identità per Amazon FSx for ONTAP NetApp

Liste di controllo degli accessi (ACL) in Amazon FSx

Supporta le ACL	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 Che cos'è 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 delle risorse Amazon FSx, consulta. Tagging delle risorse Amazon FSx.

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 risorse Amazon FSx.

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 Cambio di un ruolo (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 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, 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 azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per Amazon FSx

Supporta i ruoli di servizio	No

Ruoli collegati ai servizi per Amazon FSx

Supporta i 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 dettagli sulla creazione o la gestione di ruoli collegati ai servizi Amazon FSx, consulta. Utilizzo di ruoli collegati ai servizi per Amazon FSx

Esempi di policy basate sull'identità per Amazon FSx for ONTAP NetApp

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Amazon FSx. 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 nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da Amazon FSx, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon FSx nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Amazon FSx
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le policy basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon FSx nel tuo account. Queste azioni 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. Puoi 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 puoi 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 IAM Access Analyzer 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 Configurazione dell'accesso alle API protetto 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 console Amazon FSx

Per accedere alla console Amazon FSx for NetApp ONTAP, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Amazon FSx 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 consentire autorizzazioni minime di console per gli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS 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 continuare a utilizzare la console Amazon FSx, collega 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 dei servizi gestiti di Amazon FSx `AmazonFSxConsoleReadOnlyAccess` e altre in. AWS politiche gestite per Amazon FSx

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": "*"
        }
    ]
}
```

Risoluzione dei problemi di identità e accesso ad Amazon FSx for NetApp ONTAP

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

- Desidero consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon FSx

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 policy devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon FSx.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio anziché 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.

Desidero consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon FSx

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 servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon FSx supporta queste funzionalità, consulta. Come funziona Amazon FSx for NetApp ONTAP con IAM
- Per sapere come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, 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 tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Utilizzo dei tag con Amazon FSx

Puoi utilizzare i tag per controllare l'accesso alle risorse Amazon FSx e implementare il controllo degli accessi basato sugli attributi (ABAC). Per applicare tag alle risorse Amazon FSx 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 Amazon FSx 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`fsx:CreateFileSystem`, ad esempio`fsx:CreateStorageVirtualMachine`, o`fsx:CreateVolume`. 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 macchine virtuali di archiviazione (SVM) e di applicare loro tag durante la creazione in uno specifico. Account AWS

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

Analogamente, la seguente policy consente agli utenti di creare backup su un file system specifico e di applicare eventuali 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 delle risorse Amazon FSx, consulta. Tagging delle risorse Amazon FSx. Per ulteriori informazioni sull'uso dei tag per controllare l'accesso alle risorse Amazon FSx, consulta. Utilizzo dei tag per controllare l'accesso alle risorse Amazon FSx

Utilizzo dei tag per controllare l'accesso alle risorse Amazon FSx

Per controllare l'accesso alle risorse e alle azioni di Amazon FSx, puoi utilizzare policy IAM basate su tag. È possibile fornire il controllo in due modi:

- Puoi controllare l'accesso alle risorse Amazon FSx 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 delle risorse Amazon FSx al momento della creazione, consulta. Concessione dell'autorizzazione

all'applicazione di tag per le risorse durante la creazione Per ulteriori informazioni sull'assegnazione di tag alle risorse, consulta Tagging delle risorse Amazon FSx..

Controllo dell'accesso in base ai tag di una risorsa

Per controllare quali azioni un utente o un ruolo può eseguire su una risorsa Amazon FSx, 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 solo quando viene utilizzato un tag specifico

Questa politica consente all'utente di creare un file system solo quando lo contrassegna con una coppia chiave-valore di tag 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 dei volumi Amazon FSx NetApp for ONTAP con un tag specifico

Questa policy consente agli utenti di creare backup solo dei volumi FSx for ONTAP etichettati con la coppia chiave-valore,. `key=Department` `value=Finance` Il backup viene creato con il tag. `Department=Finance`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
```

```
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "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 volume con un tag specifico dai backup con un tag specifico

Questa politica consente agli utenti di creare volumi con tag `Department=Finance` solo a partire da backup contrassegnati con. `Department=Finance`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "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`.

```
{
    "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:TagResource"
```

```
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example Politica di esempio: elimina un volume con tag specifici

Questa politica consente a un utente di eliminare solo i volumi contrassegnati con`Department=Finance`. Se creano un backup finale, deve essere taggato con`Department=Finance`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "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 servizi per tuo conto. AWS

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 risorse Amazon FSx perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per Amazon FSx

Amazon FSx utilizza il ruolo collegato al servizio denominato AWSServiceRoleForAmazonFSx— che esegue determinate azioni nel tuo account, come la creazione di interfacce di rete elastiche per i tuoi file system nel tuo VPC e la pubblicazione di parametri di file system e volume in. CloudWatch

Per gli aggiornamenti a questa politica, consulta AmazonF SxService RolePolicy

Dettagli dell'autorizzazione

Dettagli dell'autorizzazione

Le autorizzazioni di AWSServiceRoleForAmazonFSx ruolo sono definite dalla politica gestita da AmazonF. SxService RolePolicy AWS AWSServiceRoleForAmazonFSx Ha le seguenti autorizzazioni:

> **Note**
>
> AWSServiceRoleForAmazonFSx Viene utilizzato da tutti i tipi di file system Amazon FSx; alcune delle autorizzazioni elencate non sono applicabili a FSx for ONTAP.

- `ds`— Consente ad Amazon FSx di visualizzare, autorizzare e non autorizzare le applicazioni nella tua directory. AWS Directory Service
- `ec2`— Consente ad Amazon FSx di effettuare le seguenti operazioni:
  - Visualizza, crea e dissocia le interfacce di rete associate a un file system Amazon FSx.
  - Visualizza uno o più indirizzi IP elastici associati a un file system Amazon FSx.
  - Visualizza VPC, gruppi di sicurezza e sottoreti Amazon associati a un file system Amazon FSx.
  - 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 ad Amazon FSx di pubblicare punti dati metrici nello spazio dei nomi / FSx. CloudWatch AWS
- `route53`— Consente ad Amazon FSx di associare un Amazon VPC a una zona ospitata privata.
- `logs`— Consente ad Amazon FSx di descrivere e scrivere su Logs i flussi di CloudWatch log. In questo modo gli utenti possono inviare i log di controllo degli accessi ai file per un file system FSx for Windows File Server a CloudWatch un flusso Logs.
- `firehose`— Consente ad Amazon FSx 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 Amazon FSx for Windows File Server su un flusso di distribuzione 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-*"
        }
    ]
}
```

Tutti gli aggiornamenti a questa politica sono descritti in. Amazon FSx si aggiorna alle AWS policy 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.

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 CLI AWS Management Console IAM o nell'API IAM, 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, puoi 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 il ruolo collegato al AWSServiceRoleForAmazonFSx servizio. 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 la sezione 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, è necessario eliminare tutti i file system e i backup prima di poter eliminare manualmente il ruolo collegato al servizio.

> **Note**
>
> Se il servizio Amazon FSx 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

Utilizza la console IAM, la CLI IAM o l'API IAM per eliminare il ruolo collegato al AWSServiceRoleForAmazonFSx servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi Amazon FSx

Amazon FSx supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta AWS Regioni ed endpoint di .

AWS politiche gestite per Amazon FSx

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.

AmazonF SxService RolePolicy

Consente ad Amazon FSx di gestire AWS le risorse per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

AWS politica gestita: AmazonF SxDelete ServiceLinked RoleAccess

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 ad Amazon FSx di eliminare il relativo 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 ad Amazon FSx di visualizzare, eliminare e visualizzare lo stato di eliminazione per gli accessi FSx Service Linked Roles for Amazon S3.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonF SxDelete ServiceLinked RoleAccess nella Managed Policy Reference Guide. AWS

AWS politica gestita: AmazonF Access SxFull

Puoi collegare AmazonF alle tue entità IAMSxFullAccess . Amazon FSx associa questa politica anche a un ruolo di servizio che consente ad Amazon FSx di eseguire azioni per tuo conto.

Fornisce accesso completo ad Amazon FSx e accesso ai servizi correlati AWS .

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai responsabili l'accesso completo per eseguire tutte le azioni di Amazon FSx, ad eccezione di. `BypassSnaplockEnterpriseRetention`
- `ds`— Consente ai responsabili di visualizzare le informazioni sulle directory. AWS Directory Service
- `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 servizio Amazon FSx per conto dell'utente. Ciò è necessario affinché Amazon FSx possa gestire AWS le risorse per conto dell'utente.
- `logs`— Consente ai responsabili di creare gruppi di log, flussi di log e scrivere eventi nei flussi di log. Ciò è necessario per consentire agli utenti di monitorare l'accesso al file system di FSx for Windows File Server inviando i log di accesso di controllo a Logs. CloudWatch
- `firehose`— Consente ai mandanti di scrivere record su un Amazon Data Firehose. Ciò è necessario per consentire agli utenti di monitorare l'accesso al file system FSx for Windows File Server inviando i log di accesso di controllo a Firehose.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonF SxFull Access nella Managed Policy Reference Guide. AWS

AWS politica gestita: AmazonF SxConsole FullAccess

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 servizi correlati AWS 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 gestione Amazon FSx, ad eccezione di. `BypassSnaplockEnterpriseRetention`
- `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 su tabelle di routing, elencare interfacce di rete, tabelle di routing, gruppi di sicurezza, 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.
- `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 ad Amazon FSx di eseguire azioni per conto dell'utente.

Per visualizzare le autorizzazioni per questa politica, consulta AmazonF SxConsole FullAccess nella Managed Policy Reference Guide. AWS

AWS politica gestita: AmazonF Access SxConsole ReadOnly

È possibile allegare la policy `AmazonFSxConsoleReadOnlyAccess`alle identità IAM.

Questa politica concede autorizzazioni di sola lettura ad Amazon FSx e AWS ai servizi 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 file system Amazon FSx, inclusi tutti i tag, nella console di gestione Amazon FSx.

- `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 gestione Amazon FSx.
- `ec2`
  - Consente ai responsabili di visualizzare interfacce di rete, gruppi di sicurezza, sottoreti e il VPC associato a un file system Amazon FSx nella console di gestione Amazon FSx.
  - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
- `kms`— Consente ai mandanti di visualizzare gli alias per le AWS Key Management Service chiavi nella console di gestione Amazon FSx.
- `log`— Consente 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 visualizzare la configurazione di controllo dell'accesso ai file esistente per un file system FSx for 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 di controllo dell'accesso ai file esistente per un file system FSx for Windows File Server.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonF SxConsole ReadOnly Access nella Managed Policy Reference Guide. AWS

AWS politica gestita: AmazonF SxRead OnlyAccess

È possibile allegare la policy `AmazonFSxReadOnlyAccess`alle identità IAM.

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai responsabili di visualizzare le informazioni sui file system Amazon FSx, inclusi tutti i tag, nella console di gestione Amazon FSx.
- `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 relative a questa politica, consulta AmazonF SxRead OnlyAccess nella Managed Policy Reference Guide. AWS

Amazon FSx si aggiorna alle AWS policy 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 per Amazon FSx for ONTAP NetApp

Modifica	Descrizione	Data
AmazonF: aggiornamento a una SxService RolePolicy 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
AmazonF SxRead OnlyAccess: 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
AmazonF SxConsole ReadOnly Access: 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	9 gennaio 2024

Modifica	Descrizione	Data
	sicurezza che possono essere utilizzati con un VPC.	
AmazonF SxFull Access: 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
AmazonF SxConsole 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
AmazonF SxFull Access: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica dei dati tra regioni e più account per i file system FSx for OpenZFS.	20 dicembre 2023
AmazonF: aggiornamento a una politica esistente SxConsole FullAccess	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica dei dati tra regioni e più account per i file system FSx for OpenZFS.	20 dicembre 2023

Modifica	Descrizione	Data
AmazonF Access SxFull: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione per consentire agli utenti di eseguire la replica su richiesta dei volumi per i file system FSx for OpenZFS.	26 novembre 2023
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione per consentire agli utenti di eseguire la replica su richiesta dei volumi per i file system FSx for OpenZFS.	26 novembre 2023
AmazonF Access SxFull: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare, abilitare e disabilitare il supporto VPC condiviso per i file system FSx for ONTAP Multi-AZ.	14 novembre 2023
AmazonF SxConsole 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 per i file system FSx for ONTAP Multi-AZ.	14 novembre 2023

Modifica	Descrizione	Data
AmazonF Access SxFull: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di gestire le configurazioni di rete per i file system FSx for OpenZFS Multi-AZ.	9 agosto 2023
AWS politica gestita: AmazonF — Aggiornam ento a una politica esistente SxService RolePolicy	Amazon FSx ha modificato l'`cloudwatch:PutMetr icData` autorizzazione esistente in modo che Amazon FSx pubblichi CloudWatch i parametri nello spazio dei nomi. `AWS/FSx`	24 luglio 2023
AmazonF Access SxFull: aggiornamento a una politica esistente	Amazon FSx ha aggiornat o la policy per rimuovere l'`fsx:*`autorizzazione e aggiungere azioni specifich `efsx`.	13 luglio 2023
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiornat o la policy per rimuovere l'`fsx:*`autorizzazione e aggiungere azioni specifich `efsx`.	13 luglio 2023
AmazonF SxConsole ReadOnly Access: aggiornam ento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare metriche di prestazioni migliorate e azioni consigliate per i file system FSx for Windows File Server nella console Amazon FSx.	21 settembre 2022

Modifica	Descrizione	Data
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare metriche di prestazioni migliorate e azioni consigliate per i file system FSx for Windows File Server nella console Amazon FSx.	21 settembre 2022
AmazonF: politica di tracciamento avviata SxRead OnlyAccess	Questa policy garantisce l'accesso in sola lettura a tutte le risorse Amazon FSx e a tutti i tag ad esse associati.	4 febbraio 2022
AmazonF SxDelete ServiceLi nked RoleAccess — Avviata la politica di tracciamento	Questa politica concede autorizzazioni amministrative che consentono ad Amazon FSx di eliminare il suo Service Linked Role per l'accesso ad Amazon S3.	7 gennaio 2022
AmazonF SxService RolePolic y: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di gestire le configurazioni di rete per i file system Amazon FSx for ONTAP. NetApp	2 settembre 2021
AmazonF Access SxFull: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare tag sulle tabelle di routing EC2 per chiamate con ambito limitato.	2 settembre 2021

Modifica	Descrizione	Data
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare Amazon FSx per i file system ONTAP Multi-AZ. NetApp	2 settembre 2021
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare tag sulle tabelle di routing EC2 per chiamate con ambito limitato.	2 settembre 2021
AmazonF SxService RolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di descrivere e scrivere su Logs i flussi di log. CloudWatch Ciò è necessario per consentire e agli utenti di visualizzare i registri di controllo degli accessi ai file per i file system FSx for Windows File Server utilizzando Logs. CloudWatch	8 giugno 2021

Modifica	Descrizione	Data
AmazonF: aggiornamento a una SxService RolePolicy politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di descrivere e scrivere nei flussi di distribuzione di Amazon Data Firehose. Ciò è necessario per consentir e agli utenti di visualizzare i log di controllo degli accessi ai file per un file system FSx for Windows File Server utilizzan do Amazon Data Firehose.	8 giugno 2021
AmazonF SxFull Access: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere e creare gruppi di CloudWatch log, flussi di log e scrivere eventi nei flussi di log. Ciò è necessario affinché i responsabili possano visualizz are i registri di controllo degli accessi ai file per i file system FSx for Windows File Server utilizzando Logs. CloudWatch	8 giugno 2021

Modifica	Descrizione	Data
AmazonF SxFull Access: 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 per un file system FSx for Windows File Server utilizzan do Amazon Data Firehose.	8 giugno 2021
AmazonF: aggiornamento a una SxConsole FullAccess 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 file system FSx for Windows File Server.	8 giugno 2021

Modifica	Descrizione	Data
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere i flussi di distribuz ione 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 un file system FSx for Windows File Server.	8 giugno 2021
AmazonF SxConsole ReadOnly Access: aggiornam ento 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 visualizz are la configurazione di controllo dell'accesso ai file esistente per un file system FSx for Windows File Server.	8 giugno 2021

Modifica	Descrizione	Data
AmazonF SxConsole ReadOnly Access: aggiornam ento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere i flussi di distribuz ione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano visualizz are la configurazione di controllo dell'accesso ai file esistente per un file system FSx for Windows File Server.	8 giugno 2021
Amazon FSx ha iniziato a tracciare le modifiche	Amazon FSx ha iniziato a tracciare le modifiche per le sue politiche AWS gestite.	8 giugno 2021

Controllo degli accessi ai file system con Amazon VPC

Puoi accedere ai file system e alle SVM di Amazon FSx for NetApp ONTAP utilizzando il nome DNS o l'indirizzo IP di uno dei loro endpoint, a seconda del tipo di accesso. Il nome DNS viene mappato all'indirizzo IP privato dell'interfaccia di rete elastica del file system o SVM nel tuo VPC. Solo le risorse all'interno del VPC associato o le risorse collegate al VPC associato tramite una VPN possono accedere ai dati del file system tramite i protocolli NFS, SMB AWS Direct Connect o iSCSI. Per ulteriori informazioni, consulta Cos'è Amazon VPC? nella Guida per l'utente di Amazon VPC.

> **Warning**
>
> Non è necessario modificare o eliminare le interfacce elastiche di rete associate al 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.

Gruppi di sicurezza Amazon VPC

Un gruppo di sicurezza funge da firewall virtuale per i file system FSx for ONTAP per controllare il traffico in entrata e in uscita. Le regole in entrata controllano il traffico in entrata verso il file system e le regole in uscita controllano il traffico in uscita dal file system. Quando si crea un file system, si specifica il VPC in cui viene creato e viene applicato il gruppo di sicurezza predefinito per quel VPC. È possibile aggiungere regole a ciascun gruppo di sicurezza che consentano il traffico da o verso i file system e le SVM associati. Puoi modificare le regole di un gruppo di sicurezza in qualsiasi momento. Le regole nuove e modificate vengono applicate automaticamente a tutte le risorse associate al gruppo di sicurezza. Quando Amazon FSx decide se consentire al traffico di raggiungere una risorsa, valuta tutte le regole di tutti i gruppi di sicurezza associati alla risorsa.

Per utilizzare un gruppo di sicurezza per controllare l'accesso al file system Amazon FSx, aggiungi regole in entrata e in uscita. Le regole in entrata controllano il traffico in entrata e le regole in uscita controllano il traffico in uscita dal tuo file system. Assicurati di avere le regole del traffico di rete corrette nel tuo gruppo di sicurezza per mappare la condivisione di file del tuo file system Amazon FSx 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 Guida per l'utente di Amazon EC2.

Creazione di un gruppo di sicurezza VPC

Per creare un gruppo di sicurezza per Amazon FSx

1. Apri la console Amazon EC2 all'indirizzo 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 Amazon VPC associato al tuo file system per creare il gruppo di sicurezza all'interno di quel VPC.
6. Per le regole in uscita, consenti tutto il traffico su tutte le porte.
7. Aggiungi le seguenti regole alle porte in entrata del tuo gruppo di sicurezza. Per il campo source, è necessario scegliere Personalizzato e inserire i gruppi di sicurezza o gli intervalli di indirizzi IP associati alle istanze che devono accedere al file system FSx for ONTAP, tra cui:

   - Client Linux, Windows e/o macOS che accedono ai dati del file system tramite NFS, SMB o iSCSI.

- Qualsiasi file system/cluster ONTAP da collegare al file system (ad esempio, da utilizzare o). SnapMirror SnapVault FlexCache
- Qualsiasi client che utilizzerai per accedere all'API REST, alla CLI o alle API di ONTAP (ad esempio, un'istanza NetApp Harvest/Grafana, Connector o BlueXP). NetApp

Protocollo	Porte	Ruolo
Tutte le regole ICMP	Tutti	Ping dell'istanza
SSH	22	Accesso SSH all'indirizzo IP del LIF di gestione del cluster o di un LIF di gestione dei nodi
TCP	111	Chiamata di procedura remota per NFS
TCP	135	Chiamata di procedura remota per CIFS
TCP	139	Sessione di servizio NetBIOS per CIFS
TCP	161-162	Protocollo di gestione della rete semplice (SNMP)
TCP	443	Accesso tramite API REST ONTAP all'indirizzo IP del LIF di gestione del cluster o a un LIF di gestione SVM
TCP	445	Microsoft SMB/CIFS su TCP con framing NetBIOS
TCP	635	Montaggio NFS
TCP	749	Kerberos
TCP	2049	demone del server NFS
TCP	3260	Accesso iSCSI tramite il LIF dei dati iSCSI
TCP	4045	demone di blocco NFS
TCP	4046	Monitoraggio dello stato della rete per NFS

Protocollo	Porte	Ruolo
TCP	10000	Protocollo di gestione dei dati di rete (NDMP) e NetApp SnapMirror comunicazione tra cluster
TCP	11104	Gestione della comunicazione NetApp SnapMirror tra cluster
TCP	11105	SnapMirror trasferimento dati tramite LIF intercluster
UDP	111	chiamata di procedura remota per NFS
UDP	135	Chiamata di procedura remota per CIFS
UDP	137	Risoluzione dei nomi NetBIOS per CIFS
UDP	139	Sessione di servizio NetBIOS per CIFS
UDP	161-162	Protocollo di gestione della rete semplice (SNMP)
UDP	635	Montaggio NFS
UDP	2049	demone del server NFS
UDP	4045	demone di blocco NFS
UDP	4046	Monitoraggio dello stato della rete per NFS
UDP	4049	Protocollo di quota NFS

8. Aggiungi il gruppo di sicurezza all'interfaccia elastica di rete del file system.

Impedisci l'accesso a un file system

Per impedire temporaneamente l'accesso di rete al file system da parte di tutti i client, è possibile rimuovere tutti i gruppi di sicurezza associati alle elastic network interface del file system e sostituirli con un gruppo privo di regole in entrata/in uscita.

Convalida della conformità per Amazon NetApp FSx for ONTAP

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:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

  > **Note**
  >
  > Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti 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)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: 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 per NetApp ONTAP e endpoint VPC di interfaccia ()AWS PrivateLink

Puoi migliorare il livello di sicurezza del tuo VPC configurando Amazon FSx per utilizzare un endpoint VPC di interfaccia. Gli endpoint VPC di interfaccia sono basati su una tecnologia che consente di AWS PrivateLinkaccedere in modo privato alle API Amazon FSx 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 le API di Amazon FSx. Il traffico tra il tuo VPC e Amazon FSx non esce dalla rete. AWS

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'API Amazon FSx.

Considerazioni sugli endpoint VPC con interfaccia Amazon FSx

Prima di configurare un endpoint VPC di interfaccia per Amazon FSx, assicurati di esaminare le proprietà e le limitazioni degli endpoint VPC dell'interfaccia nella Amazon VPC User Guide.

Puoi chiamare qualsiasi operazione dell'API Amazon FSx dal tuo VPC. Ad esempio, puoi creare un file system FSx for ONTAP chiamando l' CreateFileSystem API dall'interno del tuo VPC. Per l'elenco completo delle API di Amazon FSx, consulta Actions in Amazon FSx API Reference.

Considerazioni sul peering VPC

Puoi connettere altri VPC al VPC con endpoint VPC di interfaccia utilizzando il peering VPC. Il peering VPC è una connessione di rete tra due VPC. Puoi stabilire una connessione peering VPC tra i tuoi due VPC o con un VPC in un altro. Account AWS I VPC possono anche essere in due formati diversi. Regioni AWS

Il traffico tra VPC peer rimane sulla AWS rete e non attraversa la rete Internet pubblica. Una volta eseguito il peering dei VPC, risorse come le istanze Amazon Elastic Compute Cloud (Amazon EC2) in entrambi i VPC possono accedere all'API Amazon FSx tramite endpoint VPC di interfaccia creati in uno dei VPC.

Creazione di un endpoint VPC di interfaccia per l'API Amazon FSx

Puoi creare un endpoint VPC per l'API Amazon FSx utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta Creazione di un endpoint VPC di interfaccia nella Amazon VPC User Guide.

Per creare un endpoint VPC di interfaccia per Amazon FSx, utilizza uno dei seguenti:

- **`com.amazonaws.`*`region`*`.fsx`**— Crea un endpoint per le operazioni dell'API Amazon FSx.
- **`com.amazonaws.`*`region`*`.fsx-fips`**— Crea un endpoint per l'API Amazon FSx 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 l'accesso all'API Amazon FSx, puoi 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.

Resilienza in Amazon NetApp FSx per ONTAP

L'infrastruttura AWS globale è costruita attorno a zone di disponibilità. Regioni AWS Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle zone di disponibilità, vedere Global Regioni AWS Infrastructure.AWS

Oltre all'infrastruttura AWS globale, Amazon FSx offre diverse funzionalità per supportare le tue esigenze di resilienza e backup dei dati.

Backup e ripristino

Amazon FSx crea e salva backup automatici dei volumi nel file system Amazon FSx for ONTAP. NetApp Amazon FSx crea backup automatici dei volumi durante la finestra di backup del file system Amazon FSx for ONTAP. NetApp Amazon FSx salva i backup automatici dei volumi in base al periodo di conservazione dei backup specificato. Puoi anche eseguire il backup dei volumi manualmente, creando un backup avviato dall'utente. È possibile ripristinare un backup di volume in qualsiasi momento creando un nuovo volume con il backup specificato come origine.

Per ulteriori informazioni, consulta Utilizzo dei backup.

Snapshot

Amazon FSx crea copie istantanee dei volumi Amazon FSx for ONTAP. NetApp Le copie istantanee offrono protezione contro l'eliminazione o la modifica accidentale dei file nei volumi da parte degli utenti finali. Per ulteriori informazioni, consulta Utilizzo degli snapshot.

Zone di disponibilità

I file system Amazon FSx for NetApp ONTAP sono progettati per fornire una disponibilità continua dei dati anche in caso di guasto del server. Ogni file system è alimentato da due file server in almeno una zona di disponibilità, ciascuno con il proprio storage. Amazon FSx replica automaticamente i dati per proteggerli dai guasti dei componenti, monitora continuamente i guasti hardware e sostituisce automaticamente i componenti dell'infrastruttura in caso di guasto. Il failover e il back back dei file system vengono eseguiti automaticamente in base alle esigenze (in genere entro 60 secondi), mentre i client eseguono automaticamente il failover e il back back insieme al file system.

File system Multi-AZ

I file system Amazon FSx for NetApp ONTAP sono altamente disponibili e durevoli in tutte le zone di AWS disponibilità e sono progettati per fornire una disponibilità continua dei dati anche nel caso in cui una zona di disponibilità non sia disponibile.

Per ulteriori informazioni, consulta Disponibilità e durabilità.

File system Single-AZ

I file system Amazon FSx for NetApp ONTAP sono altamente disponibili e durevoli all'interno di una singola zona di AWS disponibilità e sono progettati per fornire una disponibilità continua all'interno di tale zona di disponibilità in caso di guasto di un singolo file server o disco.

Per ulteriori informazioni, consulta Disponibilità e durabilità.

Sicurezza dell'infrastruttura in Amazon FSx for ONTAP NetApp

In quanto servizio gestito, Amazon FSx for NetApp ONTAP è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere ad Amazon FSx attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (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. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Usa NetApp ONTAP Vscan con FSx per ONTAP

È possibile utilizzare la funzionalità Vscan di NetApp ONTAP per eseguire software antivirus di terze parti supportati. Per ulteriori informazioni, consulta le seguenti risorse per ciascuna delle soluzioni supportate.

- McAfee — Guida alla soluzione antivirus per Clustered Data ONTAP: McAfee
- SentinelOne — Soluzioni partner Vscan e SentinelOne Singularity Cloud Data Security
- Symantec: soluzioni partner Vscan e Symantec Protection Engine
- Trend Micro — Guida alla soluzione antivirus per Clustered Data ONTAP: Trend Micro

Ruoli e utenti in Amazon FSx for ONTAP NetApp

NetApp ONTAPinclude una funzionalità di controllo degli accessi basata sui ruoli (RBAC) robusta ed estensibile. ONTAPi ruoli definiscono le capacità e i privilegi degli utenti quando si utilizzano la ONTAP CLI e l'API REST. Ogni ruolo definisce un diverso livello di capacità e privilegi amministrativi. Assegnate ruoli agli utenti allo scopo di controllarne l'accesso alle risorse FSx for ONTAP quando utilizzate ONTAP l'API REST e la CLI. I ONTAP ruoli sono disponibili separatamente per gli utenti del file system FSx for ONTAP e per gli utenti di Storage Virtual Machine (SVM).

Quando si crea un file system FSx for ONTAP, viene creato un ONTAP utente predefinito a livello di file system e a livello SVM. È possibile creare utenti di file system e SVM aggiuntivi e creare ruoli SVM aggiuntivi per soddisfare le esigenze dell'organizzazione. Questo capitolo spiega ONTAP utenti e ruoli e fornisce procedure dettagliate per la creazione di utenti e ruoli SVM aggiuntivi.

Ruoli e utenti dell'amministratore del file system

L'utente predefinito del ONTAP file system è`fsxadmin`, a cui è assegnato il `fsxadmin` ruolo. È possibile assegnare due ruoli predefiniti agli utenti del file system, elencati di seguito:

- **`fsxadmin`**—Gli amministratori con questo ruolo dispongono di diritti illimitati nel sistema. ONTAP Possono configurare tutte le risorse a livello di file system e SVM disponibili sui file system FSx for ONTAP.
- **`fsxadmin-readonly`**—Gli amministratori con questo ruolo possono visualizzare tutto a livello di file system ma non possono apportare modifiche.

  Questo ruolo è ideale per l'uso con le applicazioni di monitoraggio, ad esempio NetApp Harvest perché ha accesso in sola lettura a tutte le risorse disponibili e alle relative proprietà, ma non può apportarvi alcuna modifica.

È possibile creare utenti del file system aggiuntivi e assegnare loro il ruolo o. `fsxadmin` `fsxadmin-readonly` Non è possibile creare nuovi ruoli o modificare i ruoli esistenti. Per ulteriori informazioni, consulta Creazione di nuovi ONTAP utenti per l'amministrazione del file system e SVM.

La tabella seguente descrive il livello di accesso dei ruoli di amministratore del file system per i comandi e le directory dei comandi ONTAP CLI e REST API.

Nome ruolo	Livello di accesso	Ai seguenti comandi o directory di comandi
`fsxadmin`	tutto	Tutte le directory di comandi disponibili in FSx for ONTAP
`fsxadmin-readonly`	tutto	`security login password` Solo per gestire il proprio account utente, la password locale e le informazioni chiave
	nessuno	`security`

Nome ruolo	Livello di accesso	Ai seguenti comandi o directory di comandi
	sola lettura	Tutte le altre directory di comandi disponibili in FSx for ONTAP

Ruoli e utenti dell'amministratore SVM

Ogni SVM ha un dominio di autenticazione separato e può essere gestita in modo indipendente dai propri amministratori. Per ogni SVM del file system, l'utente predefinito è vsadmin, a cui viene assegnato il `vsadmin` ruolo di default. Oltre al `vsadmin` ruolo, esistono altri ruoli SVM predefiniti che forniscono autorizzazioni limitate che è possibile assegnare agli utenti SVM. È inoltre possibile creare ruoli personalizzati che forniscono il livello di controllo degli accessi adatto alle esigenze dell'organizzazione.

I ruoli predefiniti per gli amministratori SVM e le relative funzionalità sono i seguenti:

Nome ruolo	Funzionalità
`vsadmin`	• Gestisci il tuo account utente, la password locale e le informazioni chiave • Gestisci i volumi, ad eccezione degli spostamenti di volume • Gestisci quote, qtree, copie istantanee e file • Gestisci le LUN • Esegui SnapLock operazioni, ad eccezione dell'eliminazione con privilegi • Configurazione dei protocolli: NFS, SMB e iSCSI • Configura i servizi: DNS, LDAP e NIS • Monitoraggio dei lavori • Monitora le connessioni di rete e l'interfaccia di rete

Nome ruolo	Funzionalità
	• Monitora lo stato della SVM
`vsadmin-volume`	• Gestisci il tuo account utente, la password locale e le informazioni chiave • Gestisci i volumi, compresi gli spostamenti di volume • Gestisci quote, qtree, copie istantanee e file • Gestisci le LUN • Configurazione dei protocolli: NFS, SMB e iSCSI • Configura i servizi: DNS, LDAP e NIS • Monitora l'interfaccia di rete • Monitora lo stato di salute della SVM
`vsadmin-protocol`	• Gestisci il tuo account utente, la password locale e le informazioni chiave • Gestisci le LUN • Configurazione dei protocolli: NFS, SMB e iSCSI • Configura i servizi: DNS, LDAP e NIS • Monitora l'interfaccia di rete • Monitora lo stato di salute della SVM
`vsadmin-backup`	• Gestisci il tuo account utente, la password locale e le informazioni chiave • Gestisci le operazioni NDMP • Effettua la lettura/scrittura di un volume ripristinato • Gestisci le SnapMirror relazioni e le copie delle istantanee • Visualizza i volumi e le informazioni di rete

Nome ruolo	Funzionalità
`vsadmin-snaplock`	• Gestisci il tuo account utente, la password locale e le informazioni chiave • Gestisci i volumi, ad eccezione degli spostamenti di volume • Gestisci quote, qtree, copie istantanee e file • Esegui SnapLock operazioni, inclusa l'elimina zione con privilegi • Configura i protocolli: NFS e SMB • Configura i servizi: DNS, LDAP e NIS • Monitoraggio dei lavori • Monitora le connessioni di rete e l'interfaccia di rete
`vsadmin-readonly`	• Gestisci il tuo account utente, la password locale e le informazioni chiave • Monitora lo stato di salute della SVM • Monitora l'interfaccia di rete • Visualizza volumi e LUN • Visualizza servizi e protocolli

Per ulteriori informazioni su come creare un nuovo ruolo SVM, vedereCreazione di un nuovo ruolo SVM.

Utilizzo di Active Directory per autenticare gli utenti ONTAP

È possibile autenticare l'accesso degli utenti del dominio Windows Active Directory a un file system FSx for ONTAP e SVM. È necessario eseguire le seguenti attività prima che gli account Active Directory possano accedere al file system:

- È necessario configurare l'accesso del controller di dominio Active Directory alla SVM.

  L'SVM utilizzato per configurare come gateway o tunnel per l'accesso al controller di dominio Active Directory deve avere CIFS abilitato, essere aggiunto a un Active Directory o entrambi. Se non stai

abilitando CIFS e stai solo unendo il tunnel SVM a un Active Directory, assicurati che l'SVM sia aggiunto al tuo Active Directory. Per ulteriori informazioni, consulta Unire SVM a Microsoft Active Directory.

- È necessario abilitare un account utente di dominio Active Directory per accedere al file system.

  È possibile utilizzare l'autenticazione tramite password o l'autenticazione a chiave pubblica SSH per gli utenti del dominio Windows che accedono alla ONTAP CLI o all'API REST.

Per le procedure che descrivono come utilizzare per configurare l'autenticazione Active Directory per gli amministratori del file system e SVM, vedere. Configurazione dell'autenticazione Active Directory per gli utenti ONTAP

Creazione di nuovi ONTAP utenti per l'amministrazione del file system e SVM

Ogni ONTAP utente è associato a un SVM o al file system. Gli utenti del file system con il `fsxadmin` ruolo possono creare nuovi ruoli e utenti SVM utilizzando il comando `security login create`ONTAPCLI.

Il `security login create` comando crea un metodo di accesso per l'utilità di gestione. Un metodo di accesso è costituito da un nome utente, un'applicazione (metodo di accesso) e un metodo di autenticazione. Un nome utente può essere associato a più applicazioni. Facoltativamente può includere un nome di ruolo per il controllo degli accessi. Se viene utilizzato un nome di gruppo Active Directory, LDAP o NIS, il metodo di login consente l'accesso agli utenti appartenenti al gruppo specificato. Se l'utente è membro di più gruppi indicati nella tabella di accesso di sicurezza, avrà accesso a un elenco combinato dei comandi autorizzati per i singoli gruppi.

Per informazioni su come creare un nuovo ONTAP utente, vedere. Creazione di un nuovo utente ONTAP

Argomenti

- Creazione di un nuovo utente ONTAP
- Creazione di un nuovo ruolo SVM
- Configurazione dell'autenticazione Active Directory per gli utenti ONTAP
- Configurazione dell'autenticazione a chiave pubblica
- Aggiornamento dei requisiti relativi alle password per i ruoli del file system e SVM

- L'aggiornamento della password fsxadmin dell'account non riesce

Creazione di un nuovo utente ONTAP

Per creare un nuovo utente SVM o del file system (ONTAPCLI)

Solo gli utenti del file system con il `fsxadmin` ruolo possono creare nuovi utenti SVM e del file system.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Utilizzate il comando `security login create` ONTAP CLI per creare un nuovo account utente sul file system FSx for ONTAP o SVM.

   Inserite i dati per i segnaposto nell'esempio per definire le seguenti proprietà obbligatorie:

   - `-vserver`— Specificate il nome della SVM in cui desiderate creare il nuovo ruolo o utente SVM. Se state creando un ruolo o un utente del file system, non specificate un SVM.
   - `-user-or-group-name`— specifica il nome utente o il nome del gruppo Active Directory del metodo di accesso. Il nome del gruppo Active Directory può essere specificato solo con il metodo di `domain` autenticazione `ontapi` e le `ssh` applicazioni.
   - `-application`— specifica l'applicazione del metodo di accesso. I valori possibili includono http, ontapi e ssh.
   - `-authentication-method`— specifica il metodo di autenticazione per l'accesso. I valori possibili sono:
     - dominio: da utilizzare per l'autenticazione di Active Directory
     - password: da utilizzare per l'autenticazione tramite password
     - publickey: utente per l'autenticazione con chiave pubblica
   - `-role`— Speciifica il nome del ruolo di controllo degli accessi per il metodo di accesso. A livello di file system, l'unico ruolo che può essere specificato è. `fsxadmin`

(Facoltativo) È inoltre possibile utilizzare uno o più dei seguenti parametri con il comando:

- `[-comment]`— Da utilizzare per includere una notazione o un commento per l'account utente. Ad esempio, **`Guest account`**. La lunghezza massima è 128 caratteri.
- `[-second-authentication-method {none|publickey|password|nsswitch}]`— Speciifica il metodo di autenticazione a secondo fattore. È possibile specificare i seguenti metodi:
  - password: da utilizzare per l'autenticazione della password
  - publickey: da utilizzare per l'autenticazione con chiave pubblica
  - nsswitch: da utilizzare per l'autenticazione NIS o LDAP
  - none: il valore predefinito se non ne specifichi uno

```
Fsx0123456::> security login create -vserver vserver_name -user-or-group-
name user_or_group_name -application login_application -authentication-
method auth_method -role role_or_account_name
```

Il comando seguente crea un nuovo utente del file system `new_fsxadmin` con il `fsxadmin-readonly` ruolo assegnato, utilizzando SSH con una password per l'accesso. Quando richiesto, fornite una password per l'utente.

```
Fsx0123456::> security login create -user-or-group-name new_fsxadmin -application
 ssh -authentication-method password -role fsxadmin-readonly

Please enter a password for user 'new_fsxadmin':
Please enter it again:

Fsx0123456::>
```

3. Il comando seguente crea un nuovo utente SVM `new_vsadmin` sulla `fsx` SVM con il `vsadmin_readonly` ruolo, configurato per utilizzare SSH con una password per l'accesso. Quando richiesto, fornite una password per l'utente.

```
Fsx0123456::> security login create -vserver fsx  -user-or-group-name new_vsadmin -
application ssh -authentication-method password -role vsadmin-readonly

Please enter a password for user 'new_vsadmin':
```

```
Please enter it again:

Fsx0123456::>
```

4. Il comando seguente crea un nuovo utente del file system di sola lettura `harvest2-user` che deve essere utilizzato dall'applicazione NetApp Harvest per raccogliere i parametri di prestazioni e capacità. Per ulteriori informazioni, consulta Monitoraggio di FSx per i file system ONTAP con Harvest e Grafana.

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application
 ssh -role fsxadmin-readonly -authentication-method password
```

Per visualizzare le informazioni per tutti gli utenti del file system e SVM

- Utilizzate il seguente comando per visualizzare tutte le informazioni di accesso per il file system e le SVM.

```
Fsx0123456::> security login show

Vserver: Fsx0123456
                                                                 Second
User/Group                Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked  Method
-------------- ----------- ------------- ---------------- ------ --------------
autosupport    console     password      autosupport      no     none
fsxadmin       http        password      fsxadmin         no     none
fsxadmin       ontapi      password      fsxadmin         no     none
fsxadmin       ssh         password      fsxadmin         no     none
fsxadmin       ssh         publickey     fsxadmin         -      none
new_fsxadmin   ssh         password      fsxadmin-readonly
                                                        no     none

Vserver: fsx
                                                                 Second
User/Group                Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked  Method
-------------- ----------- ------------- ---------------- ------ --------------
new_vsadmin    ssh         password      vsadmin-readonly no     none
vsadmin        http        password      vsadmin          yes    none
vsadmin        ontapi      password      vsadmin          yes    none
vsadmin        ssh         password      vsadmin          yes    none
```

```
10 entries were displayed.

Fsx0123456::>
```

Creazione di un nuovo ruolo SVM

Ogni SVM che crei ha un amministratore SVM predefinito a cui è assegnato il ruolo predefinito. `vsadmin` Oltre al set di ruoli SVM predefiniti, è possibile creare nuovi ruoli SVM. Se devi creare nuovi ruoli per il tuo SVM, usa il comando `security login role create` ONTAP CLI. Questo comando è disponibile per gli amministratori del file system con il ruolo. `fsxadmin`

Per creare un nuovo ruolo SVM (ONTAP CLI)

1. È possibile creare un nuovo ruolo SVM utilizzando il comando: `security login role create` ONTAP CLI

   ```
   Fsx0123456::> security login role create -role vol_role -cmddirname volume
   ```

2. Specificate i seguenti parametri obbligatori nel comando:

   - `-role`— Il nome del ruolo.
   - `-cmddirname`— Il comando o la directory dei comandi a cui il ruolo dà accesso. Racchiude i nomi delle sottodirectory dei comandi tra virgolette doppie. Ad esempio, `"volume snapshot"`. Invio `DEFAULT` per specificare tutte le directory dei comandi.

3. (Facoltativo) È inoltre possibile aggiungere uno dei seguenti parametri al comando:

   - `-vserver`— Il nome della SVM associata al ruolo.
   - `-access`— Il livello di accesso per il ruolo. Per le directory di comando, ciò include:
     - none— Nega l'accesso ai comandi nella directory dei comandi. Questo è il valore predefinito per i ruoli personalizzati.
     - `readonly`— Concede l'accesso ai comandi show nella directory dei comandi e nelle relative sottodirectory.
     - `all`— Concede l'accesso a tutti i comandi nella directory dei comandi e nelle relative sottodirectory. Per concedere o negare l'accesso ai comandi intrinseci, è necessario specificare la directory dei comandi.

Per i comandi non intrinseci (comandi che non terminano con,, o): `create` `modify` `delete` `show`

- `none`— Nega l'accesso ai comandi nella directory dei comandi. Questo è il valore predefinito per i ruoli personalizzati.
- `readonly`— Non applicabile. Non usare.
- `all`— Concede l'accesso al comando.

- `-query`— L'oggetto di interrogazione utilizzato per filtrare il livello di accesso, specificato sotto forma di un'opzione valida per il comando o per un comando nella directory dei comandi. Racchiudere l'oggetto della query tra virgolette doppie.

4. Esegui il comando `security login role create`.

   Il comando seguente crea un ruolo di controllo degli accessi denominato «admin» per il Vserver vs1.example.com. Il ruolo ha accesso completo al comando «volume» ma solo all'interno dell'aggregato «aggr0".

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-
aggr aggr0" -access all -vserver vs1.example.com
```

Configurazione dell'autenticazione Active Directory per gli utenti ONTAP

Utilizza la ONTAP CLI per configurare l'uso dell'autenticazione Active Directory per gli utenti del ONTAP file system e SVM.

È necessario essere un amministratore del file system con il `fsxadmin` ruolo necessario per utilizzare i comandi di questa procedura.

Per configurare l'autenticazione Active Directory per ONTAP gli utenti (ONTAPCLI)

I comandi di questa procedura sono disponibili per gli utenti del file system con il `fsxadmin` ruolo.

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Utilizzate il `security login domain-tunnel create`comando come illustrato per stabilire un tunnel di dominio per l'autenticazione degli utenti di Windows Active Directory. Sostituisci *`svm_name con il nome`* dell'SVM che stai utilizzando per il tunnel di dominio.

```
FsxId0123456::> security login domain-tunnel create -vserver svm_name
```

3. Utilizzate il `security login create`comando per creare account utente di dominio Active Directory che accederanno al file system.

   Specificare i seguenti parametri richiesti nel comando:

   - `-vserver`— Il nome della SVM configurata con CIFS e aggiunta all'Active Directory. Verrà utilizzato come tunnel per l'autenticazione degli utenti del dominio Active Directory nel file system, nel quale verrà creato il nuovo ruolo o utente.
   - `-user-or-group-name`— Il nome utente o il nome del gruppo Active Directory del metodo di accesso. Il nome del gruppo Active Directory può essere specificato solo con il metodo di `domain` autenticazione `ontapi` e `ssh` l'applicazione.
   - `-application`— L'applicazione del metodo di accesso. I valori possibili includono http, ontapi e ssh.
   - `-authentication-method`— Il metodo di autenticazione utilizzato per il login. I valori possibili sono:
     - dominio — per l'autenticazione di Active Directory
     - password — per l'autenticazione tramite password
     - publickey — per l'autenticazione con chiave pubblica
   - `-role`— Il nome del ruolo di controllo degli accessi per il metodo di accesso. A livello di file system, l'unico ruolo che può essere specificato è. `-role fsxadmin`

   L'esempio seguente crea un account utente di dominio Active Directory `CORP\Admin` per il `filesystem1` file system.

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
application ssh -authmethod domain -role fsxadmin
```

   L'esempio seguente crea l'account `CORP\Admin` utente con autenticazione a chiave pubblica.

```
FsxId0123456ab::> security login create -user-or-group-name "CORP\Admin" -
application ssh -authentication-method publickey -role fsxadmin
Warning: To use public-key authentication, you must create a public key for user
 "CORP\Admin".
```

Crea una chiave pubblica per l'`CORP\Admin`utente utilizzando il seguente comando:

```
FsxId0123456ab::> security login publickey create -username "CORP
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=
 cwaltham@b0be837a91bf.ant.amazon.com"
```

Per accedere al file system utilizzando SSH con credenziali Active Directory

- L'esempio seguente mostra come accedere tramite SSH al file system con le credenziali di Active Directory, se si sceglie il tipo. `ssh -application` Il formato `username "domain-name \user-name"` è il nome di dominio e il nome utente forniti durante la creazione dell'account, separati da una barra rovesciata e racchiusi tra virgolette.

  ```
  Fsx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
  ```

  Quando viene richiesto di inserire una password, utilizza la password dell'utente di Active Directory.

Configurazione dell'autenticazione a chiave pubblica

Per abilitare l'autenticazione con chiave pubblica SSH, devi prima generare una chiave SSH e associarla a un account amministratore utilizzando il comando. `security login publickey create` Ciò consente all'account di accedere alla SVM. Il `security login publickey create` comando accetta i seguenti parametri.

Parametro	Descrizione
`-vserver` (facoltativo).	Il nome della SVM a cui l'account accede. Se state configurando l'autenticazione a chiave pubblica SSH per gli utenti del file system, non includetelo. `-versver`

Parametro	Descrizione
`-username`	Il nome utente dell'account. Il valore predefini to,`admin`, è il nome predefinito dell'ammi nistratore del cluster.
`-index`	Il numero di indice della chiave pubblica. Il valore predefinito è 0 se la chiave è la prima chiave creata per l'account. Altrimenti, il valore predefinito è uno in più rispetto al numero di indice più alto esistente per l'account.
`-publickey`	La chiave pubblica OpenSSH. Racchiudere la chiave tra virgolette doppie.
`-role`	Il ruolo di controllo degli accessi assegnato all'account.
`-comment` (facoltativo).	Testo descrittivo per la chiave pubblica. Racchiudere il testo tra virgolette doppie.

L'esempio seguente associa una chiave pubblica all'account `svmadmin` di amministratore SVM per la SVM. `svm01` Alla chiave pubblica viene assegnato un numero di indice. `5`

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J/
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

> **Important**
>
> È necessario essere un amministratore di SVM o di file system per eseguire questa attività.

Aggiornamento dei requisiti relativi alle password per i ruoli del file system e SVM

È possibile aggiornare i requisiti di password per un file system o un ruolo SVM utilizzando il comando `security login role config modify`ONTAPCLI. Questo comando è disponibile solo per gli account di amministratore del file system con il `fsxadmin` ruolo. Quando si modificano i requisiti relativi alla password, il sistema avviserà se vi sono utenti esistenti con quel ruolo che saranno interessati dalla modifica.

L'esempio seguente modifica la lunghezza minima della password richiesta a 12 caratteri per gli utenti con il `vsadmin-readonly` ruolo sulla SVM. `fsx` In questo esempio, esistono utenti esistenti con questo ruolo.

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

Il sistema visualizza il seguente avviso a causa degli utenti esistenti:

```
Warning: User accounts with this role exist. Modifications to the username/password
 restrictions on this role could result in non-compliant user
         accounts.
Do you want to continue? {y|n}:

FsxId0123456::>
```

L'aggiornamento della password **`fsxadmin`** dell'account non riesce

Quando aggiorni la password per l'`fsxadmin`utente, potresti ricevere un errore se non soddisfa i requisiti di password impostati nel file system. È possibile visualizzare i requisiti della password utilizzando il comando `security login role config show` ONTAP CLI o API REST.

Per visualizzare i requisiti relativi alla password per un file system o un ruolo SVM

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

2. Il `security login role config show` comando restituisce i requisiti di password per un file system o un ruolo SVM.

```
FsxId0123456::> security login role config show -role fsxadmin -
fields password_requirement_fields
```

Per il `-fields` parametro, specificate uno o tutti i seguenti elementi:

- `passwd-minlength`— La lunghezza minima della password.
- `passwd-min-special-chars`— Il numero minimo di caratteri speciali nella password.
- `passwd-min-lowercase-chars`— Il numero minimo di caratteri minuscoli nella password.
- `passwd-min-uppercase-chars`— Il numero minimo di caratteri maiuscoli nella password.
- `passwd-min-digits`— Il numero minimo di cifre della password.
- `passwd-alphanum`— Informazioni sull'inclusione o l'esclusione di caratteri alfanumerici.
- `passwd-expiry-time`— L'ora di scadenza della password.
- `passwd-expiry-warn-time`— L'ora di avviso di scadenza della password.

3. Esegui il comando seguente per visualizzare tutti i requisiti relativi alla password:

```
FsxId0123456::> security login role config show -role fsxadmin -fields passwd-
minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
uppercase-chars

vserver                role     passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
---------------------- -------- ---------------- ---------------
 ------------------------ ------------------ --------------------------
 -------------------------- ----------------- ----------------------
FsxId0123456           fsxadmin 3                enabled         0
       unlimited          0                        0                         0
               unlimited
```

Migrazione ad Amazon NetApp FSx for ONTAP

Le seguenti sezioni forniscono informazioni su come migrare i file system NetApp ONTAP esistenti su Amazon FSx for ONTAP. NetApp

> **Note**
>
> Se prevedi di utilizzare la politica di `All` tiering per migrare i dati al livello del pool di capacità, tieni presente che i metadati dei file vengono sempre archiviati sul livello SSD e che tutti i nuovi dati utente vengono prima scritti sul livello SSD. Quando i dati vengono scritti sul livello SSD, il processo di tiering in background inizierà a suddividere i dati su più livelli nello storage del pool di capacità, ma il processo di suddivisione in più livelli non è immediato e consuma risorse di rete. È necessario dimensionare il livello SSD per tenere conto dei metadati dei file (3-7% delle dimensioni dei dati utente), come buffer per i dati utente prima di suddividerli su più livelli in base al pool di capacità. Ti consigliamo di non superare l'80% di utilizzo del livello SSD.
> Durante la migrazione dei dati, assicurati di monitorare il livello SSD utilizzando i parametri del CloudWatch file system per assicurarti che non si riempia più velocemente di quanto il processo di suddivisione in più livelli consenta di spostare i dati nello storage del pool di capacità.

Argomenti

Migrazione a FSx for ONTAP utilizzando NetApp SnapMirror

Puoi migrare i tuoi file system NetApp ONTAP su Amazon FSx for ONTAP utilizzando. NetApp NetApp SnapMirror

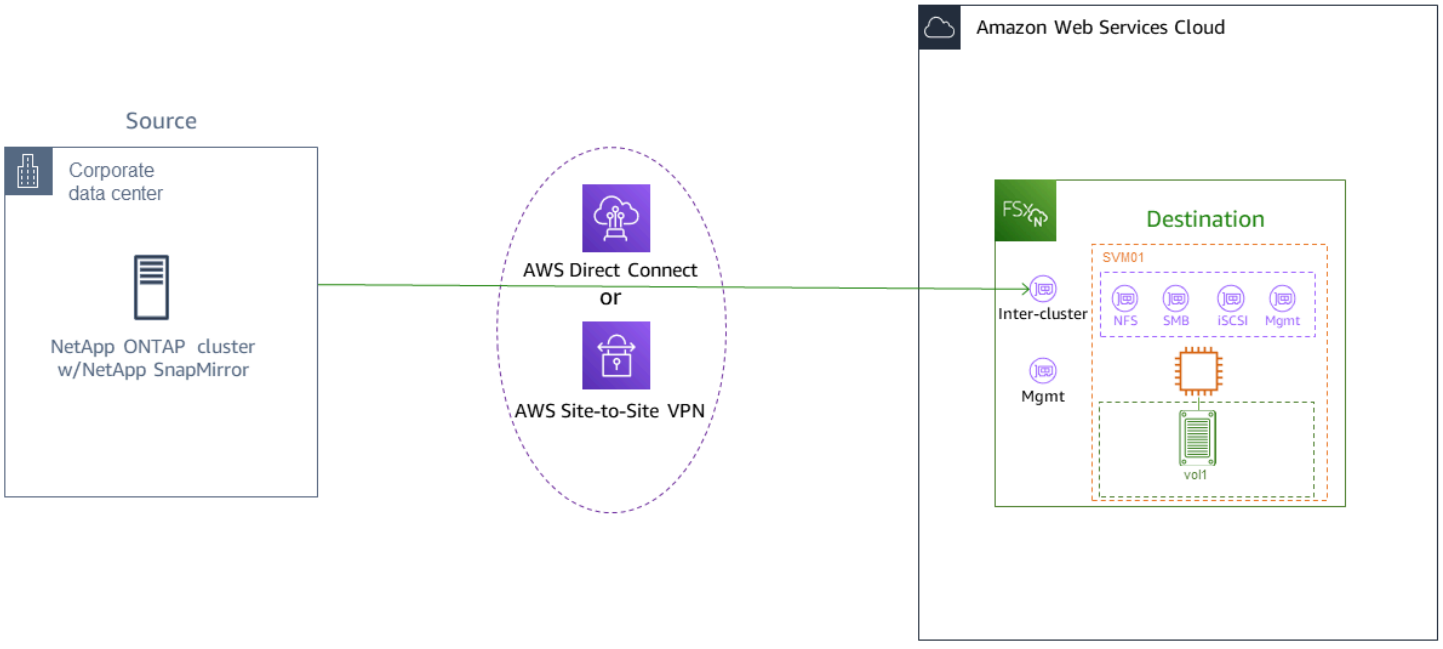
NetApp SnapMirror utilizza la replica a livello di blocco tra due file system ONTAP, replicando i dati da un volume di origine specificato a un volume di destinazione. Si consiglia di SnapMirror utilizzarlo per migrare i file system ONTAP locali su FSx for NetApp ONTAP. NetApp SnapMirrorla replica a livello di blocco è rapida ed efficiente anche per i file system con:

- Strutture di directory complesse
- Oltre 50 milioni di file
- File di dimensioni molto ridotte (dell'ordine dei kilobyte)

Quando si esegue la migrazione SnapMirror a FSx for ONTAP, i dati deduplicati e compressi rimangono in tali stati, il che riduce i tempi di trasferimento e la quantità di larghezza di banda richiesta per la migrazione. Le istantanee esistenti sui volumi ONTAP di origine vengono conservate durante la migrazione ai volumi di destinazione. La migrazione dei file system NetApp ONTAP locali a FSx for ONTAP prevede le seguenti attività di alto livello:

1. Crea il volume di destinazione in Amazon FSx.
2. Raccogli interfacce logiche di origine e destinazione (LIF).
3. Stabilisci il peering del cluster tra i file system di origine e di destinazione.
4. Crea una relazione di peering SVM.
5. Crea la relazione. SnapMirror
6. Mantieni un cluster di destinazione aggiornato.
7. Passate al file system FSx for ONTAP.

Il diagramma seguente illustra lo scenario di migrazione descritto in questa sezione.



Argomenti

Prima di iniziare

Prima di iniziare a utilizzare le procedure descritte nelle sezioni seguenti, accertatevi di aver soddisfatto i seguenti prerequisiti:

- FSx for ONTAP dà priorità al traffico client rispetto alle attività in background, tra cui la suddivisione dei dati su più livelli, l'efficienza dello storage e i backup. Durante la migrazione dei dati, e come best practice generale, consigliamo di monitorare la capacità del livello SSD per garantire che non superi l'80% di utilizzo. Puoi monitorare l'utilizzo del tuo livello SSD utilizzando le metriche del file system. CloudWatch Per ulteriori informazioni, consulta Parametri di volume.
- Se imposti la politica di suddivisione dei dati su più livelli del volume di destinazione `All` durante la migrazione dei dati, tutti i metadati dei file vengono archiviati sul livello di archiviazione SSD principale. I metadati dei file vengono sempre archiviati sul livello primario basato su SSD, indipendentemente dalla politica di suddivisione dei dati su più livelli del volume. Si consiglia di assumere un rapporto di 1:10 per livello primario: capacità, capacità di storage a livello di pool.
- I file system di origine e di destinazione sono collegati nello stesso VPC o si trovano in reti peerizzate utilizzando Amazon VPC Peering, Transit Gateway o. AWS Direct Connect AWS VPN Per ulteriori informazioni, consulta Accesso ai dati dall'interno AWS e Cos'è il peering VPC? nella Amazon VPC Peering Guide.
- Il gruppo di sicurezza VPC per il file system FSx for ONTAP dispone di regole in entrata e in uscita che consentono ICMP e TCP sulle porte 443, 10000, 11104 e 11105 per gli endpoint inter-cluster (LIF).
- Verifica che i volumi di origine e di destinazione eseguano versioni ONTAP compatibili prima di creare una relazione di protezione dei dati. NetApp SnapMirror Per ulteriori informazioni, consulta Versioni ONTAP compatibili per le SnapMirror relazioni nella documentazione per gli utenti NetApp

di ONTAP. Le procedure qui presentate utilizzano un file system NetApp ONTAP locale come sorgente.

- Il file system NetApp ONTAP locale (sorgente) include una licenza. SnapMirror
- È stato creato un file system di destinazione FSx for ONTAP con un SVM, ma non è stato creato un volume di destinazione. Per ulteriori informazioni, consulta Creazione di FSx per i file system ONTAP.

I comandi di queste procedure utilizzano i seguenti alias di cluster, SVM e volume:

- *FSx-Dest*— l'ID del cluster di destinazione (FSx) (nel formato F SxIdabcdef 1234567890a).
- *OnPrem-Source*— l'ID del cluster di origine.
- *DestSVM*— il nome SVM di destinazione.
- *SourceSVM*— il nome SVM di origine.
- Entrambi i nomi del volume di origine e di destinazione sono`vol1`.

> **Note**
>
> Un file system FSx for ONTAP viene definito cluster in tutti i comandi ONTAP CLI.

Le procedure in questa sezione utilizzano i seguenti comandi NetApp ONTAP CLI.

- comando volume create
- comandi cluster
- comandi vserver peer
- comandi snapmirror

Utilizzerai l' NetApp ONTAP CLI per creare e gestire SnapMirror una configurazione sul tuo file system FSx for ONTAP. Per ulteriori informazioni, consulta Utilizzo della CLI NetApp ONTAP.

Create il volume di destinazione

Puoi creare un volume di destinazione per la protezione dei dati (DP) utilizzando la console Amazon FSx, AWS CLI l'API Amazon FSx, oltre all'interfaccia a riga di comando di NetApp ONTAP e all'API

REST. Per informazioni sulla creazione di un volume di destinazione utilizzando la console Amazon FSx eAWS CLI, consulta. Creazione di volumi

Nella procedura seguente, si utilizzerà l' NetApp ONTAP CLI per creare un volume di destinazione sul file system FSx for ONTAP. Sono necessari la `fsxadmin` password e l'indirizzo IP o il nome DNS della porta di gestione del file system.

1. Stabilisci una sessione SSH con il file system di destinazione utilizzando l'utente `fsxadmin` e la password che hai impostato quando hai creato il file system.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Crea un volume sul cluster di destinazione con una capacità di archiviazione almeno uguale alla capacità di archiviazione del volume di origine. `-type DP`Da utilizzare per designarlo come destinazione per una SnapMirror relazione.

   Se prevedi di utilizzare il tiering dei dati, ti consigliamo di `-tiering-policy` impostarlo su. `all` In questo modo i dati vengono trasferiti immediatamente su uno storage con pool di capacità e si evita l'esaurimento della capacità del livello SSD. Dopo la migrazione, puoi passare `-tiering-policy` a. `auto`

   > **Note**
   >
   > I metadati dei file vengono sempre archiviati sul livello primario basato su SSD, indipendentemente dalla politica di suddivisione dei dati su più livelli del volume.

   ```
   FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
   type DP -tiering-policy all
   ```

Registra i LIF intercluster di origine e destinazione

SnapMirror utilizza interfacce logiche intercluster (LIF), ciascuna con un indirizzo IP univoco, per facilitare il trasferimento dei dati tra i cluster di origine e di destinazione.

1. Per i file system FSx for ONTAP di destinazione, puoi recuperare gli endpoint inter-cluster - indirizzi IP dalla console Amazon FSx accedendo alla scheda Amministrazione nella pagina dei dettagli del file system.

2. Per il cluster NetApp ONTAP di origine, recupera gli indirizzi IP LIF tra cluster utilizzando l'ONTAP CLI. Esegui il comando seguente:

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
             inter_2    up/up  10.0.1.69/24
```

> **Note**
>
> Per i file system con scalabilità orizzontale, sono disponibili due indirizzi IP intercluster per ogni coppia ad alta disponibilità (HA). Salva questi valori per utilizzarli in un secondo momento.

Salva gli indirizzi `inter_2` IP `inter_1` e. Sono referenziati in `FSx-Dest` as `dest_inter_1` `dest_inter_2` e for `OnPrem-Source` as `source_inter_1` and`source_inter_2`.

Stabilisci il peering del cluster tra origine e destinazione

Stabilisci una relazione peer del cluster sul cluster di destinazione fornendo gli indirizzi IP tra cluster. Sarà inoltre necessario creare una passphrase da inserire quando si stabilisce il peering del cluster sul cluster di origine.

1. Imposta il peering sul cluster di destinazione utilizzando il seguente comando. Per i file system con scalabilità orizzontale, è necessario fornire ogni indirizzo IP intercluster.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. Successivamente, stabilisci la relazione peer del cluster sul cluster di origine. Dovrai inserire la passphrase che hai creato sopra per autenticarti. Per i file system con scalabilità orizzontale, dovrai fornire ogni indirizzo IP intercluster.

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. Verifica che il peering sia andato a buon fine utilizzando il seguente comando sul cluster di origine. Nell'output, `Availability` dovrebbe essere impostato su. `Available`

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

Crea una relazione di peering SVM

Una volta stabilito il peering del cluster, il passaggio successivo è il peering delle SVM. Crea una relazione di peering SVM sul cluster di destinazione (FSX-Dest) utilizzando il comando. `vserver peer` Gli alias aggiuntivi utilizzati nei seguenti comandi sono i seguenti:

- `DestLocalName`— questo è il nome usato per identificare la SVM di destinazione durante la configurazione del peering SVM sulla SVM di origine.
- `SourceLocalName`— questo è il nome usato per identificare la SVM di origine durante la configurazione del peering SVM sulla SVM di destinazione.

1. Utilizzate il seguente comando per creare una relazione di peering SVM tra le SVM di origine e di destinazione.

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName

 Info: [Job 207] 'vserver peer create' job queued
```

2. Accetta la relazione di peering sul cluster di origine:

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. Verifica lo stato del peering SVM utilizzando il seguente comando; `Peer State` dovrebbe essere impostato su `peered` nella risposta.

```
OnPrem-Source::> vserver peer show

Peer    Peer     Peer   Peering  Remote
vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------ ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

Crea la relazione SnapMirror

Dopo aver effettuato il peering delle SVM di origine e di destinazione, i passaggi successivi consistono nel creare e inizializzare la SnapMirror relazione nel cluster di destinazione.

> **Note**
>
> Dopo aver creato e inizializzato una SnapMirror relazione, i volumi di destinazione sono di sola lettura fino a quando la relazione non viene interrotta.

- Utilizzare il `snapmirror create` comando per creare la SnapMirror relazione nel cluster di destinazione. Il `snapmirror create` comando deve essere utilizzato dalla SVM di destinazione.

  È possibile utilizzare facoltativamente `-throttle` per impostare la larghezza di banda massima (in KB/sec) per la relazione. SnapMirror

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
path DestSVM:vol1 -vserver DestSVM -throttle unlimited

 Operation succeeded: snapmirror create for the relationship with destination
 "DestSVM:vol1".
```

Trasferimento dei dati sul file system FSx for ONTAP

Ora che hai creato la SnapMirror relazione, puoi trasferire i dati al file system di destinazione.

1. È possibile trasferire i dati nel file system di destinazione eseguendo il comando seguente sul file system di destinazione.

   > **Note**
   >
   > Una volta eseguito questo comando, SnapMirror inizia a trasferire istantanee dei dati dal volume di origine al volume di destinazione.

   ```
   FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
   path SourceLocalName:vol1
   ```

2. Se stai migrando dati che vengono utilizzati attivamente, dovrai aggiornare il cluster di destinazione in modo che rimanga sincronizzato con il cluster di origine. Per eseguire un aggiornamento una tantum del cluster di destinazione, esegui il comando seguente.

   ```
   FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
   ```

3. È inoltre possibile pianificare aggiornamenti orari o giornalieri prima di completare la migrazione e spostare i client su FSx for ONTAP. È possibile stabilire una pianificazione degli SnapMirror aggiornamenti utilizzando il comando. `snapmirror modify`

   ```
   FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
   ```

Passaggio ad Amazon FSx

Per prepararsi al cutover del file system FSx for ONTAP, effettuate le seguenti operazioni:

- Disconnettete tutti i client che scrivono nel cluster di origine.
- Esegui un SnapMirror trasferimento finale per assicurarti che non vi sia alcuna perdita di dati durante il taglio.
- Rompete la SnapMirror relazione.
- Connect tutti i client al file system FSx for ONTAP.

1. Per garantire che tutti i dati dal cluster di origine vengano trasferiti al file system FSx for ONTAP, eseguite un trasferimento finale con Snapmirror.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. Assicurati che la migrazione dei dati sia completa verificando che `Mirror State` sia impostata su e `Relationship Status` sia impostata su. `Snapmirrored` `Idle` È inoltre necessario assicurarsi che la `Last Transfer End Timestamp` data sia quella prevista, in quanto indica quando è avvenuto l'ultimo trasferimento al volume di destinazione.

3. Eseguite il comando seguente per mostrare lo SnapMirror stato.

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      ---------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. Disabilita eventuali SnapMirror trasferimenti futuri utilizzando il `snapmirror quiesce` comando.

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. Verifica che sia `Relationship Status` passato all'`Quiescedusosnapmirror show`.

```
FSx-Dest::> snapmirror show

Source           Destination   Mirror        Relationship
Path             Path          State         Status
-----------      ------------  ------------- --------
sourcesvm1:vol1  svm01:DestVol Snapmirrored  Quiesced
```

6. Durante la migrazione, il volume di destinazione è di sola lettura. Per abilitare la lettura/scrittura, è necessario interrompere la SnapMirror relazione e passare al file system FSx for ONTAP. Interrompi la SnapMirror relazione usando il seguente comando.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. Una volta completata la SnapMirror replica e dopo aver interrotto la SnapMirror relazione, è possibile montare il volume per rendere disponibili i dati.

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

Il volume è ora disponibile con i dati dal volume di origine completamente migrati al volume di destinazione. Il volume è inoltre disponibile per la lettura e la scrittura da parte dei client. Se in precedenza hai impostato il `tiering-policy` volume `suall`, puoi cambiarlo in `auto` or `snapshot-only` e i dati passeranno automaticamente da un livello di storage all'altro in base ai modelli di accesso. Per rendere questi dati accessibili a client e applicazioni, vedereAccesso ai dati .

Migrazione a FSx for ONTAP utilizzando AWS DataSync

Consigliamo di AWS DataSync utilizzarlo per trasferire dati tra file system FSx for ONTAP e file system non ONTAP, tra cui FSx for Lustre, FSx per OpenZFS, FSx for Windows File Server, Amazon EFS, Amazon S3 e filer locali. Se trasferisci file tra FSx for ONTAP NetApp e ONTAP, ti consigliamo di utilizzare. NetApp SnapMirror AWS DataSyncè un servizio di trasferimento dati che semplifica, automatizza e accelera lo spostamento e la replica dei dati tra sistemi di storage autogestiti e servizi di archiviazione su Internet o. AWS AWS Direct Connect DataSync può trasferire i dati e i metadati del file system, come proprietà, timestamp e autorizzazioni di accesso.

È possibile utilizzarli DataSync per trasferire file tra due file system FSx for ONTAP e anche per spostare i dati su un file system di un account o diversoRegione AWS. AWS È inoltre possibile utilizzarlo DataSync con i file system FSx for ONTAP per altre attività. Ad esempio, è possibile 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.

In DataSync, una posizione è un endpoint per un file system FSx for ONTAP. Per informazioni su scenari di trasferimento specifici, consultate Lavorare con le posizioni nella Guida per l'AWS DataSyncutente.

> **Note**
>
> Se prevedi di utilizzare la politica di `All` tiering per migrare i dati al livello del pool di capacità, tieni presente che i metadati dei file vengono sempre archiviati sul livello SSD e che tutti i nuovi dati utente vengono prima scritti sul livello SSD. Quando i dati vengono scritti sul livello SSD, il processo di tiering in background inizierà a suddividere i dati su più livelli nello storage

del pool di capacità, ma il processo di suddivisione in più livelli non è immediato e consuma risorse di rete. È necessario dimensionare il livello SSD per tenere conto dei metadati dei file (3-7% delle dimensioni dei dati utente), come buffer per i dati utente prima di suddividerli su più livelli in base al pool di capacità. Si consiglia di non superare l'80% di utilizzo dell'unità SSD.
Durante la migrazione dei dati, assicurati di monitorare il livello SSD utilizzando i parametri del CloudWatch file system per assicurarti che non si riempia più velocemente di quanto il processo di suddivisione in più livelli consenta di spostare i dati nello storage del pool di capacità. Puoi anche limitare DataSync i trasferimenti a una velocità inferiore a quella di suddivisione in più livelli per garantire che il livello SSD non superi l'80% di utilizzo.
Ad esempio, per i file system con una capacità di throughput di almeno 512 MBps, un acceleratore da 200 MBps in genere bilancia le velocità di trasferimento e di suddivisione dei dati su più livelli.

Prerequisiti

Per migrare i dati nella configurazione di FSx for ONTAP, sono necessari un server e una rete che soddisfino i requisiti. DataSync Per ulteriori informazioni, consulta la sezione Requisiti DataSync nella Guida per l'AWS DataSyncutente.

Passaggi di base per la migrazione dei file tramite DataSync

Il trasferimento di file da un'origine a una destinazione utilizzando DataSync prevede i seguenti passaggi di base:

- Scaricate e installate un agente nel vostro ambiente e attivatelo (non necessario in caso di trasferimento da un ambiente all'altro). Servizi AWS
- Crea una posizione di origine e una di destinazione.
- Creare un'attività.
- Eseguire l'attività per trasferire i file dall'origine alla destinazione.

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utenteAWS DataSync:

- Trasferimento di dati tra storage autogestito e AWS
- Creazione di una posizione per Amazon FSx for ONTAP NetApp

Monitoraggio di Amazon FSx per ONTAP NetApp

Puoi utilizzare i seguenti servizi e strumenti per monitorare l'utilizzo e l'attività di Amazon FSx for NetApp ONTAP:

- Amazon CloudWatch: puoi monitorare i file system utilizzando Amazon CloudWatch, che raccoglie ed elabora automaticamente i dati grezzi da FSx for ONTAP in metriche leggibili. Queste statistiche vengono conservate per un periodo di 15 mesi in modo da poter accedere alle informazioni storiche e vedere le prestazioni del file system. Puoi anche impostare allarmi in base alle tue metriche in un periodo di tempo specificato ed eseguire una o più azioni in base al valore delle metriche relative alle soglie specificate.
- Eventi ONTAP EMS: è possibile monitorare il file system FSx for ONTAP utilizzando gli eventi generati dall'Events Management System (EMS) di ONTAP. Gli eventi EMS sono notifiche di ricorrenze nel file system, come la creazione di LUN iSCSI o il dimensionamento automatico dei volumi.
- NetApp Cloud Insights: puoi monitorare le metriche di configurazione, capacità e prestazioni per i tuoi file system FSx for ONTAP utilizzando NetApp il servizio Cloud Insights. Puoi anche creare avvisi in base a condizioni metriche.
- NetApp Harvest e NetApp Grafana: è possibile monitorare il file system FSx for ONTAP utilizzando Harvest e Grafana. NetApp NetApp NetApp Harvest monitora i file system ONTAP raccogliendo parametri relativi a prestazioni, capacità e hardware dai file system FSx for ONTAP. Grafana fornisce una dashboard in cui è possibile visualizzare le metriche Harvest raccolte.
- AWS CloudTrail— È possibile utilizzarlo AWS CloudTrail per acquisire tutte le chiamate API per Amazon FSx come eventi. Questi eventi forniscono una registrazione delle azioni intraprese da un utente, ruolo o AWS servizio in Amazon FSx.

Argomenti

Monitoraggio con Amazon CloudWatch

Puoi monitorare i file system utilizzando Amazon CloudWatch, che raccoglie ed elabora i dati grezzi da Amazon FSx NetApp for ONTAP 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 per determinare le prestazioni del file system. Per impostazione predefinita, i dati metrici di FSx for ONTAP vengono inviati automaticamente CloudWatch a periodi di 1 minuto. Per ulteriori informazioni su CloudWatch, consulta What is Amazon CloudWatch? nella Amazon CloudWatch User Guide.

> **Note**
>
> Per impostazione predefinita, FSx for ONTAP invia i dati delle metriche a periodi di 1 minuto, ad eccezione delle seguenti metriche che vengono inviate CloudWatch a intervalli di 5 minuti:
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch le metriche per FSx for ONTAP sono organizzate in quattro categorie, definite dalle dimensioni utilizzate per interrogare ciascuna metrica. Per ulteriori informazioni sulle dimensioni, consulta Dimensions nella Amazon CloudWatch User Guide.

- Metriche del file system: metriche delle ile-system-level prestazioni e della capacità di archiviazione F.
- Metriche dettagliate del file system: parametri di ile-system-level storage F per livello di storage (SSD e pool di capacità).
- Metriche del volume: metriche delle prestazioni e della capacità di archiviazione per volume.
- Metriche dettagliate sul volume: metriche della capacità di storage per volume per livello di storage o per tipo di dati (utente, snapshot o altro).

Tutte le CloudWatch metriche per FSx for ONTAP vengono pubblicate nel namespace in`AWS/FSx`. CloudWatch

Argomenti

- Come usare FSx per le metriche ONTAP CloudWatch
- Accesso alle CloudWatch metriche

- Metriche del file system
- Metriche del file system con scalabilità orizzontale
- Parametri di volume
- Avvertenze e raccomandazioni sulle prestazioni
- Creazione di CloudWatch allarmi Amazon per monitorare Amazon FSx

Come usare FSx per le metriche ONTAP CloudWatch

Le CloudWatch metriche riportate da Amazon FSx forniscono informazioni preziose sui file system e sui volumi FSx for ONTAP.

Argomenti

- Monitoraggio dei parametri del file system nella console Amazon FSx
- Monitoraggio delle metriche del volume nella console Amazon FSx

Monitoraggio dei parametri del file system nella console Amazon FSx

Puoi utilizzare il pannello Monitoraggio e prestazioni sulla dashboard del tuo file system nella console Amazon FSx per visualizzare i parametri descritti nella tabella seguente. Per ulteriori informazioni, consulta Accesso alle CloudWatch metriche.

Monitoraggio e prestazioni	Come posso...	Grafico	Parametri rilevanti
Riepilogo	... determinare la quantità di capacità di storage disponibile sul mio file system?	Capacità di archiviazione principale disponibile (byte)	`StorageCapacity {SSD} - StorageUsed {SSD}`
	... determinare il throughput totale del client del mio file system?	Throughput totale	SUM (`DataReadBytes +DataWrite`

Monitoraggio e prestazioni	Come posso...	Grafico	Parametri rilevanti
		del client (byte/sec)	`Bytes`) /PERIOD (in secondi)
	... determinare gli IOPS totali del client del mio file system?	IOPS totali del client (operazioni/sec)	SUM (`DataRead0perations + DataWriteOperations +MetadataOperations`) /PERIOD (in secondi)
	... determinare la latenza media per le operazioni di lettura, scrittura e metadati del mio file system?	Latenza media (ms/operazione)	Latenza di lettura media: * 1000/ `DataRead0perationTime DataReadOperations` Latenza media di scrittura: * 1000/ `DataWrite OperationTime DataWriteOperations` Latenza media dei metadati: * 1000/ `Metadata0perationTime MetadataOperations`

Monitoraggio e prestazioni	Come posso...	Grafico	Parametri rilevanti
Storage	... determinare la distribuzione della capacità di archiviazione utilizzata e gratuita sul mio file system?	Distribuzione dello storage	Livello primario disponibile: `StorageCapacity {SSD} - StorageUsed {SSD}` Livello primario utilizzato: `StorageUsed {SSD}` Pool di capacità utilizzato: `StorageUsed {StandardCapacityPool }`
	... determinare i risparmi derivanti dall'efficienza dello storage (compressione, deduplicazione e compattazione)?	Risparmi sull'efficienza dello storage	`StorageEfficiencySavings`
	... determinare la quantità di storage principale disponibile?	Capacità di archiviazione principale disponibile (byte)	`StorageCapacity {SSD} - StorageUsed {SSD}`
	... determinare la percentuale di storage principale utilizzato per il mio file system?	Utilizzo della capacità di storage principale (percentuale)	`StorageUsed {SSD} * 100/ StorageCapacity {} SSD`

Monitoraggio e prestazioni	Come posso...	Grafico	Parametri rilevanti
Prestazioni del file server	... determinare se il mio file system si sta avvicinando al limite di throughput di rete?	Throughput di rete: utilizzo (percentuale)	`NetworkThroughputUtilization`
	... determinare se il mio file system si sta avvicinando al limite di velocità effettiva del disco?	Velocità effettiva del disco: utilizzo (percentuale)	`FileServerDiskThroughputUtilization`
	... determinare se il mio file system ha esaurito i crediti di burst consentiti per la velocità effettiva del disco?	Velocità effettiva del disco: bilanciamento del burst (percentuale)	`FileServerDiskThroughputBalance`
	... determinare se il mio file system si sta avvicinando al limite di IOPS SSD dei relativi file server?	IOPS del disco: utilizzo (percentuale)	`FileServerDiskIopsUtilization`

Monitoraggio e prestazioni	Come posso...	Grafico	Parametri rilevanti
	... determinare se il mio file system ha esaurito i crediti burst consentiti dai file server per gli IOPS su disco SSD?	IOPS su disco: saldo del burst (percentuale)	`FileServerDiskIopsBalance`
	... determinare l'utilizzo medio della CPU del file system?	Utilizzo della CPU (percentuale)	`CPUUtilization`
	... determinare se il mio carico di lavoro utilizza in modo efficiente la RAM e le cache di lettura NVMe del mio file system?	Rapporto di accesso alla cache (percentuale)	`FileServerCacheHitRatio`
Prestazioni disco	... determinare se il mio file system si sta avvicinando alla capacità IOPS SSD attualmente fornita?	IOPS del disco: utilizzo (SSD) (percentuale)	`DiskIopsUtilization`

Note

Si consiglia di mantenere un utilizzo medio della capacità di throughput in qualsiasi dimensione correlata alle prestazioni, come l'utilizzo della rete, l'utilizzo della CPU e l'utilizzo

degli IOPS delle unità SSD, a meno del 50%. Ciò garantisce una capacità di throughput di riserva sufficiente per picchi imprevisti del carico di lavoro, nonché per qualsiasi operazione di storage in background (come la sincronizzazione dello storage, la suddivisione in più livelli dei dati o i backup).

Monitoraggio delle metriche del volume nella console Amazon FSx

Puoi visualizzare il pannello di monitoraggio sulla dashboard del tuo volume nella console Amazon FSx per visualizzare ulteriori metriche prestazionali. Per ulteriori informazioni, consulta Accesso alle CloudWatch metriche.

Monitoraggio	Come posso...	Grafico	Parametri rilevanti
	... determinare la capacità di archiviazione disponibile del mio volume?	Capacità di archiviazione disponibile	`StorageCapacity`
	... determinare il throughput totale dei client del mio volume?	Throughput totale del client (byte/sec)	SUM (`DataReadBytes +DataWriteBytes`) /PERIOD (in secondi)
	... determinare gli IOPS totali del client del mio volume?	IOPS totali del client (operazioni/sec)	SUM (`DataReadOperations + DataWriteOperations +MetadataOperations`) /PERIOD (in secondi)
	... determinare quante operazioni di lettura e scrittura provengono o vanno a finire nel livello del pool di capacità?	IOPS del pool di capacità (operazioni/sec)	Operazioni di lettura: `CapacityPoolReadOperations`

Monitoraggio	Come posso...	Grafico	Parametri rilevanti
			Operazioni di scrittura: `CapacityPoolWriteOperations`
	... determinare la latenza media per le operazioni di lettura, scrittura e metadati del mio volume?	Latenza media (ms/operazione)	Latenza di lettura media: * 1000/ `DataReadOperationTime` `DataReadOperations` Latenza media di scrittura: * 1000/ `DataWriteOperationTime` `DataWriteOperations` Latenza media dei metadati: * 1000/ `MetadataOperationTime` `MetadataOperations`
	... determinare la quantità di file o inode disponibili sul mio volume?	File disponibili (inode)	`FilesCapacity - FilesUsed`
	... determinare la distribuzione della capacità di archiviazione utilizzata e disponibile sul mio volume?	Distribuzione dello storage	`StorageCapacity - StorageUsed`

Accesso alle CloudWatch metriche

Puoi visualizzare i CloudWatch parametri Amazon per Amazon FSx nei seguenti modi:

- La console Amazon FSx
- La CloudWatch console Amazon
- Il AWS Command Line Interface (AWS CLI) per CloudWatch

- L' CloudWatch API

La procedura seguente spiega come visualizzare i CloudWatch parametri del file system con la console Amazon FSx.

Per visualizzare i CloudWatch parametri per il tuo file system utilizzando la console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli File system, quindi scegli il file system di cui desideri visualizzare le metriche.
3. Nella pagina di riepilogo, scegli Monitoraggio e prestazioni dal secondo pannello per visualizzare i grafici relativi alle metriche del 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 e le metriche di utilizzo.
- Scegli Performance per visualizzare le metriche delle prestazioni dei file server e dello storage.
- Scegli gli CloudWatch allarmi per visualizzare i grafici di tutti gli allarmi configurati per il tuo file system.

La procedura seguente spiega come visualizzare le CloudWatch metriche del volume con la console Amazon FSx.

Per visualizzare i CloudWatch parametri relativi al volume utilizzando la console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli Volumi, quindi scegli il volume di cui desideri visualizzare le metriche.
3. Nella pagina di riepilogo, scegli Monitoraggio (la scheda predefinita) dal secondo pannello per visualizzare i grafici delle metriche del volume.

La procedura seguente spiega come visualizzare le CloudWatch metriche del file system con la CloudWatch console Amazon.

Per visualizzare i parametri utilizzando la console Amazon CloudWatch

1. Nella pagina di riepilogo del tuo file system, scegli Monitoraggio e prestazioni dal secondo pannello per visualizzare i grafici relativi alle metriche del file system.
2. Scegli Visualizza nelle metriche dal menu delle azioni in alto a destra del grafico che desideri visualizzare nella CloudWatch console Amazon. Si apre la pagina Metriche nella CloudWatch console Amazon.

La procedura seguente spiega come aggiungere i parametri del file system FSx for ONTAP a un pannello di controllo nella console Amazon. CloudWatch

Per aggiungere metriche a una console Amazon CloudWatch

1. Scegli il set di parametri (Riepilogo, Storage o Performance) nel pannello Monitoraggio e prestazioni della console Amazon FSx.
2. Scegli Aggiungi alla dashboard nella parte superiore destra del pannello. Verrà aperta la CloudWatch console Amazon.
3. Seleziona una CloudWatch dashboard esistente dall'elenco o creane una nuova. Per ulteriori informazioni, consulta Using Amazon CloudWatch dashboard nella Amazon CloudWatch User Guide.

La procedura seguente spiega come accedere alle metriche del file system con. AWS CLI

Per accedere alle metriche da AWS CLI

- Utilizzate il CloudWatch comando CLI list-metrics con il parametro. `--namespace "AWS/FSx"` Per ulteriori informazioni, consulta la sezione relativa alle informazioni di riferimento ai comandi di AWS CLI.

La procedura seguente spiega come accedere alle metriche del file system con l'API. CloudWatch

Per accedere alle metriche dall'API CloudWatch

- Chiama l'operazione dell'API GetMetricStatistics. Per ulteriori informazioni, consulta Amazon CloudWatch API Reference.

Metriche del file system

Le metriche del file system Amazon FSx for NetApp ONTAP sono classificate come metriche del file system o metriche dettagliate del file system.

- Le metriche del file system sono parametri aggregati di prestazioni e storage per un singolo file system che occupano un'unica dimensione,. `FileSystemId` Queste metriche misurano le prestazioni di rete e l'utilizzo della capacità di archiviazione per il file system.
- Le metriche dettagliate del file system misurano la capacità di storage del file system e lo storage utilizzato in ogni livello di storage (ad esempio, storage SSD e storage con pool di capacità). Ogni metrica include una dimensione `FileSystemIdStorageTier`, e. `DataType`

Tieni presente quanto segue su quando Amazon FSx pubblica i punti dati per queste metriche su: CloudWatch

- Per i parametri di utilizzo (qualsiasi metrica il cui nome termina con Utilizzo, ad esempio`NetworkThroughputUtilization`), viene emesso un punto dati ogni periodo per ogni file server o aggregato attivo. Ad esempio, Amazon FSx emette una metrica al minuto per ogni file server attivo e una metrica al minuto per `FileServerDiskIopsUtilization` aggregato per. `DiskIopsUtilization`
- Per tutti gli altri parametri, viene emesso un singolo punto dati in ogni periodo, corrispondente al valore totale della metrica su tutti i file server attivi (ad esempio per i parametri dei file server) o su tutti gli aggregati (come `DataReadBytes` per i parametri di storage). `DiskReadBytes`

Argomenti

Metriche di I/O di rete

Tutte queste metriche hanno una sola dimensione,. `FileSystemId`

Parametro	Descrizione
`NetworkThroughputUtilization`	La percentuale di utilizzo del throughput di rete per il file system. La `Average` statistica è l'utilizzo medio del throughput di rete del file system in un periodo specificato. La `Minimum` statistica è l'utilizzo più basso del throughput di rete del file system in un periodo specificato. La `Maximum` statistica indica il massimo utilizzo del throughput di rete del file system in un periodo specificato. Unità: percentuale Statistiche valide:`Average`, e `Minimum` `Maximum`
`NetworkSentBytes`	Il numero di byte (I/O di rete) inviati dal file system. La `Sum` statistica è il numero totale di byte inviati dal file system in un periodo specificato. Per calcolare la velocità effettiva inviata (byte al secondo) per qualsiasi statistica, dividi la statistica per i secondi del periodo specificato. Unità: byte Statistiche valide: `Sum`
`NetworkReceivedBytes`	Il numero di byte (I/O di rete) ricevuti dal file system.

Parametro	Descrizione
	La `Sum` statistica è il numero totale di byte ricevuti dal file system in un periodo specificato. Per calcolare la velocità effettiva ricevuta (byte al secondo) per qualsiasi statistica, dividi la statistica per i secondi del periodo specificato. Unità: byte Statistiche valide: `Sum`
`DataReadBytes`	Il numero di byte (I/O di rete) generati dalle letture effettuate dai client sul file system. La `Sum` statistica è il numero totale di byte associati alle operazioni di lettura durante il periodo specificato. Per calcolare la velocità effettiva media (byte al secondo) per un periodo, dividi la `Sum` statistica per il numero di secondi nel periodo specificato. Unità: byte Statistiche valide: `Sum`
`DataWriteBytes`	Il numero di byte (I/O di rete) generati dalle scritture effettuate dai client sul file system. La `Sum` statistica è il numero totale di byte associati alle operazioni di scrittura durante il periodo specificato. Per calcolare la velocità effettiva media (byte al secondo) per un periodo, dividi la `Sum` statistica per il numero di secondi nel periodo specificato. Unità: byte Statistiche valide: `Sum`

Parametro	Descrizione
`DataReadOperations`	Il numero di operazioni di lettura (I/O di rete) dalle letture effettuate dai client al file system. La `Sum` statistica è il numero totale di operazioni di I/O avvenute in un periodo specificato. Per calcolare la media delle operazioni di lettura al secondo per un periodo, dividi la `Sum` statistica per il numero di secondi nel periodo specificato. Unità: numero Statistiche valide: `Sum`
`DataWriteOperations`	Il numero di operazioni di scrittura (I/O di rete) derivanti dalle scritture effettuate dai client sul file system. La `Sum` statistica è il numero totale di operazioni di I/O avvenute in un periodo specificato. Per calcolare la media delle operazioni di scrittura al secondo per un periodo, dividi la `Sum` statistica per il numero di secondi nel periodo specificato. Unità: numero Statistiche valide: `Sum`

Parametro	Descrizione
`MetadataOperations`	Il numero di operazioni sui metadati (I/O di rete) da parte dei client al file system. La `Sum` statistica è il numero totale di operazioni di I/O avvenute in un periodo specificato. Per calcolare la media delle operazioni sui metadati al secondo per un periodo, dividi la `Sum` statistica per il numero di secondi nel periodo specificato. Unità: numero Statistiche valide: `Sum`
`DataReadOperationTime`	La somma del tempo totale impiegato all'interno del file system per le operazioni di lettura (I/O di rete) dei client che accedono ai dati nel file system. La `Sum` statistica è il numero totale di secondi trascorsi dalle operazioni di lettura durante il periodo specificato. Per calcolare la latenza media di lettura per un periodo, dividi la `Sum` statistica per la `DataReadOperations` metrica `Sum` relativa allo stesso periodo. Unità: secondi Statistiche valide: `Sum`

Parametro	Descrizione
`DataWriteOperationTime`	La somma del tempo totale impiegato all'inter no del file system per eseguire le operazioni di scrittura (I/O di rete) dei client che accedono ai dati nel file system. La `Sum` statistica è il numero totale di secondi trascorsi dalle operazioni di scrittura durante il periodo specificato. Per calcolare la latenza media di scrittura per un periodo, dividi la `Sum` statistica per la `DataWriteOperations` metrica `Sum` relativa allo stesso periodo. Unità: secondi Statistiche valide: `Sum`
`CapacityPoolReadBytes`	Il numero di byte letti (I/O di rete) dal livello del pool di capacità del file system. Per garantire l'integrità dei dati, ONTAP esegue un'operazione di lettura sul pool di capacità immediatamente dopo l'esecuzione di un'operazione di scrittura. La `Sum` statistica è il numero totale di byte letti dal livello del pool di capacità del file system in un periodo specificato. Per calcolare i byte del pool di capacità al secondo, dividi la `Sum` statistica per i secondi in un periodo specificato. Unità: byte Statistiche valide: `Sum`

Parametro	Descrizione
`CapacityPoolReadOperations`	Il numero di operazioni di lettura (I/O di rete) dal livello del pool di capacità del file system. Ciò si traduce in una richiesta di lettura del pool di capacità. Per garantire l'integrità dei dati, ONTAP esegue un'operazione di lettura sul pool di capacità immediatamente dopo l'esecuzione di un'operazione di scrittura. La `Sum` statistica è il numero totale di operazioni di lettura dal livello del pool di capacità del file system in un periodo specificato. Per calcolare le richieste del pool di capacità al secondo, dividi la `Sum` statistica per i secondi in un periodo specificato. Unità: numero Statistiche valide: `Sum`

Parametro	Descrizione
`CapacityPoolWriteBytes`	Il numero di byte scritti (I/O di rete) nel livello del pool di capacità del file system. Per garantire l'integrità dei dati, ONTAP esegue un'operazione di lettura sul pool di capacità immediatamente dopo l'esecuzione di un'operazione di scrittura. La `Sum` statistica è il numero totale di byte scritti nel livello del pool di capacità del file system in un periodo specificato. Per calcolare i byte del pool di capacità al secondo, dividi la `Sum` statistica per i secondi in un periodo specificato. Unità: byte Statistiche valide: `Sum`

Parametro	Descrizione
`CapacityPoolWriteOperations`	Il numero di operazioni di scrittura (I/O di rete) sul file system a partire dal livello del pool di capacità. Ciò si traduce in una richiesta di scrittura. Per garantire l'integrità dei dati, ONTAP esegue un'operazione di lettura sul pool di capacità immediatamente dopo l'esecuzione di un'operazione di scrittura. La `Sum` statistica è il numero totale di operazioni di scrittura nel livello del pool di capacità del file system in un periodo specificato. Per calcolare le richieste del pool di capacità al secondo, dividi la `Sum` statistica per i secondi in un periodo specificato. Unità: numero Statistiche valide: `Sum`

Metriche del file server

Tutte queste metriche hanno una sola dimensione,. `FileSystemId`

Parametro	Descrizione
`CPUUtilization`	La percentuale di utilizzo delle risorse della CPU del file system. La `Average` statistica è l'utilizzo medio della CPU del file system in un periodo specificato. La `Minimum` statistica è l'utilizzo più basso della CPU del file system in un periodo specificato.

Parametro	Descrizione
	La `Maximum` statistica indica il massimo utilizzo della CPU del file system in un periodo specificato. Unità: percentuale Statistiche valide:`Average`,, e `Minimum` `Maximum`
`FileServerDiskThroughputUtilization`	La velocità effettiva del disco tra il file server e il livello primario, come percentuale del limite assegnato determinato dalla capacità di throughput. La `Average` statistica è la percentuale media di utilizzo della velocità effettiva del disco dei file server in un determinato periodo. La `Minimum` statistica è la percentuale più bassa di utilizzo della velocità effettiva del disco dei file server in un periodo specificato. La `Maximum` statistica indica il massimo utilizzo della velocità effettiva del disco dei file server in un periodo specificato. Unità: percentuale Statistiche valide:,, e `Average` `Minimum` `Maximum`

Parametro	Descrizione
`FileServerDiskThroughputBalance`	La percentuale di crediti burst disponibili per la velocità effettiva del disco tra il file server e il livello primario. Ciò è valido per i file system dotati di una capacità di throughput pari o inferiore a 512 MBps. La `Average` statistica è il saldo medio di burst disponibile in un determinato periodo. La `Minimum` statistica è il saldo burst minimo disponibile in un determinato periodo. La `Maximum` statistica è il saldo burst massimo disponibile in un determinato periodo. Unità: percentuale Statistiche valide:`Average`,, e `Minimum` `Maximum`

Parametro	Descrizione
`FileServerDiskIopsBalance`	La percentuale di crediti burst disponibili per gli IOPS del disco tra il file server e il livello primario. Ciò è valido per i file system dotati di una capacità di throughput pari o inferiore a 512 MBps. La `Average` statistica è il saldo medio di burst disponibile in un determinato periodo. La `Minimum` statistica è il saldo burst minimo disponibile in un determinato periodo. La `Maximum` statistica è il saldo burst massimo disponibile in un determinato periodo. Unità: percentuale Statistiche valide:`Average`,, e `Minimum` `Maximum`

Parametro	Descrizione
`FileServerDiskIopsUtilization`	La percentuale di utilizzo IOPS della capacità IOPS del disco disponibile per il file server. La `Average` statistica è l'utilizzo medio degli IOPS del disco da parte del file system in un periodo specificato. La `Minimum` statistica indica l'utilizzo minimo degli IOPS del disco da parte del file system in un periodo specificato. La `Maximum` statistica indica l'utilizzo massimo degli IOPS del disco da parte del file system in un periodo specificato. Unità: percentuale Statistiche valide:`Average`, e `Minimum` `Maximum`

Parametro	Descrizione
`FileServerCacheHitRatio`	La percentuale di tutte le richieste di lettura servite dai dati presenti nelle cache RAM e NVMe del file system. Una percentuale più alta indica che le cache di lettura del file system forniscono più letture. Unità: percentuale La `Average` statistica è la percentuale media di accessi alla cache per il file system in un periodo specificato. La `Minimum` statistica è la percentuale più bassa di accessi alla cache per il file system in un periodo specificato. La `Maximum` statistica è la percentuale più alta di accessi alla cache per il file system in un periodo specificato. Statistiche valide:`Average`,`Minimum`, e `Maximum`

Metriche di I/O del disco

Tutte queste metriche hanno un'unica dimensione,. `FileSystemId`

Parametro	Descrizione
`DiskReadBytes`	Il numero di byte (I/O del disco) di qualsiasi disco viene letto sul livello primario del file system. La `Sum` statistica è il numero totale di byte letti dal file system in un periodo specificato.

Parametro	Descrizione
	Per calcolare la velocità effettiva del disco di lettura (byte al secondo) per qualsiasi statistica, dividi la `Sum` statistica per i secondi nel periodo specificato. Unità: byte Statistiche valide: `Sum`
`DiskWriteBytes`	Il numero di byte (I/O del disco) di ogni disco in scrittura sul livello primario del file system. La `Sum` statistica è il numero totale di byte scritti dal file system in un periodo specificato. Per calcolare la velocità effettiva del disco di scrittura (byte al secondo) per qualsiasi statistic a, dividi `Sum` la statistica per i secondi nel periodo specificato. Unità: byte Statistiche valide: `Sum`

Parametro	Descrizione
`DiskIopsUtilization`	Gli IOPS del disco tra il file server e i volumi di storage, in percentuale dei livelli primari, hanno fornito il limite di IOPS del disco. La `Average` statistica è l'utilizzo medio degli IOPS del disco da parte del file system in un periodo specificato. La `Minimum` statistica indica l'utilizzo minimo degli IOPS del disco da parte del file system in un periodo specificato. La `Maximum` statistica indica l'utilizzo massimo degli IOPS del disco da parte del file system in un periodo specificato. Unità: percentuale Statistiche valide:`Average`, e `Minimum` `Maximum`
`DiskReadOperations`	Il numero di operazioni di lettura (I/O del disco) dal livello primario del file system. La `Sum` statistica è il numero totale di operazion i di lettura dal livello primario in un periodo specificato. Unità: numero Statistiche valide: `Sum`

Parametro	Descrizione
`DiskWriteOperations`	Il numero di operazioni di scrittura (I/O del disco) sul livello primario del file system. La `Sum` statistica è il numero totale di operazioni di scrittura sul livello primario in un periodo specificato. Unità: numero Statistiche valide: `Sum`

Parametri della capacità di archiviazione

Tutte queste metriche hanno un'unica dimensione,. `FileSystemId`

Parametro	Descrizione
`StorageEfficiencySavings`	I byte salvati dalle funzionalità di efficienza dello storage (compressione, deduplicazione e compattazione). La `Average` statistica è il risparmio medio in termini di efficienza dello storage in un determinato periodo. Per calcolare il risparmio in termini di efficienza dello storage come percentuale di tutti i dati archiviati, su un periodo di un minuto, dividi `StorageEfficiencySavings` per la somma di `StorageEfficiencySavings` e per la metrica del `StorageUsed` file system, utilizzando la `Sum` statistica per. `StorageUsed` La `Minimum` statistica è il risparmio minimo in termini di efficienza di archiviazione in un periodo specificato.

Parametro	Descrizione
	La `Maximum` statistica rappresenta il massimo risparmio in termini di efficienza di archiviazione in un determinato periodo. Unità: byte Statistiche valide: `AverageMinimum`, e `Maximum`
`StorageUsed`	La quantità totale di dati fisici archiviati nel file system, sia sul livello primario (SSD) che sul livello del pool di capacità. Questa metrica include i risparmi derivanti da funzionalità di efficienza dello storage, come la compressione e la deduplicazione dei dati. Unità: byte Statistiche valide:, e `Average` `Minimum` `Maximum`

Parametro	Descrizione
`LogicalDataStored`	La quantità totale di dati logici archiviati nel file system, considerando sia il livello SSD che il livello del pool di capacità. Questa metrica include la dimensione logica totale delle istantanee e FlexClones, a titolo esemplificativo, i risparmi in termini di efficienza di storage ottenuti tramite compressione, compattazione e deduplicazione. Per calcolare i risparmi in termini di efficienza dello storage in byte, prendete il valore `Average` dell'o in un determinato periodo e `StorageUsed` sottraetelo dal risultato ottenuto nello stesso periodo. `Average` `LogicalDataStored` Per calcolare i risparmi in termini di efficienza dello storage come percentuale della dimensione totale dei dati logici, prendiamo il valore di in un determinato periodo e lo `Average` `StorageUsed` sottraiamo dal risultato ottenuto nello stesso periodo. `Average` `LogicalDataStored` Quindi dividi la differenza per il o nello stesso periodo`Average`. `LogicalDataStored` Unità: byte Statistiche valide:`Average`,`Minimum`, e `Maximum`

Metriche dettagliate del file system

Le metriche dettagliate del file system sono metriche dettagliate sull'utilizzo dello storage per ciascuno dei livelli di storage. Le metriche dettagliate del file system hanno tutte le dimensioni, e. `FileSystemId` `StorageTier` `DataType`

- La `StorageTier` dimensione indica il livello di archiviazione misurato dalla metrica, con i possibili valori di `SSD` e. `StandardCapacityPool`
- La `DataType` dimensione indica il tipo di dati misurati dalla metrica, con il valore possibile. `All`

Esiste una riga per ogni combinazione univoca di una determinata coppia chiave-valore metrica e dimensionale, con una descrizione di ciò che misura quella combinazione.

Parametro	Descrizione
`StorageCapacityUtilization`	L'utilizzo della capacità di archiviazione per ciascuno degli aggregati del file system. Ogni minuto viene emessa una metrica per ogni aggregato del file system. La `Average` statistica è la quantità media di utilizzo della capacità di storage per il livello di prestazioni del file system nel periodo specifica to. La `Minimum` statistica è la quantità più bassa di utilizzo della capacità di storage per il livello di prestazioni del file system nel periodo specifica to. La `Maximum` statistica è la quantità massima di utilizzo della capacità di storage per il livello di prestazioni del file system nel periodo specifica to. Unità: percentuale

Parametro	Descrizione
	Statistiche valide:`Average`,, e `Minimum` `Maximum`
`StorageCapacity`	La capacità di archiviazione totale del livello primario (SSD). Unità: byte Statistiche valide: `Maximum`

Parametro	Descrizione
`StorageUsed`	La capacità di archiviazione fisica utilizzata, espressa in byte, specifica per il livello di storage. Questo valore include i risparmi derivanti da funzionalità di efficienza dello storage, come la compressione e la deduplicazione dei dati. I valori di dimensione validi per `StorageTier` sono `SSD` e `StandardCapacityPool`, corrispondenti al livello di archiviazione misurato da questa metrica. Questa metrica richiede anche la `DataType` dimensione con il valore. `All` Le `Maximum` statistiche `Average` `Minimum`, e si riferiscono al consumo di storage per livello in byte per il periodo specificato. Per calcolare l'utilizzo della capacità di archiviazione del livello di storage principale (SSD), dividi tutte queste statistiche per lo stesso periodo, con la dimensione uguale a. `Maximum` `StorageCapacity` `StorageTier` `SSD` Per calcolare la capacità di archiviazione gratuita del livello di storage primario (SSD) in byte, sottrai tutte queste statistiche relative allo stesso periodo, con la dimensione uguale a. `Maximum` `StorageCapacity` `StorageTier` `SSD` Unità: byte Statistiche valide:`Average`, e `Minimum` `Maximum`

Metriche del file system con scalabilità orizzontale

Le seguenti metriche sono fornite per i file system FSx for ONTAP con due o più coppie ad alta disponibilità (HA). Per le metriche, viene emesso un datapoint per ogni coppia HA e per ogni aggregato (per i parametri di utilizzo dello storage).

> **Note**
>
> Se disponi di un file system con più coppie HA, puoi anche utilizzare le metriche del file system a coppia singola e le metriche del volume.

Argomenti

Metriche di I/O di rete

Tutte queste metriche assumono due dimensioni, e. `FileSystemId` `FileServer`

- `FileSystemId`— ID di AWS risorsa del file system.
- `FileServer`— Il nome di un file server (o nodo) in ONTAP (ad esempio,`FsxId01234567890abcdef-01`). I file server con numeri dispari sono file server preferiti (ovvero gestiscono il traffico a meno che il file system non abbia effettuato il failover sul file server secondario), mentre i file server con numero pari sono file server secondari (ovvero servono il traffico solo quando il partner non è disponibile). Per questo motivo, i file server secondari in genere mostrano un utilizzo inferiore rispetto ai file server preferiti.

Parametro	Descrizione
`NetworkThroughputUtilization`	Utilizzo del throughput di rete come percentua le del throughput di rete disponibile per il file system. Questa metrica è equivalente al valore massimo `NetworkSentBytes` e `NetworkRe`

Parametro	Descrizione
	`ceivedBytes` in percentuale della capacità di trasmissione di rete di una coppia HA per il file system. In questa metrica viene preso in considerazione tutto il traffico, incluse le attività in background (ad esempio SnapMirror, tiering e backup). Ogni minuto viene emessa una metrica per ogni file server del file system. La `Average` statistica è l'utilizzo medio del throughput di rete per un determinato file server nel periodo specificato. La `Minimum` statistica è l'utilizzo più basso del throughput di rete per il file server specificato nell'arco di un minuto, per il periodo specificato. La `Maximum` statistica è l'utilizzo massimo del throughput di rete per il file server specificato nell'arco di un minuto, per il periodo specificato. Unità: percentuale Statistiche valide:`Average`,, e `Minimum` `Maximum`

Parametro	Descrizione
`NetworkSentBytes`	Il numero di byte (IO di rete) inviati dal file system. In questa metrica viene considerato tutto il traffico, incluse le attività in backgroun d (ad esempio SnapMirror, tiering e backup). Ogni minuto viene emessa una metrica per ogni file server del file system. La `Sum` statistica è il numero totale di byte inviati in rete dal file server specificato nel periodo specificato. La `Average` statistica è il numero medio di byte inviati in rete dal file server specificato nel periodo specificato. La `Minimum` statistica è il numero più basso di byte inviati in rete dal file server specificato nel periodo specificato. La `Maximum` statistica è il numero massimo di byte inviati in rete dal file server 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`,, e `Average` `Minimum` `Maximum`

Parametro	Descrizione
`NetworkReceivedBytes`	Il numero di byte (IO di rete) ricevuti dal file system. In questa metrica viene considerato tutto il traffico, incluse le attività in backgroun d (ad esempio SnapMirror, tiering e backup). Ogni minuto viene emessa una metrica per ogni file server del file system. La `Sum` statistica è il numero totale di byte ricevuti in rete dal file server specificato nel periodo specificato. La `Average` statistica è il numero medio di byte ricevuti in rete dal file server specificato ogni minuto nel periodo specificato. La `Minimum` statistica è il numero più basso di byte ricevuti in rete dal file server specificato ogni minuto nel periodo specificato. La `Maximum` statistica è il numero massimo di byte ricevuti in rete dal file server specificato ogni minuto nel periodo specificato. Per calcolare la velocità effettiva ricevuta (byte al secondo) per qualsiasi statistica, dividi la statistica per i secondi del periodo. Unità: byte Statistiche valide:`Sum`,, e `Average` `Minimum` `Maximum`

Metriche dei file server

Tutte queste metriche assumono due dimensioni, `FileSystemId` e. `FileServer`

Parametro	Descrizione
`CPUUtilization`	La percentuale di utilizzo delle risorse della CPU del file system. Ogni minuto viene emessa una metrica per ogni file server del file system. La `Average` statistica è l'utilizzo medio della CPU del file system in un periodo specificato. La `Minimum` statistica è l'utilizzo più basso della CPU per il file server specificato nel periodo specificato. La `Maximum` statistica è l'utilizzo massimo della CPU per il file server specificato nel periodo specificato. Unità: percentuale Statistiche valide:`Average`,, e `Minimum` `Maximum`
`FileServerDiskThroughputUtilization`	La velocità effettiva del disco tra il file server e l'aggregato, come percentuale del limite fornito determinato dalla capacità di throughput. In questa metrica viene considerato tutto il traffico, incluse le attività in background (ad esempio SnapMirror, tiering e backup). Questa metrica è equivalente alla somma `DiskReadBytes` e `DiskWriteBytes` in percentuale della capacità di throughput su disco del file server di una coppia HA per il file system. Ogni minuto viene emessa una metrica per ogni file server del file system. La `Average` statistica è l'utilizzo medio della velocità effettiva del disco del file server per un determinato file server nel periodo specificato.

Parametro	Descrizione
	La `Minimum` statistica è l'utilizzo più basso della velocità effettiva del disco del file server per un determinato file server nel periodo specificato. La `Maximum` statistica è l'utilizzo più elevato della velocità effettiva del disco del file server per un determinato file server nel periodo specificato. Unità: percentuale Statistiche valide:`Average`,, e `Minimum` `Maximum`

Parametro	Descrizione
`FileServerDiskIopsUtilization`	L'utilizzo IOPS della capacità IOPS disponibi le su disco per il file server, come percentua le del limite IOPS del disco. Ciò si differenz ia dal `DiskIopsUtilization` fatto che l'utilizzo degli IOPS del disco supera il limite massimo che il file server è in grado di gestire, rispetto agli IOPS del disco assegnati. In questa metrica viene considerato tutto il traffico, incluse le attività in background (ad esempio SnapMirror, tiering e backup). Ogni minuto viene emessa una metrica per ogni file server del file system. La `Average` statistica è l'utilizzo medio degli IOPS del disco per un determinato file server nel periodo specificato. La `Minimum` statistica è l'utilizzo IOPS del disco più basso per il file server specificato nel periodo specificato. La `Maximum` statistica è l'utilizzo massimo di IOPS del disco per il file server specificato nel periodo specificato. Unità: percentuale Statistiche valide:`Average`, e `Minimum` `Maximum`

Parametro	Descrizione
`FileServerCacheHitRatio`	La percentuale di tutte le richieste di lettura fornite dai dati che risiedono nella RAM o nelle cache NVMe del file system per ciascuna delle coppie HA (ad esempio, il file server attivo in una coppia HA). Una percentuale più alta indica un rapporto più elevato tra le letture memorizza te nella cache e le letture totali. Vengono presi in considerazione tutti gli I/O, incluse le attività in background (come la suddivisione in più livelli SnapMirror e i backup). Ogni minuto viene emessa una metrica per ogni file server del file system. Unità: percentuale La `Average` statistica è il rapporto medio di accessi alla cache per una delle coppie HA del file system nel periodo specificato. La `Minimum` statistica è il rapporto di accessi alla cache più basso per una delle coppie HA del file system nel periodo specificato. La `Maximum` statistica è il rapporto di accessi alla cache più elevato per una delle coppie HA del file system nel periodo specificato. Statistiche valide:`Average`,`Minimum`, e `Maximum`

Metriche di I/O del disco

Tutte queste metriche hanno due dimensioni e. `FileSystemId` `Aggregate`

- `FileSystemId`— ID di AWS risorsa del file system.

- `Aggregate`— Il livello di prestazioni del file system è costituito da più pool di storage denominati aggregati. Esiste un aggregato per ogni coppia HA. Ad esempio, aggrega `aggr1` le mappe al file server `FsxId01234567890abcdef-01` (il file server attivo) e al file server `FsxId01234567890abcdef-02` (il file server secondario) in una coppia HA.

Parametro	Descrizione
`DiskReadBytes`	Il numero di byte (I/O del disco) di ogni disco letti da questo aggregato. In questa metrica viene considerato tutto il traffico, incluse le attività in background (ad esempio SnapMirro r, tiering e backup). Ogni minuto viene emessa una metrica per ogni aggregato del file system. La `Sum` statistica è il numero totale di byte letti ogni minuto dall'aggregato specificato nel periodo specificato. La `Average` statistica è il numero medio di byte letti ogni minuto dall'aggregato dato nel periodo specificato. La `Minimum` statistica è il numero più basso di byte letti ogni minuto dall'aggregato dato nel periodo specificato. La `Maximum` statistica è il numero massimo di byte letti ogni minuto dall'aggregato dato 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`

Parametro	Descrizione
`DiskWriteBytes`	Il numero di byte (I/O del disco) di ogni disco in scrittura su questo aggregato. In questa metrica viene considerato tutto il traffico, incluse le attività in background (ad esempio SnapMirro r, tiering e backup). Ogni minuto viene emessa una metrica per ogni aggregato del file system. La `Sum` statistica è il numero totale di byte scritti nell'aggregato specificato nel periodo specifica to. La `Average` statistica è il numero medio di byte scritti nell'aggregato dato ogni minuto nel periodo specificato. La `Minimum` statistica è il numero più basso di byte scritti nell'aggregato dato ogni minuto nel periodo specificato. La `Maximum` statistica è il numero massimo di byte scritti nell'aggregato dato ogni minuto nel periodo specificato. Per calcolare la velocità effettiva del disco di scrittura (byte al secondo) per qualsiasi statistic a, dividi la statistica per i secondi nel periodo specificato. Unità: byte Statistiche valide:`Sum`,, e `Average` `Minimum` `Maximum`

Parametro	Descrizione
`DiskIopsUtilization`	L'utilizzo di IOPS su disco di un aggregato , come percentuale del limite IOPS su disco dell'aggregato (ovvero, gli IOPS totali del file system diviso per il numero di coppie HA del file system). Ciò differisce dal `FileServe rDiskIopsUtilization` fatto che si tratta dell'utilizzo degli IOPS su disco assegnati rispetto al limite di IOPS assegnato, rispetto al limite massimo di IOPS del disco supportat o dal file server (ovvero, dettato dalla capacità di throughput configurata per coppia HA). In questa metrica viene considerato tutto il traffico, incluse le attività in background (ad esempio, tiering e backup). SnapMirror Ogni minuto viene emessa una metrica per ogni aggregato del file system. La `Average` statistica è l'utilizzo medio degli IOPS del disco per un dato aggregato nel periodo specificato. La `Minimum` statistica è l'utilizzo più basso degli IOPS del disco per un dato aggregato nel periodo specificato. La `Maximum` statistica è il massimo utilizzo di IOPS del disco per un dato aggregato nel periodo specificato. Unità: percentuale Statistiche valide:, e `Average` `Minimum` `Maximum`

Parametro	Descrizione
`DiskReadOperations`	Il numero di operazioni di lettura (IO del disco) su questo aggregato. In questa metrica viene considerato tutto il traffico, incluse le attività in background (ad esempio SnapMirror, tiering e backup). Ogni minuto viene emessa una metrica per ogni aggregato del file system. La `Sum` statistica è il numero totale di operazioni di lettura eseguite dall'aggregato specificato nel periodo specificato. La `Average` statistica è il numero medio di operazioni di lettura eseguite ogni minuto dall'aggregato dato nel periodo specificato. La `Minimum` statistica è il numero più basso di operazioni di lettura eseguite ogni minuto dall'aggregato dato nel periodo specificato. La `Maximum` statistica è il numero massimo di operazioni di lettura eseguite ogni minuto dall'aggregato dato 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 (IO del disco) su questo aggregato. In questa metrica viene considerato tutto il traffico, incluse le attività in background (ad esempio SnapMirro r, tiering e backup). Ogni minuto viene emessa una metrica per ogni aggregato del file system. La `Sum` statistica è il numero totale di operazion i di scrittura eseguite dall'aggregato specificato nel periodo specificato. La `Average` statistica è il numero medio di operazioni di scrittura eseguite ogni minuto dall'aggregato dato 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: e `Sum` `Average`

Metriche dettagliate del file system

Le metriche dettagliate del file system sono metriche dettagliate sull'utilizzo dello storage per ciascuno dei livelli di storage. Le metriche dettagliate del file system hanno le dimensioni`FileSystemId`,, e oppure le `DataType` dimensioni`StorageTier`,, and. `FileSystemId` `StorageTier` `DataType` `Aggregate`

- Quando la `Aggregate` dimensione non viene fornita, le metriche si riferiscono all'intero file system. Le `StorageCapacity` metriche `StorageUsed` and hanno un singolo punto dati ogni minuto corrispondente allo storage totale consumato dal file system (per livello di storage) e alla capacità di archiviazione totale (per il livello SSD). Nel frattempo, la `StorageCapacityUtilization` metrica emette una metrica ogni minuto per ogni aggregato.
- Quando viene fornita la `Aggregate` dimensione, le metriche si riferiscono a ciascun aggregato.

Il significato delle dimensioni è il seguente:

- `FileSystemId`— ID di AWS risorsa del file system.
- `Aggregate`— Il livello di prestazioni del file system è costituito da più pool di storage denominati aggregati. Esiste un aggregato per ogni coppia HA. Ad esempio, aggrega `aggr1` le mappe al file server `FsxId01234567890abcdef-01` (il file server attivo) e al file server `FsxId01234567890abcdef-02` (il file server secondario) in una coppia HA.
- `StorageTier`— Indica il livello di storage misurato dalla metrica, con i possibili valori di `SSD` e. `StandardCapacityPool`
- `DataType`— Indica il tipo di dati misurati dalla metrica, con il valore possibile. `All`

Esiste una riga per ogni combinazione univoca di una determinata coppia chiave-valore metrica e dimensionale, con una descrizione di ciò che misura quella combinazione.

Parametro	Descrizione
`StorageCapacityUtilization`	L'utilizzo della capacità di archiviazione per un determinato aggregato di file system. Ogni minuto viene emessa una metrica per ogni aggregato del file system. La `Average` statistica è la quantità media di utilizzo della capacità di storage per un dato aggregato nel periodo specificato. La `Minimum` statistica è la quantità minima di utilizzo della capacità di storage per un dato aggregato nel periodo specificato. La `Maximum` statistica è la quantità massima di utilizzo della capacità di storage per un dato aggregato nel periodo specificato. Unità: percentuale Statistiche valide:`Average`,, e `Minimum` `Maximum`

Parametro	Descrizione
`StorageCapacity`	La capacità di archiviazione per un determina to aggregato di file system. Ogni minuto viene emessa una metrica per ogni aggregato del file system. La `Average` statistica è la quantità media di capacità di archiviazione per un dato aggregato nel periodo specificato. La `Minimum` statistica è la quantità minima di capacità di archiviazione per un dato aggregato nel periodo specificato. La `Maximum` statistica è la quantità massima di capacità di archiviazione per un dato aggregato nel periodo specificato. Unità: byte Statistiche valide:`Average`, e `Minimum` `Maximum`

Parametro	Descrizione
`StorageUsed`	La capacità di archiviazione fisica utilizzata, espressa in byte, specifica per il livello di storage. Questo valore include i risparmi derivanti da funzionalità di efficienza dello storage, come la compressione e la deduplicazione dei dati. I valori di dimensione validi per `StorageTier` sono `SSD` e `StandardCapacityPool`, corrispondenti al livello di archiviazione misurato da questa metrica. Ogni minuto viene emessa una metrica per ogni aggregato del file system. La `Average` statistica è la quantità media di capacità di storage fisica consumata su un determinato livello di storage da un dato aggregato nel periodo specificato. La `Minimum` statistica è la quantità minima di capacità di storage fisica consumata su un determinato livello di storage da un dato aggregato nel periodo specificato. La `Maximum` statistica è la quantità massima di capacità di storage fisica consumata su un determinato livello di storage dal dato aggregato nel periodo specificato. Unità: byte Statistiche valide:`Average`, e `Minimum` `Maximum`

Parametri di volume

Il file system Amazon FSx for NetApp ONTAP può avere uno o più volumi per archiviare i dati. Ciascuno di questi volumi ha una serie di parametri, classificati come metriche di volume o metriche di volume dettagliate.

- Le metriche di volume sono metriche di prestazioni e archiviazione per volume che assumono due dimensioni, e. `FileSystemId` `VolumeId` `FileSystemId`mappa il file system a cui appartiene il volume.
- Le metriche dettagliate sul volume sono per-storage-tier metriche che misurano il consumo di storage per livello con la `StorageTier` dimensione (con i possibili valori di `SSD` and`StandardCapacityPool`) e per tipo di dati con la `DataType` dimensione (con i possibili valori di `UserSnapshot`, e`Other`). Queste metriche hanno le dimensioni`FileSystemId`, `VolumeId``StorageTier`, e. `DataType`

Argomenti

Metriche di I/O di rete

Tutte queste metriche assumono due dimensioni, e. `FileSystemId` `VolumeId`

Parametro	Descrizione
`DataReadBytes`	Il numero di byte (I/O di rete) letti dal volume dai client. La `Sum` statistica è il numero totale di byte associati alle operazioni di lettura durante il periodo specificato. Per calcolare la velocità effettiva media (byte al secondo) per un periodo, dividi la `Sum` statistica per il numero di secondi nel periodo specificato. Unità: byte

Parametro	Descrizione
	Statistiche valide: `Sum`
`DataWriteBytes`	Il numero di byte (I/O di rete) scritti nel volume dai client. La `Sum` statistica è il numero totale di byte associati alle operazioni di scrittura durante il periodo specificato. Per calcolare la velocità effettiva media (byte al secondo) per un periodo, dividi la `Sum` statistica per il numero di secondi nel periodo specificato. Unità: byte Statistiche valide: `Sum`
`DataReadOperations`	Il numero di operazioni di lettura (I/O di rete) sul volume per client. La `Sum` statistica è il numero totale di operazion i di lettura durante il periodo specificato. Per calcolare la media delle operazioni di lettura al secondo per un periodo, dividi la `Sum` statistica per il numero di secondi nel periodo specificato. Unità: numero Statistiche valide: `Sum`

Parametro	Descrizione
`DataWriteOperations`	Il numero di operazioni di scrittura (I/O di rete) sul volume per client. La `Sum` statistica è il numero totale di operazioni di scrittura durante il periodo specificato. Per calcolare la media delle operazioni di scrittura al secondo per un periodo, dividi la `Sum` statistica per il numero di secondi nel periodo specificato. Unità: numero Statistiche valide: `Sum`
`MetadataOperations`	Il numero di operazioni di I/O (I/O di rete) dalle attività di metadati da parte dei client al volume. La `Sum` statistica è il numero totale di operazioni sui metadati durante il periodo specificato. Per calcolare la media delle operazioni sui metadati al secondo per un periodo, dividi la `Sum` statistica per il numero di secondi nel periodo specificato. Unità: numero Statistiche valide: `Sum`

Parametro	Descrizione
`DataReadOperationTime`	La somma del tempo totale impiegato all'inter no del volume per le operazioni di lettura (I/O di rete) dei client che accedono ai dati nel volume. La `Sum` statistica è il numero totale di secondi trascorsi dalle operazioni di lettura durante il periodo specificato. Per calcolare la latenza media di lettura per un periodo, dividi la `Sum` statistica per la `DataReadOperations` metrica `Sum` relativa allo stesso periodo. Unità: secondi Statistiche valide: `Sum`
`DataWriteOperationTime`	La somma del tempo totale impiegato all'inter no del volume per eseguire le operazioni di scrittura (I/O di rete) dei client che accedono ai dati del volume. La `Sum` statistica è il numero totale di secondi trascorsi dalle operazioni di scrittura durante il periodo specificato. Per calcolare la latenza media di scrittura per un periodo, dividi la `Sum` statistica per la `DataWriteOperations` metrica `Sum` relativa allo stesso periodo. Unità: secondi Statistiche valide: `Sum`

Parametro	Descrizione
`MetadataOperationTime`	La somma del tempo totale impiegato all'inter no del volume per eseguire le operazioni sui metadati (I/O di rete) dei client che accedono ai dati del volume. La `Sum` statistica è il numero totale di secondi trascorsi dalle operazioni di lettura durante il periodo specificato. Per calcolare la latenza media per un periodo, dividi la `Sum` statistic a per la `Sum` dello stesso `MetadataO perations` periodo. Unità: secondi Statistiche valide: `Sum`
`CapacityPoolReadBytes`	Il numero di byte letti (I/O di rete) dal livello del pool di capacità del volume. Per garantire l'integrità dei dati, ONTAP esegue un'operazione di lettura sul pool di capacità immediatamente dopo l'esecuzione di un'operazione di scrittura. La `Sum` statistica è il numero totale di byte letti dal livello del pool di capacità del volume in un periodo specificato. Per calcolare i byte del pool di capacità al secondo, dividi la `Sum` statistica per i secondi in un periodo specificato. Unità: byte Statistiche valide: `Sum`

Parametro	Descrizione
`CapacityPoolReadOperations`	Il numero di operazioni di lettura (I/O di rete) dal livello del pool di capacità del volume. Ciò si traduce in una richiesta di lettura del pool di capacità. Per garantire l'integrità dei dati, ONTAP esegue un'operazione di lettura sul pool di capacità immediatamente dopo l'esecuzione di un'operazione di scrittura. La `Sum` statistica è il numero totale di operazioni di lettura dal livello del pool di capacità del volume in un periodo specificato. Per calcolare le richieste del pool di capacità al secondo, dividi la `Sum` statistica per i secondi in un periodo specificato. Unità: numero Statistiche valide: `Sum`

Parametro	Descrizione
`CapacityPoolWriteBytes`	Il numero di byte scritti (I/O di rete) nel livello del pool di capacità del volume. Per garantire l'integrità dei dati, ONTAP esegue un'operazione di lettura sul pool di capacità immediatamente dopo l'esecuzione di un'operazione di scrittura. La `Sum` statistica è il numero totale di byte scritti nel livello del pool di capacità del volume in un periodo specificato. Per calcolare i byte del pool di capacità al secondo, dividi la `Sum` statistica per i secondi in un periodo specificato. Unità: byte Statistiche valide: `Sum`
`CapacityPoolWriteOperations`	Il numero di operazioni di scrittura (I/O di rete) sul volume dal livello del pool di capacità. Ciò si traduce in una richiesta di scrittura. Per garantire l'integrità dei dati, ONTAP esegue un'operazione di lettura sul pool di capacità immediatamente dopo l'esecuzione di un'operazione di scrittura. La `Sum` statistica è il numero totale di operazion i di scrittura nel livello del pool di capacità del volume in un periodo specificato. Per calcolare le richieste del pool di capacità al secondo, dividi la `Sum` statistica per i secondi in un periodo specificato. Unità: numero Statistiche valide: `Sum`

Parametri della capacità di archiviazione

Tutte queste metriche hanno due dimensioni, `FileSystemId` e. `VolumeId`

Parametro	Descrizione
`StorageCapacity`	La dimensione del volume in byte. Unità: byte Statistiche valide: `Maximum`
`StorageUsed`	La capacità di archiviazione logica utilizzata del volume. Unità: byte Statistiche valide: `AverageMinimum`, e `Maximum`
`StorageCapacityUtilization`	L'utilizzo della capacità di archiviazione del volume. Unità: percentuale Statistiche valide: `Average`
`FilesUsed`	I file utilizzati (numero di file o inode) sul volume. Unità: numero Statistiche valide: `AverageMinimum`, e `Maximum`
`FilesCapacity`	Il numero totale di inode che possono essere creati sul volume. Unità: numero Statistiche valide: `Maximum`

Metriche dettagliate del volume

Le metriche dettagliate sul volume richiedono più dimensioni rispetto alle metriche di volume, consentendo misurazioni più granulari dei dati. Tutte le metriche dettagliate sul volume hanno le dimensioni`FileSystemId`,, e`VolumeId`. `StorageTier` `DataType`

- La `StorageTier` dimensione indica il livello di archiviazione misurato dalla metrica, con i possibili valori di `AllSSD`, e. `StandardCapacityPool`
- La `DataType` dimensione indica il tipo di dati misurati dalla metrica, con i possibili valori di`All`, `UserSnapshot`, e. `Other`

La tabella seguente definisce le misure `StorageUsed` metriche per le dimensioni elencate.

Parametro	Descrizione
`StorageUsed`	La quantità di spazio logico utilizzato, in byte. Questa metrica misura diversi tipi di consumo di spazio a seconda delle dimension i utilizzate con questa metrica. Quando si imposta `StorageTier` su `SSD` o `StandardC apacityPool` e si imposta `DataType` su`All`, questa metrica misura l'utilizzo dello spazio logico per questo volume rispettiv amente per i livelli SSD e del pool di capacità. Quando si imposta la `DataType` dimensione su `UserSnapshot`, o e si imposta `StorageTi er` su `OtherAll`, questa metrica misura l'utilizzo dello spazio logico per ogni rispettiv o tipo di dati. Il consumo di `Snapshot` dati include la riserva di istantanee, che per impostazione predefinita corrisponde al 5% della dimensione del volume. Unità: byte Statistiche valide: `AverageMinimum`, e `Maximum`

Parametro	Descrizione
`StorageCapacityUtilization`	La percentuale di spazio fisico su disco utilizzato dal volume. Unità: percentuale Statistiche valide: `Maximum`

Avvertenze e raccomandazioni sulle prestazioni

FSx for ONTAP visualizza un avviso per le CloudWatch metriche ogni volta che 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 del pannello di controllo Monitoraggio e prestazioni. Tutti gli avvisi sulle prestazioni di Amazon FSx attivi o recenti e tutti gli CloudWatch allarmi configurati per il file system che si trovano in uno stato ALARM 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.

Puoi creare CloudWatch allarmi per qualsiasi metrica di Amazon FSx. Per ulteriori informazioni, consulta Creazione di CloudWatch allarmi Amazon per monitorare Amazon FSx.

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. Questi consigli descrivono come affrontare un potenziale problema di prestazioni. È possibile eseguire l'azione consigliata se si prevede che l'attività continui o se ciò influisce sulle prestazioni del file system. A seconda del parametro che ha generato un avviso, puoi risolverlo aumentando la capacità di trasmissione o la capacità di archiviazione del file system, come descritto nella tabella seguente.

Sezione Dashboard	Se è presente un avviso per questa metrica	Esegui questa operazione
Storage	Utilizzo della capacità di storage principale	Aumenta la capacità di archiviazione principale del file system se il file system non ha già raggiunto la

Sezione Dashboard	Se è presente un avviso per questa metrica	Esegui questa operazione
		capacità di archiviazione SSD massima. Per ulteriori informazioni, consulta Modifica della capacità di archiviazione SSD e degli IOPS assegnati. Se il file system ha più coppie HA e l'utilizzo della capacità di storage principale è maggiore solo per un sottoinsieme degli aggregati del file system (i pool di storage che costituiscono il livello di storage principal e), è possibile anche ribilanciare il carico di lavoro in modo che l'utilizzo della capacità di storage principale sia distribuito in modo più uniforme sul file system. Per ulteriori informazioni sul ribilanciamento dei carichi di lavoro, consulta. Monitoraggio di FSx per il bilanciam ento del carico di lavoro ONTAP
Prestazioni del file server	Throughput di rete Velocità effettiva del disco IOPS del disco Utilizzo CPU	Aumentate la capacità di throughput del file system se il file system non ha già raggiunto la capacità di throughput massima. Per ulteriori informazioni sull'aggiornamento della capacità di throughput, vedere. Come modificare la capacità di throughput Se il file system ha più coppie HA e l'utilizzo è elevato solo per un sottoinsieme di file server, è possibile ribilanciare il carico di lavoro in modo che utilizzi in modo più uniforme le funzionalità prestazionali di ciascuna coppia HA del file system. Per ulteriori informazioni sul ribilanciamento dei carichi di lavoro, consulta. Monitoraggio di FSx per il bilanciamento del carico di lavoro ONTAP

Sezione Dashboard	Se è presente un avviso per questa metrica	Esegui questa operazione
Prestazioni disco	IOPS su disco	Aumentate gli IOPS SSD se il file system non ha già raggiunto il livello massimo di IOPS SSD per l'attuale capacità di throughput del file system. Per ulteriori informazioni sull'aggiornamento degli IOPS forniti dal file system, consulta. Modifica della capacità di archiviazione SSD e degli IOPS assegnati Se il file system ha più coppie HA e l'utilizzo degli IOPS del disco è maggiore solo per un sottoinsieme degli aggregati del file system (i pool di storage che costituiscono il livello di storage principale), è possibile anche ribilanciare il carico di lavoro in modo che gli IOPS del disco vengano utilizzati in modo più uniforme su tutto il file system. Per ulteriori informazioni sul ribilanciamento dei carichi di lavoro, consulta. Monitoraggio di FSx per il bilanciamento del carico di lavoro ONTAP

Per ulteriori informazioni sulle prestazioni del file system, vedere. Amazon FSx per NetApp prestazioni ONTAP

Creazione di CloudWatch allarmi Amazon per monitorare Amazon FSx

Puoi creare un CloudWatch allarme che invia un messaggio Amazon Simple Notification Service (Amazon SNS) quando l'allarme cambia stato. Un allarme monitora un singolo parametro per un periodo di tempo specificato. Se necessario, l'allarme esegue quindi una o più azioni in base al valore della metrica relativa a una determinata soglia per un certo numero di periodi di tempo. L'operazione corrisponde all'invio di una notifica a un argomento di Amazon SNS o a una policy di Auto Scaling.

Gli allarmi richiamano azioni solo per cambiamenti di stato sostenuti. CloudWatch gli allarmi non richiamano azioni solo perché si trovano in uno stato particolare; lo stato deve essere cambiato ed essere stato mantenuto per un determinato numero di periodi. Puoi creare un allarme dalla console Amazon FSx o dalla console Amazon CloudWatch .

Le seguenti procedure descrivono come creare allarmi utilizzando la console Amazon FSx AWS Command Line Interface ,AWS CLI() e l'API.

Per impostare allarmi utilizzando la console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli File system, quindi scegli il file system per cui desideri creare l'allarme.
3. Nella pagina di riepilogo, scegli Monitoraggio e prestazioni dal secondo pannello.
4. Scegli la scheda CloudWatch Allarmi.
5. Scegli Crea CloudWatch allarme. Sarai reindirizzato alla console CloudWatch.
6. Scegli Select Metric (Seleziona parametro).
7. Nella sezione Metriche, scegli FSx.
8. Scegli una categoria metrica:
   - Metriche del file system
   - Metriche dettagliate del file system
   - Metriche del volume
   - Metriche dettagliate sul volume
9. Scegli la metrica per cui desideri impostare l'allarme, quindi scegli Seleziona metrica.
10. Nella sezione Condizioni, scegli le condizioni che desideri per l'allarme, quindi 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

11. Se desideri CloudWatch inviarti un'e-mail o una notifica Amazon SNS quando lo stato di allarme avvia l'azione, scegli uno stato di allarme per Attivazione dello stato di allarme.

    Per Invia una notifica al seguente argomento SNS, scegli un'opzione. Se si sceglie Create topic (Crea argomento), è possibile 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. Seleziona Successivo.

> **Note**
>
> 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 l'allarme passa allo stato definito. Se lo stato cambia prima della verifica degli indirizzi e-mail, questi non riceveranno una notifica.

12. Compila i campi Nome dell'avviso e Descrizione dell'avviso, quindi scegli Avanti.
13. Nella pagina Anteprima e creazione, esamina l'avviso che stai per creare, quindi scegli Crea avviso.

Per impostare allarmi utilizzando la console CloudWatch

1. Apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegli Create Alarm per avviare la Create Alarm Wizard.
3. Segui la procedura descritta in Per impostare gli allarmi utilizzando la console Amazon FSx, a partire dal passaggio 6.

Per impostare un allarme utilizzando il AWS CLI

- Richiama il comando CLI put-metric-alarm. Per ulteriori informazioni, consulta la sezione relativa alle informazioni di riferimento ai comandi di AWS CLI.

Per impostare un allarme utilizzando l'API CloudWatch

- Chiama l'operazione PutMetricAlarm API. Per ulteriori informazioni, consulta Amazon CloudWatch API Reference.

Monitoraggio di FSx per il bilanciamento del carico di lavoro ONTAP

Se si dispone di un file system con più coppie HA, le prestazioni e il throughput sono distribuiti su ciascuna delle coppie HA. FSx for ONTAP bilancia automaticamente i file man mano che vengono scritti sul file system, ma in rari casi è possibile che i dati del carico di lavoro o l'I/O si squilibrino tra le

coppie HA, il che può influire sulle prestazioni complessive del carico di lavoro. È possibile monitorare il carico di lavoro per garantire che rimanga bilanciato su ciascuna delle coppie HA del file system (e sui relativi file server e aggregati corrispondenti, i pool di storage che costituiscono il livello di storage principale).

Argomenti

Equilibrio nell'utilizzo dello storage principale

La capacità di storage principale del file system è suddivisa equamente tra ciascuna delle coppie HA in pool di storage denominati aggregati. Ogni coppia HA ha un aggregato. Si consiglia di mantenere un utilizzo medio non superiore all'80% per il livello di storage principale su base continuativa. Per i file system con più coppie HA, si consiglia di mantenere un utilizzo medio fino all'80% per ogni aggregato.

Il mantenimento dell'80% di utilizzo garantisce lo spazio libero per i nuovi dati in entrata e mantiene un buon sovraccarico per le operazioni di manutenzione che possono temporaneamente occupare spazio libero sugli aggregati.

Se noti che gli aggregati sono squilibrati, puoi aumentare la capacità di storage principale del file system (aumentando proporzionalmente la capacità di archiviazione di ciascun aggregato) oppure puoi spostare i volumi tra gli aggregati utilizzando il comando volume move nella CLI di ONTAP.

Squilibrio nell'utilizzo delle prestazioni del file server e del disco

Le prestazioni totali del file system (ad esempio la velocità effettiva di rete, il throughput e gli IOPS da file server a disco e IOPS su disco) sono suddivise equamente tra le coppie HA del file system. Si consiglia di mantenere un utilizzo medio inferiore al 50% (e un utilizzo di picco massimo inferiore all'80%) per tutti i limiti di prestazioni su base continuativa, sia per l'utilizzo complessivo delle risorse del file server del file system su tutte le coppie HA, sia per il singolo file server.

Se noti che l'utilizzo delle prestazioni del file server è squilibrato e i file server su cui è sbilanciato il carico di lavoro hanno un utilizzo continuo superiore all'80%, puoi utilizzare la CLI di ONTAP e

l'API REST per diagnosticare ulteriormente la causa dello squilibrio delle prestazioni e porvi rimedio. Di seguito è riportata una tabella dei possibili indicatori di squilibrio e delle fasi successive per un'ulteriore diagnosi.

Se il tuo file system è...	Allora...
La velocità effettiva del disco del file server o gli IOPS del disco del file server non sono bilanciati	È possibile che si verifichi un hotspotting di I/O su un sottoinsieme di coppie HA (un sottoinsieme di volumi contenente una quantità enorme di dati a cui si accede), il che può limitare le prestazioni complessive del carico di lavoro perché è ostacolato rispetto a un sottoinsieme di coppie HA. Per ogni file server molto utilizzato, controlla i volumi più utilizzat i per vedere quali sono i volumi con la maggiore attività all'interno di un aggregato. Per ulteriori informazioni su questa procedura, consulta Ribilanciamento dei volumi altamente utilizzati.
Il throughput di rete non è bilanciato, ma il throughput del disco del file server, gli IOPS del disco del file server o gli IOPS del disco non sono sbilanciati	I tuoi dati sono distribuiti in modo uniforme tra le coppie HA, a differenza dei tuoi client. Per i file server che utilizzano maggiormente il throughpu t di rete rispetto agli altri, controllate i client principali per ogni file server, quindi ribilanciate i client smontando tutti i volumi di quei client e rimontandoli utilizzando un endpoint diverso su una coppia HA diversa. Per ulteriori informazioni su questa procedura, consulta Ribilanciamento dei client ad alto traffico.

Mappatura delle CloudWatch dimensioni alle risorse dell'API REST e della CLI ONTAP

Il tuo file system con scalabilità orizzontale ha CloudWatch metriche Amazon con la `FileServer` dimensione or. `Aggregate` Per diagnosticare ulteriormente i casi di squilibrio, è necessario mappare questi valori di dimensione su file server (o nodi) e aggregati specifici nella CLI ONTAP o nell'API REST.

- Per i file server, ogni nome di file server è mappato a un nome di file server (o nodo) in ONTAP (ad esempio,). `FsxId01234567890abcdef-01` I file server con numeri dispari sono file server preferiti (ovvero gestiscono il traffico a meno che il file system non abbia effettuato il failover sul file server secondario), mentre i file server con numero pari sono file server secondari (ovvero servono

il traffico solo quando il partner non è disponibile). Per questo motivo, i file server secondari in genere mostrano un utilizzo inferiore rispetto ai file server preferiti.

- Per gli aggregati, ogni nome aggregato viene mappato a un aggregato in ONTAP (ad esempio,). `aggr1` Esiste un aggregato per ogni coppia HA, il che significa che l'aggregato `aggr1` è condiviso dai file server `FsxId01234567890abcdef-01` (il file server attivo) e `FsxId01234567890abcdef-02` (il file server secondario) in una coppia HA, l'aggregato `aggr2` è condiviso dai file server e così via. `FsxId01234567890abcdef-03` `FsxId01234567890abcdef-04`

È possibile visualizzare le mappature tra tutti gli aggregati e i file server utilizzando la CLI di ONTAP.

1. Per accedere tramite SSH alla NetApp CLI ONTAP del tuo file system, segui i passaggi documentati nella sezione della Guida per Utilizzo della CLI NetApp ONTAP l'utente di Amazon FSx for ONTAP. NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilizza il comando storage aggregate show, specificando il parametro. `-fields node`

   ```
   ::> storage aggregate show -fields node
   aggregate                     node
   ----------------------------- -------------------------
   aggr1                         FsxId01234567890abcdef-01
   aggr2                         FsxId01234567890abcdef-03
   aggr3                         FsxId01234567890abcdef-05
   aggr4                         FsxId01234567890abcdef-07
   aggr5                         FsxId01234567890abcdef-09
   aggr6                         FsxId01234567890abcdef-11
   6 entries were displayed.
   ```

Ribilanciamento dei client ad alto traffico

Se si riscontra uno squilibrio di I/O tra i file server (in particolare a causa dell'utilizzo del throughput di rete), la causa potrebbe essere un numero elevato di client di I/O. Per identificare i client ad alto traffico, utilizza la CLI di ONTAP.

1. Per accedere tramite SSH alla NetApp CLI ONTAP del tuo file system, segui i passaggi documentati nella sezione della Guida per Utilizzo della CLI NetApp ONTAP l'utente di Amazon FSx for ONTAP. NetApp

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. Per visualizzare i client con il traffico più elevato, utilizzate il comando Statistics top client show ONTAP CLI. Facoltativamente, puoi specificare il `-node` parametro per visualizzare solo i client principali per un file server specifico. Se state diagnosticando uno squilibrio per un file server specifico, utilizzate il `-node` parametro, sostituendolo `node_name` con il nome del file server (ad esempio,). `FsxId01234567890abcdef-01`

   Facoltativamente, è possibile aggiungere il `-interval` parametro, fornendo l'intervallo di misurazione (in secondi) prima dell'output di ogni report. L'aumento dell'intervallo (ad esempio, fino a un massimo di 300 secondi) fornisce un campione a lungo termine della quantità di traffico indirizzata verso ciascun volume. L'impostazione predefinita è 5 (secondi).

```
::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
```

   Nell'output, i client principali vengono visualizzati in base all'indirizzo IP e alla porta.

```
                                                    *Total     Total
            Client   Vserver          Node              Ops     (Bps)
------------------ --------- ------------------------ ------ ---------
 172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
```

3. È possibile ribilanciare un sottoinsieme dei client ad alto traffico elencati su altri file server. A tale scopo, smonta il volume dal client e rimontalo utilizzando il nome DNS dell'endpoint NFS/SMB di SVM: in questo modo viene restituito un endpoint casuale corrispondente a una coppia HA casuale.

   Ti consigliamo di riutilizzare il nome DNS, ma hai la possibilità di scegliere esplicitamente quale coppia HA monta un determinato client. Per garantire il montaggio di un client su un endpoint diverso, puoi invece specificare un indirizzo IP dell'endpoint diverso da quello corrispondente al nodo che presenta un traffico elevato. È possibile farlo eseguendo il comando seguente:

```
::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
 address,curr-node
```

```
vserver   lif                  address      curr-node
--------- -------------------- ------------ ------------------------
svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
svm01 nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
2 entries were displayed.
```

In base all'output di esempio del `statistics top client show` comando, il client `172.17.236.53` sta indirizzando un traffico elevato verso`FsxId01234567890abcdef-01`. L'output del `network interface show` comando indica che questo è l'indirizzo`172.31.15.89`. Per eseguire il montaggio su un dispositivo diverso, selezionate qualsiasi altro indirizzo (in questo esempio, l'unico altro indirizzo è`172.31.8.112`, corrispondente a`FsxId01234567890abcdef-03`).

Ribilanciamento dei volumi altamente utilizzati

Se riscontri uno squilibrio di I/O tra i tuoi volumi o aggregati, puoi ribilanciare i volumi per ridistribuire il traffico di I/O tra i volumi.

> **Note**
>
> Se si riscontra uno squilibrio nell'utilizzo dello storage tra gli aggregati, in genere non vi è alcun impatto sulle prestazioni a meno che l'elevato utilizzo non sia associato a uno squilibrio di I/O. Sebbene sia possibile spostare i volumi tra gli aggregati per bilanciare l'utilizzo dello storage, consigliamo di spostare i volumi solo se si riscontra un impatto sulle prestazioni, poiché lo spostamento dei volumi può avere un impatto negativo sulle prestazioni se non si considera anche l'I/O determinato da ciascun volume che si intende spostare.

1. Per accedere tramite SSH alla NetApp CLI ONTAP del tuo file system, segui i passaggi documentati nella sezione della Guida per Utilizzo della CLI NetApp ONTAP l'utente di Amazon FSx for ONTAP. NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilizza il comando Statistics Volume Show ONTAP CLI per visualizzare i volumi di traffico più elevati per un determinato aggregato, con le seguenti modifiche:

   - Sostituisci *`aggregate_name con il nome`* dell'aggregato (ad esempio,). `aggr1`

- Facoltativamente, puoi aggiungere il `-interval` parametro, fornendo l'intervallo di misurazione (in secondi) prima dell'output di ogni rapporto. L'aumento dell'intervallo (ad esempio, fino a un massimo di 300 secondi) fornisce un campione a lungo termine della quantità di traffico indirizzata verso ciascun volume. L'impostazione predefinita è 5 (secondi).

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
 [5,300]]
```

A seconda dell'intervallo scelto, la visualizzazione dei dati può richiedere fino a 5 minuti. Il comando mostra tutti i volumi dell'aggregato, insieme alla quantità di traffico indirizzata verso ciascun aggregato.

```
                           *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (us)
---------- ------- --------- ------ ---- ----- ----- --------- ----- -------
vol1__0007    svm1     aggr1   4078 4078     0     0 267255808     0    1092
vol1__0005    svm1     aggr1   4078 4078     0     0 267255808     0    1086
vol1__0003    svm1     aggr1   4077 4077     0     0 267223040     0    1086
vol1__0001    svm1     aggr1   4077 4077     0     0 267239424     0    1087
vol1__0008    svm1     aggr2   2314 2314     0     0 151650304     0    1112
vol1__0006    svm1     aggr2   2144 2144     0     0 140509184     0    1104
vol1__0002    svm1     aggr2   2183 2183     0     0 143065088     0    1106
vol1__0004    svm1     aggr2   2183 2183     0     0 143065088     0    1103
```

Le statistiche sul volume vengono visualizzate per costituente (ad esempio, `vol1__0015` è il quindicesimo costituente di). FlexGroup `vol1` Come si può vedere dall'output di esempio, i componenti di sono più utilizzati rispetto ai componenti per`aggr1`. `aggr2` Per bilanciare il traffico tra gli aggregati, puoi spostare i volumi costituenti tra gli aggregati in modo che il traffico sia distribuito in modo più uniforme.

3. Per spostare un volume tra gli aggregati, utilizzate il comando volume move start ONTAP CLI, sostituendo i seguenti valori:

   - Sostituisci *`svm_name con il nome`* dell'SVM che ospita il volume che stai spostando.
   - Sostituite *`volume_name con il nome`* del costituente del volume (ad esempio,). `vol1__0001`
   - Sostituite *`aggregate_name con il nome`* dell'aggregato di destinazione per il volume.

> **Important**
>
> Lo spostamento dei volumi consuma le risorse di rete e del disco per i file server di origine e di destinazione. Di conseguenza, le prestazioni del carico di lavoro possono essere influenzate da eventuali spostamenti di volume in corso. Inoltre, è prevista una fase di interruzione del processo di spostamento del volume che sospende temporaneamente l'I/O per l'eventuale traffico diretto al volume.

```
::> volume move start -vserver svm_name -volume volume_name -
destination aggregate_name -foreground false
[Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".
Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the
 status of this operation.
```

Per controllare lo stato dell'operazione di spostamento del volume, utilizzate il comando `volume move show` ONTAP CLI.

```
::> volume move show -vserver svm_name -volume volume_name
                            Vserver Name: svm01
                             Volume Name: vol1__0001
                    Actual Completion Time: -
                           Bytes Remaining: 1.00TB
              Specified Action For Cutover: retry_on_failure
            Specified Cutover Time Window: 30
                   Destination Aggregate: aggr2
                        Destination Node: FsxId01234567890abcdef-03
                         Detailed Status: Transferring data: 12.23GB sent.
                      Percentage Complete: 1%
                                Move Phase: replicating
                  Prior Issues Encountered: -
               Estimated Remaining Duration: 00:40:25
                     Replication Throughput: 434.3MB/s
                           Duration of Move: 00:00:27
                           Source Aggregate: aggr2
                                Source Node: FsxId01234567890abcdef-01
                                 Move State: healthy
```

Questo comando mostra il tempo stimato per completare lo spostamento, come uno dei campi informativi. Al termine dell'operazione, lo stesso comando mostrerà che il `Move Phase` campo è completato.

È necessario assicurarsi che ciascuno FlexGroup sia distribuito uniformemente tra gli aggregati, idealmente con gli 8 componenti consigliati per aggregato. Se spostate un volume costituente su un altro aggregato per ottenere un risultato altrimenti bilanciatoFlexGroup, dovreste a sua volta spostare un altro volume costituente (meno utilizzato) sull'aggregato di origine per mantenere l'equilibrio.

Monitoraggio degli eventi FSx per ONTAP EMS

È possibile monitorare gli eventi del file system FSx for ONTAP utilizzando l'Events Management System (EMS) nativo di NetApp ONTAP. È possibile visualizzare questi eventi utilizzando la CLI di NetApp ONTAP.

Argomenti

- Panoramica degli eventi EMS
- Visualizzazione degli eventi EMS
- Inoltro di eventi EMS a un server Syslog

Panoramica degli eventi EMS

Gli eventi EMS sono notifiche generate automaticamente che avvisano l'utente quando si verifica una condizione predefinita nel file system FSx for ONTAP. Queste notifiche ti tengono informato in modo da prevenire o correggere problemi che possono portare a problemi più gravi, come problemi di autenticazione delle macchine virtuali di archiviazione (SVM) o volumi completi.

Per impostazione predefinita, gli eventi vengono registrati nel registro del sistema di gestione degli eventi. Utilizzando EMS, è possibile monitorare eventi quali le modifiche delle password degli utenti, la presenza di un componente con capacità FlexGroup quasi esaurita, l'inserimento manuale in linea o offline di un numero di unità logico (LUN) o il ridimensionamento automatico di un volume.

Per ulteriori informazioni sugli eventi ONTAP EMS, vedere ONTAP EMS Reference nel Centro documentazione ONTAP. NetApp Per visualizzare le categorie di eventi, usa il riquadro di navigazione a sinistra del documento.

> **Note**
>
> Solo alcuni messaggi ONTAP EMS sono disponibili per i file system FSx for ONTAP. Per visualizzare un elenco dei messaggi ONTAP EMS disponibili, utilizzare il comando NetApp ONTAP CLI event catalog show.

Le descrizioni degli eventi EMS contengono i nomi degli eventi, la gravità, le possibili cause, i messaggi di registro e le azioni correttive che possono aiutarti a decidere come rispondere. Ad esempio, un evento WAFL.vol.AutoSize.fail si verifica quando il dimensionamento automatico di un volume non riesce. In base alla descrizione dell'evento, l'azione correttiva consiste nell'aumentare la dimensione massima del volume durante l'impostazione della dimensione automatica.

Visualizzazione degli eventi EMS

Utilizzate il comando NetApp ONTAP CLI event log show per visualizzare il contenuto del registro degli eventi. Questo comando è disponibile se hai il `fsxadmin` ruolo nel tuo file system. La sintassi del comando è la seguente:

```
event log show [event_options]
```

Gli eventi più recenti vengono elencati per primi. Per impostazione predefinita, questo comando visualizza `EMERGENCY` gli eventi a `ERROR` livello di gravità con le seguenti informazioni: `ALERT`

- Ora: l'ora dell'evento.
- Nodo: il nodo in cui si è verificato l'evento.
- Gravità: il livello di gravità dell'evento. Per visualizzare o `NOTICE` definire `INFORMATIONAL` gli eventi a `DEBUG` livello di gravità, utilizzare l'opzione. `-severity`
- Evento: il nome e il messaggio dell'evento.

Per visualizzare informazioni dettagliate sugli eventi, utilizzate una o più delle opzioni di evento elencate nella tabella seguente.

Opzione evento	Descrizione
`-detail`	Visualizza informazioni aggiuntive sull'evento.

Opzione evento	Descrizione
`-detailtime`	Visualizza informazioni dettagliate sugli eventi in ordine cronologico inverso.
`-instance`	Visualizza informazioni dettagliate su tutti i campi.
`-node` *`nodename`*`|local`	Visualizza un elenco di eventi per il nodo specifica to. Utilizzate questa opzione con `-seqnum` per visualizzare informazioni dettagliate.
`-seqnum` *`sequence_number`*	Seleziona gli eventi che corrispondono a questo numero nella sequenza. Utilizzare con `-node` per visualizzare informazioni dettagliate.

Opzione evento	Descrizione

`-time MM/DD/YYYY HH:MM:SS`	Seleziona gli eventi che si sono verificati in questo momento specifico. Usa il formato: MM/GG/AAAA HH:MM:SS [+- HH:MM]. È possibile specificare un intervallo di tempo utilizzando l'operatore tra due istruzioni temporali. `..`
	`event log show -time "04/17/2023 05:55:00".."04/17/2023 06:10:00"`
	I valori temporali comparativi sono relativi all'ora corrente in cui si esegue il comando. L'esempio seguente mostra come visualizzare solo gli eventi che si sono verificati nell'ultimo minuto:
	`event log show -time >1m`
	I campi del mese e della data di questa opzione non hanno il riempimento zero. Questi campi possono essere composti da una sola cifra; per esempio,. `4/1/2023 06:45:00`

Opzione evento	Descrizione
`-severity sev_level`	Seleziona gli eventi che corrispondono al valore *sev_level* , che deve essere uno dei seguenti: • EMERGENCY — Interruzione • ALERT— Unico punto di guasto • ERROR— Degradazione • NOTICE— Informazioni • INFORMATIONAL — Informazioni • DEBUG— Informazioni di debug Per visualizzare tutti gli eventi, specificare la gravità come segue: `event log show -severity <=DEBUG`

Opzione evento	Descrizione
`-ems-severity` *ems_sev_level*	Seleziona gli eventi che corrispondono al valore *ems_sev_level* , che deve essere uno dei seguenti: • `NODE_FAULT` — Viene rilevato un danneggiamento dei dati o il nodo non è in grado di fornire il servizio client. • `SVC_FAULT` — Viene rilevata una perdita temporanea del servizio, in genere un errore temporane o del software. • `NODE_ERROR` — Viene rilevato un errore hardware che non è immediatamente fatale. • `SVC_ERROR` — Viene rilevato un errore software che non è immediatamente fatale. • `WARNING`— Un messaggio ad alta priorità che non indica un errore. • `NOTICE`— Un messaggio con priorità normale che non indica un errore. • `INFO`— Un messaggio a bassa priorità che non indica un errore.

Opzione evento	Descrizione
	• DEBUG— Un messaggio di debug. • VAR— Un messaggio con gravità variabile, selezionato in fase di esecuzione. Per visualizzare tutti gli eventi, specificare la gravità come segue: `event log show -ems-severity <=DEBUG`
`-source` *`text`*	Seleziona gli eventi che corrispondono al valore del *`testo`*. La fonte è in genere un modulo software.
`-message-name` *`message_name`*	Seleziona gli eventi che corrispondono al valore *`message_name`* . I nomi dei messaggi sono descritti vi, quindi filtrando l'output in base al nome del messaggio vengono visualizzati messaggi di un tipo specifico.
`-event` *`text`*	*`Seleziona gli eventi che corrispondono al valore del testo.`* Il `event` campo contiene il testo completo dell'evento, inclusi eventuali parametri.

Opzione evento	Descrizione
`-kernel-generation-num` *integer*	Seleziona gli eventi che corrispondono al *valore intero.* Solo gli eventi che provengono dal kernel hanno numeri di generazione del kernel.
`-kernel-sequence-num` *integer*	*Seleziona gli eventi che corrispondono al valore intero.* Solo gli eventi che provengono dal kernel hanno numeri di sequenza del kernel.
`-action` *text*	*Seleziona gli eventi che corrispondono al valore del testo.* Il `action` campo descrive le eventuali azioni correttive da intraprendere per porre rimedio alla situazione.
`-description` *text*	Seleziona gli eventi che corrispondono al valore del *testo*. Il `descripti on` campo descrive perché l'evento si è verificato e cosa significa.

Opzione evento	Descrizione
`-filter-name` *`filter_name`*	Seleziona gli eventi che corrispondono al valore *`filter_name`* . Vengono visualizzati solo gli eventi inclusi dai filtri esistenti che corrispondono a questo valore.
`-fields` *`fieldname`* `,...`	Indica che l'output del comando include anche il campo o i campi specifica ti. È possibile utilizzare `-fields ?` per scegliere i campi che si desidera specificare.

Per visualizzare gli eventi EMS

1. Per accedere tramite SSH alla NetApp CLI ONTAP del tuo file system, segui i passaggi documentati nella sezione della Guida per Utilizzo della CLI NetApp ONTAP l'utente di Amazon FSx for ONTAP. NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Usa il `event log show` comando per visualizzare il contenuto del registro degli eventi.

   ```
   ::> event log show
   Time                Node          Severity      Event
   ------------------- ------------- ------------- -----------------------
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0a.
   6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
    received on node node1, port e0d.
   ```

Per informazioni sugli eventi EMS restituiti dal `event log show` comando, consulta ONTAP EMS Reference nel Centro di documentazione NetApp ONTAP.

Inoltro di eventi EMS a un server Syslog

È possibile configurare gli eventi EMS per inoltrare le notifiche a un server Syslog. L'inoltro degli eventi EMS viene utilizzato per il monitoraggio in tempo reale del file system per determinare e isolare le cause principali di un'ampia gamma di problemi. Se l'ambiente non contiene già un server Syslog per le notifiche degli eventi, è necessario prima crearne uno. Il DNS deve essere configurato sul file system per risolvere il nome del server Syslog.

Per configurare gli eventi EMS per inoltrare le notifiche a un server Syslog

1. Per accedere tramite SSH alla NetApp CLI ONTAP del tuo file system, segui i passaggi documentati nella sezione della Guida per Utilizzo della CLI NetApp ONTAP l'utente di Amazon FSx for ONTAP. NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Utilizza il comando event notification destination create per creare una destinazione di notifica di evento di tipo`syslog`, specificando i seguenti attributi:

   - *`dest_name`*— Il nome della destinazione di notifica da creare (ad esempio,`syslog-ems`). Il nome della destinazione di una notifica di eventi deve contenere da 2 a 64 caratteri. I caratteri validi sono i seguenti caratteri ASCII: A-Z, a-z, 0-9, «_» e «-». Il nome deve iniziare e terminare con: A-Z, a-z o 0-9.
   - *`syslog_name`*— Il nome host o l'indirizzo IP del server Syslog a cui vengono inviati i messaggi Syslog.
   - *`transport_protocol`*— Il protocollo utilizzato per inviare gli eventi:
     - `udp-unencrypted`— User Datagram Protocol senza sicurezza. Questo è il protocollo predefinito.
     - `tcp-unencrypted`— Transmission Control Protocol senza sicurezza.
     - `tcp-encrypted`— Protocollo di controllo della trasmissione con Transport Layer Security (TLS). Quando viene specificata questa opzione, FSx for ONTAP verifica l'identità dell'host di destinazione convalidandone il certificato.
   - *`port_number`*— La porta del server Syslog a cui vengono inviati i messaggi Syslog. Il `syslog-port` parametro del valore predefinito dipende dall'impostazione del parametro.

`syslog-transport` Se `syslog-transport` è impostato su`tcp-encrypted`, il valore `syslog-port` predefinito è`6514`. Se `syslog-transport` è impostato su`tcp-unencrypted`, `syslog-port` ha il valore predefinito`601`. Altrimenti, la porta predefinita è impostata su`514`.

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. Utilizzate il comando event notification create per creare una nuova notifica di un set di eventi definito da un filtro di eventi alla destinazione della notifica creata nel passaggio precedente, specificando i seguenti attributi:

   - *node_name*— Il nome del filtro degli eventi. Gli eventi inclusi nel filtro degli eventi vengono inoltrati alle destinazioni specificate nel `-destinations` parametro.
   - *dest_name*— Il nome della destinazione di notifica esistente a cui vengono inviate le notifiche degli eventi.

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. Utilizzate il `event notification destination check` comando per generare un messaggio di prova e verificare che la configurazione funzioni. Specificate i seguenti attributi con il comando:

   - *node_name*— Il nome del nodo (ad esempio,`FsxId07353f551e6b557b4-01`).
   - *dest_name*— Il nome della destinazione di notifica esistente a cui vengono inviate le notifiche degli eventi.

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

Monitoraggio con Cloud Insights

NetApp Cloud Insights è un NetApp servizio che puoi utilizzare per monitorare i tuoi file system Amazon FSx for NetApp ONTAP insieme ad altre NetApp soluzioni di storage. Con Cloud Insights,

puoi monitorare le metriche di configurazione, capacità e prestazioni nel tempo per comprendere le tendenze del tuo carico di lavoro e pianificare le future esigenze di prestazioni e capacità di archiviazione. Puoi anche creare avvisi basati su condizioni metriche che possono integrarsi con i flussi di lavoro e gli strumenti di produttività esistenti.

> **Note**
>
> Cloud Insights non è supportato per i file system con scalabilità orizzontale.

Cloud Insights offre:

- Un'ampia gamma di metriche e log: raccogli i parametri di configurazione, capacità e prestazioni. Scopri l'andamento del tuo carico di lavoro con dashboard, avvisi e report predefiniti.
- Analisi degli utenti e protezione dal ransomware: con le istantanee Cloud Secure e ONTAP puoi controllare, rilevare, bloccare e riparare gli errori degli utenti e il ransomware.
- SnapMirror reportistica: comprendi le tue SnapMirror relazioni e imposta avvisi sui problemi di replica.
- Pianificazione della capacità: comprendi i requisiti di risorse dei carichi di lavoro locali per aiutarti a migrare il carico di lavoro verso una configurazione FSx for ONTAP più efficiente. È inoltre possibile utilizzare queste informazioni per pianificare quando saranno necessarie maggiori prestazioni o capacità per l'implementazione di FSx for ONTAP.

Per ulteriori informazioni su Cloud Insights, consulta NetApp Cloud Insights on NetApp Cloud Central.

Monitoraggio di FSx per i file system ONTAP con Harvest e Grafana

NetApp Harvest è uno strumento open source per raccogliere metriche di prestazioni e capacità dai sistemi ONTAP ed è compatibile con FSx for ONTAP. Puoi usare Harvest con Grafana per una soluzione di monitoraggio open source.

Guida introduttiva a Harvest e Grafana

La sezione seguente descrive in dettaglio come impostare e configurare Harvest e Grafana per misurare le prestazioni e l'utilizzo della capacità di storage del file system FSx for ONTAP.

Puoi monitorare il tuo file system Amazon FSx for NetApp ONTAP utilizzando Harvest e Grafana. NetApp Harvest monitora i data center ONTAP raccogliendo parametri relativi a prestazioni, capacità e hardware dai file system FSx for ONTAP. Grafana fornisce una dashboard in cui è possibile visualizzare le metriche Harvest raccolte.

Dashboard Harvest supportati

Amazon FSx for NetApp ONTAP espone un set di parametri diverso rispetto a ONTAP locale. NetApp Pertanto, solo le seguenti dashboard out-of-the-box Harvest contrassegnate con `fsx` sono attualmente supportate per l'uso con FSx for ONTAP. In alcuni pannelli di queste dashboard potrebbero mancare informazioni non supportate.

- ONTAP: Conformità
- ONTAP: istantanee sulla protezione dei dati
- ONTAP: sicurezza
- ONTAP: SVM
- ONTAP: Volume

AWS CloudFormation modello

Per iniziare, puoi implementare un AWS CloudFormation modello che avvii automaticamente un'istanza Amazon EC2 che esegue Harvest e Grafana. Come input per il AWS CloudFormation modello, specifichi l'`fsxadmin`utente e l'endpoint di gestione Amazon FSx per il file system che verrà aggiunto come parte di questa distribuzione. Una volta completata l'implementazione, puoi accedere alla dashboard di Grafana per monitorare il tuo file system.

Questa soluzione consente AWS CloudFormation di automatizzare l'implementazione della soluzione Harvest e Grafana. Il modello crea un'istanza Amazon EC2 Linux e installa i software Harvest e Grafana. Per utilizzare questa soluzione, scarica il modello fsx-ontap-harvest-grafana.template. AWS CloudFormation

> **Note**
>
> L'implementazione di questa soluzione comporta la fatturazione per i servizi associati. AWS Per ulteriori informazioni, consulta le pagine dei dettagli sui prezzi di tali servizi.

Tipi di istanza Amazon EC2

Quando configuri il modello, fornisci il tipo di istanza Amazon EC2. NetAppper la dimensione dell'istanza, i consigli di cui si consiglia l'uso dipendono dal numero di file system monitorati e dal numero di parametri che si sceglie di raccogliere. Con la configurazione predefinita, per ogni 10 file system monitorati, NetApp consiglia:

- CPU: 2 core
- Memoria: 1 GB
- Disco: 500 MB (utilizzato principalmente dai file di registro)

Di seguito sono riportate alcune configurazioni di esempio e il tipo di `t3` istanza che è possibile scegliere.

File system	CPU	Disk	Tipo di istanza
Meno di 10	2 core	500 MB	`t3.micro`
10—40	4 core	1000 MB	`t3.xlarge`
40 o più	8 core	2000 MB	`t3.2xlarge`

Per ulteriori informazioni sui tipi di istanze Amazon EC2, consulta la sezione Istanze generiche nella Guida per l'utente di Amazon EC2.

Regole delle porte delle istanze

Quando configuri l'istanza Amazon EC2, assicurati che le porte 3000 e 9090 siano aperte per il traffico in entrata per il gruppo di sicurezza in cui si trova l'istanza Amazon EC2 Harvest e Grafana. Poiché l'istanza lanciata si connette a un endpoint tramite HTTPS, deve risolvere l'endpoint, che richiede la porta 53 TCP/UDP per DNS. Inoltre, per raggiungere l'endpoint è necessaria la porta 443 TCP per HTTPS e l'accesso a Internet.

Procedura di distribuzione

La procedura seguente configura e implementa la soluzione Harvest/Grafana. L'implementazione richiede circa cinque minuti. Prima di iniziare, devi avere un file system FSx for ONTAP in esecuzione

in un Amazon Virtual Private Cloud (Amazon VPC) nel tuo AWS account e le informazioni sui parametri per il modello elencate di seguito. Per ulteriori informazioni sulla creazione di un file system, consulta. Creazione di FSx per i file system ONTAP

Per avviare lo stack di soluzioni Harvest/Grafana

1. Scarica il modello fsx-ontap-harvest-grafana.template. AWS CloudFormation Per ulteriori informazioni sulla creazione di uno stack, vedere Creazione di uno AWS CloudFormation stack sulla console nella Guida per l'utente. AWS CloudFormation AWS CloudFormation

   > **Note**
   >
   > Per impostazione predefinita, questo modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). AWS È necessario avviare questa soluzione in un Regione AWS luogo in cui Amazon FSx è disponibile. Per ulteriori informazioni, consulta gli endpoint e le quote di Amazon FSx nel.Riferimenti generali di AWS

2. Per i parametri, esamina i parametri del modello e modificali in base alle esigenze del tuo file system. Questa soluzione utilizza i seguenti valori predefiniti.

Parametro	Predefinito	Descrizione
InstanceType	`t3.micro`	Il tipo di istanza Amazon EC2. Di seguito sono riportati i tipi di `t3` istanza. • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` Per l'elenco completo dei valori dei tipi di istanza Amazon EC2 consentit

Parametro	Predefinito	Descrizione
		i per questo parametro, consulta .template. fsx-ontap -harvest-grafana
KeyPair	Nessun valore predefinito	La coppia di chiavi utilizzat a per accedere all'istanza Amazon EC2.
SecurityGroup	Nessun valore predefinito	L'ID del gruppo di sicurezza per l'istanza Harvest/G rafana. Assicurati che le porte in entrata 3000 e 9090, oltre alle porte 53 e 443, siano aperte dai client che desideri utilizzare per accedere alla dashboard Grafana.
Tipo di sottorete	Nessun valore predefinito	Specificare il tipo di sottorete , oppure`public`. `private` Utilizza una `public` sottorete per le risorse che devono essere connesse a Internet e una sottorete privata per le risorse che non saranno connesse a Internet. Per ulteriori informazioni, consulta i tipi di sottorete nella Guida per l'utente di Amazon VPC.

Parametro	Predefinito	Descrizione
Sottorete	Nessun valore predefinito	Specificate la stessa sottorete della sottorete preferita del file system Amazon FSx NetApp for ONTAP. Puoi trovare l'ID di sottorete preferito del file system nella console Amazon FSx, nella scheda Rete e sicurezza della pagina dei dettagli del file system FSx for ONTAP
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	La versione più recente dell'AMI Amazon Linux 2 in un dato momento Regione AWS.
SxEndPunto F	Nessun valore predefinito	L'indirizzo IP dell'endpoint di gestione del file system. È possibile trovare l'indirizzo IP dell'endpoint di gestione del file system nella console Amazon FSx, nella scheda Amministrazione della pagina dei dettagli del file system FSx for ONTAP.
SecretName	Nessun valore predefinito	AWS Secrets Manager nome segreto contenente la password per l'utente del file system. `fsxadmin` Questa è la password che hai fornito quando hai creato il file system.

3. Seleziona 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.

Accedere a Grafana

Al termine della distribuzione, utilizza il browser per accedere alla dashboard Grafana sull'IP e sulla porta 3000 dell'istanza Amazon EC2:

```
http://EC2_instance_IP:3000
```

Quando richiesto, utilizzate il nome utente predefinito di Grafana `admin` () e la password `pass` (). Ti consigliamo di cambiare la password non appena effettui l'accesso.

Per ulteriori informazioni, consulta la pagina NetApp Harvest su GitHub.

Risoluzione dei problemi relativi a Harvest e Grafana

Se riscontri dei dati mancanti menzionati nelle dashboard Harvest e Grafana o hai problemi a configurare Harvest e Grafana con FSx for ONTAP, consulta i seguenti argomenti per una potenziale soluzione.

Argomenti

- I dashboard SVM e Volume sono vuoti
- CloudFormation stack è stato ripristinato dopo il timeout

I dashboard SVM e Volume sono vuoti

Se lo AWS CloudFormation stack è stato distribuito correttamente e può contattare Grafana ma i dashboard SVM e volume sono vuoti, utilizza la seguente procedura per risolvere i problemi del tuo ambiente. Avrai bisogno dell'accesso SSH all'istanza Amazon EC2 su cui sono distribuiti Harvest e Grafana.

1. Accedi tramite SSH all'istanza Amazon EC2 su cui sono in esecuzione i tuoi client Harvest e Grafana.

```
[~]$ ssh ec2-user@ec2_ip_address
```

2. Usa il seguente comando per aprire il `harvest.yml` file e:
   - Verifica che sia stata creata una voce per l'istanza FSx for ONTAP come. `Cluster-2`
   - Verifica che le immissioni relative a nome utente e password corrispondano alle tue `fsxadmin` credenziali.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/
harvest.yml
```

3. Se il campo della password è vuoto, apri il file in un editor e aggiornalo con la `fsxadmin` password, come segue:

```
[ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
harvest.yml
```

4. Assicurati che le credenziali `fsxadmin` utente siano archiviate in Secrets Manager nel seguente formato per eventuali distribuzioni future, sostituendole *`fsxadmin_password`* con la tua password.

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

CloudFormation stack è stato ripristinato dopo il timeout

Se non riesci a distribuire correttamente lo stack e lo CloudFormation stack viene ripristinato con errori, utilizza la procedura seguente per risolvere il problema. Avrai bisogno dell'accesso SSH all'istanza EC2 distribuita dallo stack. CloudFormation

1. Ridistribuisci lo CloudFormation stack, assicurandoti che il rollback automatico sia disabilitato.
2. Accedi tramite SSH all'istanza Amazon EC2 su cui sono in esecuzione i tuoi client Harvest e Grafana.

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. Verifica che i contenitori docker siano stati avviati correttamente utilizzando il seguente comando.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

Nella risposta dovresti vedere cinque contenitori come segue:

```
CONTAINER ID   IMAGE                    COMMAND                  CREATED
 STATUS                          PORTS                    NAMES
6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
 Restarting (1) 20 seconds ago                            harvest_cluster-2
3cf3e3623fde   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago   Up
 About a minute                                           harvest_cluster-1
708f3b7ef6f8   grafana/grafana         "/run.sh"                8 minutes ago   Up
 8 minutes                   0.0.0.0:3000->3000/tcp   harvest_grafana
0febee61cab7   prom/alertmanager       "/bin/alertmanager -…"   8
 minutes ago   Up 8 minutes                    0.0.0.0:9093->9093/tcp
 harvest_prometheus_alertmanager
1706d8cd5a0c   prom/prometheus         "/bin/prometheus --c…"   8 minutes ago   Up
 8 minutes                   0.0.0.0:9090->9090/tcp   harvest_prometheus
```

4. Se i contenitori docker non sono in esecuzione, verifica la presenza di errori nel `/var/log/cloud-init-output.log` file come segue.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
     PLAY [Manage Harvest]
 ****************************************************

TASK [Gathering Facts] ********************************************************
ok: [localhost]

TASK [Verify images] **********************************************************
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
```

```
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
 "changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
 ('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
 "changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP *********************************************************************
localhost                  : ok=1    changed=0    unreachable=0    failed=1
 skipped=0    rescued=0    ignored=0
```

5. In caso di errori, esegui i seguenti comandi per distribuire i contenitori Harvest e Grafana.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
     [ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml --tags api
```

6. Convalida i contenitori avviati correttamente eseguendoli sudo docker ps e connettendoti ai tuoi URL Harvest e Grafana.

Registrazione di FSx per le chiamate API ONTAP conAWS CloudTrail

Amazon FSx è integrato conAWS CloudTrailun servizio che fornisce un record delle operazioni eseguite da un utente, un ruolo o unAWSservizio in Amazon FSx. CloudTrail acquisisce tutte le chiamate API Amazon FSx per Amazon FSx NetApp ONTAP come eventi. Le chiamate acquisite includono le chiamate dalla console Amazon FSx e le chiamate del codice alle operazioni API Amazon FSx.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi in un bucket Amazon S3, inclusi gli eventi per Amazon FSx. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti in CloudTrail console inCronologia eventi. Con le informazioni raccolte da CloudTrail, puoi determinare quale richiesta è stata effettuata ad Amazon FSx. 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 su CloudTrail, consultare la AWS CloudTrailGuida per l'utente di .

Informazioni su Amazon FSx in CloudTrail

CloudTrail è abilitato sull'account AWS al momento della sua creazione. Quando si verifica un'attività API in Amazon FSx, tale attività viene registrata in un CloudTrail evento insieme ad altriAWSeventi del servizio inCronologia eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account AWS. Per ulteriori informazioni, consultaVisualizzazione di eventi con CloudTrail Cronologia eventi.

Per una registrazione continuativa di attività ed eventiAWSUn account, inclusi gli eventi per Amazon FSx, crea un trail. UNpistaabilita CloudTrail per distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un trail nella console, il trail sarà valido in tutte le regioni AWS. Il percorso registra gli eventi da tutte le regioni AWSnella partizione AWS e distribuisce i file di log nel bucket Simple Storage Service (Amazon S3) specificato. Inoltre, è possibile configurare altriAWSservizi per analizzare con maggiore dettaglio e usare i dati raccolti in CloudTrail registri. Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utenteAWS CloudTrail:

- Creazione di un trail per il tuo Account AWS
- AWSintegrazioni di servizi con CloudTrail Log
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione CloudTrail file di log da più regioneRicezione di file di log CloudTrail da più account

Tutte le Amazon FSxChiamate APIsono registrati da CloudTrail. Ad esempio, le chiamate alle operazioni`CreateFileSystem`e `TagResource`le operazioni generano voci nel CloudTrail file di log.

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 servizio AWS.

Per ulteriori informazioni, consulta la .Elemento userIdentity di CloudTrailnellaAWS CloudTrailGuida per l'utente di .

Informazioni sulle voci dei file di log Amazon FSx

UNpistaè una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato. CloudTrail I file di log di contengono una o più voci di log. Un recordeventorappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. CloudTrail I file di log di non sono una traccia stack ordinata delle chiamate pubbliche dell'API, quindi non vengono visualizzati in un ordine specifico.

Il seguente esempio mostra un CloudTrail voce di log che illustra l'operazione`TagResource`operazione 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”
}
```

Il seguente esempio mostra un CloudTrail voce di log che illustra l'operazione`UntagResource`operazione di eliminazione di 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": "2018-11-14T23:40:54Z"
            }
        }
    },
    "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"
}
```

Quote

Di seguito, puoi scoprire le quote quando lavori con Amazon FSx NetApp for ONTAP.

Argomenti

Quote che è possibile incrementare

Di seguito sono riportate le quote per Amazon FSx NetApp for ONTAP per Account AWS ciascuna unità che Regione AWS puoi aumentare.

Risorsa	Predefinito	Descrizione
File system ONTAP	100	Il numero massimo di file system Amazon FSx for NetApp ONTAP che puoi creare in questo account.
ONTAPCapacità di archiviazione SSD	524.288	La quantità massima di capacità di archiviazione SSD (in GiB) per tutti i file system Amazon FSx NetApp for ONTAP che puoi avere in questo account.
ONTAPcapacità di throughput	10,240	La quantità massima di capacità di throughput (in MBps) per tutti i file system Amazon FSx for NetApp ONTAP che puoi avere in questo account.
ONTAPIOPS SSD	1.000.000	La quantità massima di IOPS SSD per tutti i file system

Risorsa	Predefinito	Descrizione
		Amazon FSx for NetApp ONTAP che puoi avere in questo account.
ONTAPbackup per file system	10.000	Il numero massimo di backup di volume avviati dall'utente per tutti i file system Amazon FSx for NetApp ONTAP che puoi avere in questo account.

Richiesta di un aumento delle quote

1. Aprire la pagina AWS Support, effettuare l'accesso se necessario, quindi selezionare Create Case (Crea caso).
2. Per Crea caso, scegli Account e supporto per la fatturazione.
3. Nel pannello dei dettagli del caso, inserisci le seguenti voci:
   - Per Tipo scegli Account.
   - Per Categoria scegli Altri problemi relativi all'account.
   - Per Oggetto inserisci**`Amazon FSx for NetApp ONTAP service limit increase request`**.
   - Fornisci una descrizione dettagliata della tua richiesta, tra cui:
     - La quota FSx che si desidera aumentare e il valore a cui si desidera aumentarla, se noto.
     - Il motivo per cui stai cercando l'aumento della quota.
     - L'ID e la regione del file system per ogni file system per cui si richiede un aumento.
4. Indica le tue opzioni di contatto preferite e scegli Invia.

Quote di risorse per ogni file system

La tabella seguente elenca le quote sulle risorse Amazon FSx NetApp for ONTAP per ogni file system in un. Regione AWS

Risorsa	Limite per file system
Capacità minima di archiviazione SSD	1.024 GiB per coppia ad alta disponibilità (HA)
Capacità massima di archiviazione SSD	• Scalabilità orizzontale: 512 TiB per coppia HA, fino a 1 PiB • Scalabilità: 192 TiB
Numero massimo di IOPS SSD	Scalabilità orizzontale: • 200.000 per coppia HA (fino a 12 coppie) Scalabilità verticale: • 160.000 nella regione Stati Uniti orientali (Ohio), nella regione degli Stati Uniti orientali (Virginia settentrionale), nella regione degli Stati Uniti occidentali (Oregon) e in Europa (Irlanda) • 80.000 in tutti gli altri paesi in Regioni AWS cui è disponibile FSx for ONTAP
Capacità di throughput minima	• Scalabilità orizzontale: 3.072 MBps per coppia HA • Scalabilità verticale: 128 MBps
Capacità di throughput massima	Scalabilità orizzontale: • 73.728 MBps 1 Scalabilità verticale:

Risorsa	Limite per file system
	• 4.096 MBps [2] nella regione Stati Uniti orientali (Ohio), nella regione Stati Uniti orientali (Virginia settentrionale), nella regione Stati Uniti occidentali (Oregon) e in Europa (Irlanda) • 2.048 MBps in tutti gli altri paesi in cui è disponibile Regioni AWS FSx for ONTAP
Numero massimo di volumi	• Scalabilità orizzontale: 1.000 • Scalabilità verticale: 500
Numero massimo di istantanee	1.023 per volume 3
Numero massimo di backup	4.091 per volume 4
Numero massimo di SVM	Scalabilità orizzontale: • 5 Scalabilità verticale: • 6 (capacità di throughput di 128 MBps) • 6 (capacità di throughput di 256 MBps) • 14 (capacità di throughput di 512 MBps) • 14 (capacità di trasmissione di 1.024 MBps) • 24 (capacità di throughput di 2.048 MBps) • 24 (capacità di throughput di 4.096 MBps)

Risorsa	Limite per file system
Numero massimo di tag	50
Periodo massimo di conservazione per i backup automatici	90 giorni
Periodo massimo di conservazione per i backup avviati dall'utente	Nessun limite di conservazione
Numero massimo di rotte supportate per file system	50 [5]

Note

[1] Su un file system scalabile con 12 coppie HA (6.144 MBps per coppia HA). Per ulteriori informazioni, consulta Coppie ad alta disponibilità (HA).

[2] Per fornire 4 GBps di capacità di throughput, il file system scalabile FSx for ONTAP richiede una configurazione del numero massimo di IOPS SSD (160.000) e un minimo di 5.120 GiB di capacità di storage SSD in un ambiente supportato. Regione AWS Per ulteriori informazioni su quali dispositivi supportano una capacità di throughput di 4.096 MBps, vedere. Regioni AWS Impatto della capacità di throughput sulle prestazioni

[3] È possibile archiviare fino a 1.023 istantanee per volume in qualsiasi momento. Una volta raggiunto questo limite, è necessario eliminare un'istantanea esistente prima di poter creare una nuova istantanea del volume.

[4] È possibile archiviare fino a 4.091 backup per volume in qualsiasi momento. Una volta raggiunto questo limite, è necessario eliminare un backup esistente prima di poter creare un nuovo backup del volume.

[5] È possibile configurare fino a 50 percorsi per file system in qualsiasi momento. Una volta raggiunto questo limite, è necessario eliminare una rotta esistente prima di poter configurare una nuova rotta. Il numero di route del file system è determinato dal numero di SVM presenti e dal numero di tabelle di route ad esso associate. È possibile determinare il numero esistente di route verso un file system utilizzando la seguente equazione: (1+ numero di SVM nel file system) * (tabelle di routing associate al file system).

Risoluzione dei problemi di Amazon FSx per ONTAP NetApp

Utilizzate le seguenti sezioni per risolvere i problemi riscontrati con FSx for ONTAP.

Argomenti

Il mio file system Multi-AZ è in uno stato **`MISCONFIGURED`**

Esistono diverse cause potenziali per cui un file system si trova in `MISCONFIGURED` uno stato, ognuna con la propria risoluzione, come segue.

Argomenti

L'account proprietario del VPC ha disabilitato la condivisione VPC Multi-AZ

I file system Multi-AZ creati da un partecipante Account AWS in una sottorete VPC condivisa entreranno in uno `MISCONFIGURED` stato per uno dei seguenti motivi:

- L'account proprietario che condivideva la sottorete VPC ha disabilitato il supporto di condivisione VPC Multi-AZ per i file system FSx for ONTAP.
- L'account del proprietario ha annullato la condivisione della sottorete VPC.

Se l'account del proprietario non ha condiviso la sottorete VPC, nella console per quel file system verrà visualizzato il seguente messaggio:

```
The vpc ID vpc-012345abcde does not exist
```

Per risolvere il problema, devi contattare l'account proprietario che ha condiviso con te la sottorete VPC. Per ulteriori informazioni, vedere Creazione di file system FSx per ONTAP in sottoreti condivise per ulteriori informazioni.

Non è possibile creare una nuova SVM su un file system Multi-AZ

Per i file system Multi-AZ creati da un partecipante Account AWS a un VPC condiviso, non sarà possibile creare una nuova SVM per uno dei seguenti motivi:

- L'account proprietario che condivideva la sottorete VPC ha disabilitato il supporto di condivisione VPC Multi-AZ per i file system FSx for ONTAP.
- L'account del proprietario ha annullato la condivisione della sottorete VPC.

Per risolvere il problema, devi contattare l'account proprietario che ha condiviso con te la sottorete VPC. Per ulteriori informazioni, vedere Creazione di file system FSx per ONTAP in sottoreti condivise per ulteriori informazioni.

Non puoi accedere al tuo file system

Esistono diverse cause potenziali per cui non è possibile accedere al file system, ognuna con la propria risoluzione, come segue.

Argomenti

- Impossibile accedere a un file system tramite NFS, SMB, ONTAP CLI o ONTAP REST API da un client in un altro VPC o in locale

L'interfaccia elastic network del file system è stata modificata o eliminata

Non è necessario modificare o eliminare alcuna delle interfacce di rete elastiche del file system. La modifica o l'eliminazione di un'interfaccia di rete può causare una perdita permanente della connessione tra il cloud privato virtuale (VPC) e il file system. Crea un nuovo file system e non modificare o eliminare l'interfaccia di rete Amazon FSx. Per ulteriori informazioni, consulta Controllo degli accessi ai file system con Amazon VPC.

L'indirizzo IP elastico collegato all'interfaccia elastica di rete del file system è stato eliminato

Amazon FSx non supporta l'accesso ai file system dalla rete Internet pubblica. Amazon FSx scollega 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. Per ulteriori informazioni, consulta Client supportati.

Il gruppo di sicurezza VPC del file system non dispone delle regole di ingresso richieste

Esamina le regole in entrata specificate in Gruppi di sicurezza Amazon VPC e assicurati che il gruppo di sicurezza associato al tuo file system disponga delle regole in entrata corrispondenti.

Il gruppo di sicurezza VPC dell'istanza di calcolo non dispone delle regole in uscita richieste

Controlla le regole in uscita specificate in Gruppi di sicurezza Amazon VPC e assicurati che il gruppo di sicurezza associato all'istanza di calcolo disponga delle regole in uscita corrispondenti.

La sottorete dell'istanza di calcolo non utilizza nessuna delle tabelle di routing associate al file system

FSx for ONTAP crea endpoint per l'accesso al file system in una tabella di routing VPC. Ti consigliamo di configurare il file system per utilizzare tutte le tabelle di routing VPC associate alle sottoreti in cui si trovano i tuoi client. Per impostazione predefinita, Amazon FSx utilizza la tabella

di routing principale del tuo VPC. Facoltativamente, puoi specificare una o più tabelle di routing per Amazon FSx da utilizzare quando crei il tuo file system.

Se riesci a eseguire il ping dell'endpoint Intercluster del file system ma non riesci a eseguire il ping dell'endpoint di gestione del file system (consulta Risorse del file system per ulteriori informazioni), è probabile che il client non si trovi in una sottorete associata a una delle tabelle di routing del file system. Per accedere al file system, associa una delle tabelle di routing del file system alla sottorete del client. Per informazioni sull'aggiornamento delle tabelle di routing Amazon VPC del tuo file system, consulta. Aggiornamento di un file system

Amazon FSx non è in grado di aggiornare la tabella di routing per i file system Multi-AZ creati utilizzando AWS CloudFormation

Amazon FSx gestisce le tabelle di routing VPC per file system Multi-AZ utilizzando l'autenticazione basata su tag. Queste tabelle di routing sono contrassegnate con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Quando si creano o si aggiornano file system FSx for ONTAP Multi-AZ, si AWS CloudFormation consiglia di aggiungere il tag manualmente. `Key: AmazonFSx; Value: ManagedByAmazonFSx`

Se non riesci a raggiungere il tuo file system Multi-AZ, controlla se le tabelle di routing VPC associate al file system sono etichettate con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` In caso contrario, Amazon FSx non può aggiornare tali tabelle di routing per instradare gli indirizzi IP mobili delle porte di gestione e dati al file server attivo quando si verifica un evento di failover. Per informazioni sull'aggiornamento delle tabelle di routing Amazon VPC del tuo file system, consulta. Aggiornamento di un file system

Impossibile accedere a un file system tramite iSCSI da un client in un altro VPC

Per accedere a un file system tramite il protocollo Internet Small Computer Systems Interface (iSCSI) da un client in un altro VPC, puoi configurare il peering Amazon VPC o tra AWS Transit Gateway il VPC associato al tuo file system e il VPC in cui risiede il client. Per ulteriori informazioni, consulta Creare e accettare connessioni peering VPC nella guida Amazon Virtual Private Cloud.

L'account proprietario ha annullato la condivisione della sottorete VPC

Se hai creato il file system in una sottorete VPC che è stata condivisa con te, l'account proprietario potrebbe aver annullato la condivisione della sottorete VPC.

Se l'account del proprietario non ha condiviso la sottorete VPC, nella console per quel file system verrà visualizzato il seguente messaggio:

```
The vpc ID vpc-012345abcde does not exist
```

Dovrai contattare l'account proprietario in modo che possa condividere nuovamente la sottorete con te.

Impossibile accedere a un file system tramite NFS, SMB, ONTAP CLI o ONTAP REST API da un client in un altro VPC o in locale

Per accedere a un file system tramite Network File System (NFS), Server Message Block (SMB) o NetApp ONTAP CLI e API REST da un client in un altro VPC o in locale, devi configurare il routing utilizzando AWS Transit Gateway il VPC associato al file system e la rete in cui risiede il client. Per ulteriori informazioni, consulta Accesso ai dati .

Non è possibile aggiungere una macchina virtuale di archiviazione (SVM) ad Active Directory

Se non riesci a unire una SVM a un Active Directory (AD), verifica innanzitutto. Unire SVM a Microsoft Active Directory I problemi più comuni che impediscono a una SVM di unirsi ad Active Directory sono elencati nelle sezioni seguenti, inclusi i messaggi di errore generati per ogni circostanza.

Argomenti

- Il nome NetBIOS SVM è lo stesso del nome NetBIOS per il dominio principale.
- L'SVM è già aggiunto a un'altra Active Directory
- Amazon FSx non può connettersi ai controller di dominio Active Directory perché il nome NetBIOS di SVM è già in uso
- Amazon FSx non è in grado di comunicare con i controller di dominio Active Directory
- Amazon FSx non riesce a connettersi ad Active Directory a causa di requisiti di porta o autorizzazioni per account di servizio non soddisfatti
- Amazon FSx non può connettersi ai controller di dominio Active Directory perché le credenziali dell'account di servizio non sono valide
- Amazon FSx non può connettersi ai controller di dominio Active Directory a causa di credenziali dell'account di servizio insufficienti

- Amazon FSx non è in grado di comunicare con i server DNS o i controller di dominio Active Directory
- Amazon FSx non è in grado di comunicare con Active Directory a causa di un nome di dominio Active Directory non valido.
- L'account di servizio non può accedere al gruppo di amministratori specificato nella configurazione SVM Active Directory
- Amazon FSx non può connettersi ai controller di dominio Active Directory perché l'unità organizzativa specificata non esiste o non è accessibile

Il nome NetBIOS SVM è lo stesso del nome NetBIOS per il dominio principale.

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx non è in grado di stabilire una connessione con Active Directory. Questo perché il nome del server specificato è il nome NetBIOS del dominio principale. Per risolvere questo problema, scegliete un nome NetBIOS per la SVM diverso dal nome NetBIOS del dominio principale. Quindi ritentate di aggiungere la SVM ad Active Directory.

Per risolvere questo problema, segui la procedura descritta in Unire una SVM a un Active Directory utilizzando l'API e AWS Management ConsoleAWS CLI Per riprovare a unire SVM ad AD. Assicurati di utilizzare un nome NetBIOS per la tua SVM diverso dal nome NetBIOS del dominio principale di Active Directory.

L'SVM è già aggiunto a un'altra Active Directory

L'aggiunta di una SVM a un Active Directory non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx non è in grado di stabilire una connessione con Active Directory. Questo perché la SVM è già aggiunta a un dominio. Per aggiungere questa SVM a un dominio diverso, puoi utilizzare la CLI ONTAP o l'API REST per annullare l'iscrizione a questa SVM da Active Directory. Quindi ritenta di aggiungere la tua SVM a un'altra Active Directory.

Per risolvere il problema, procedi come segue:

1. Utilizzate la CLI NetApp ONTAP per annullare l'accesso alla SVM dall'Active Directory corrente. Per ulteriori informazioni, consulta Annulla l'accesso a un Active Directory dal tuo SVM utilizzando la CLI NetApp di ONTAP.
2. Segui la procedura descritta in Unire una SVM a un Active Directory utilizzando l'API e AWS Management ConsoleAWS CLI per riprovare a unire la SVM al nuovo AD.

Amazon FSx non può connettersi ai controller di dominio Active Directory perché il nome NetBIOS di SVM è già in uso

La creazione di una SVM unita al tuo AD autogestito non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx non è in grado di stabilire una connessione con Active Directory. Questo perché il nome NetBIOS (computer) specificato è già in uso in Active Directory. Per risolvere questo problema, scegli un nome NetBIOS per la tua SVM che non è in uso in Active Directory., specificando un NetBIOS (computer) Quindi riprova a unire la SVM all'Active Directory.

Per risolvere questo problema, seguite la procedura descritta in Unire una SVM a un Active Directory utilizzando l'API e AWS Management ConsoleAWS CLI Per riprovare a unire la SVM all'AD. Assicurati di utilizzare un nome NetBIOS per la tua SVM che sia univoco e non già in uso in Active Directory.

Amazon FSx non è in grado di comunicare con i controller di dominio Active Directory

L'aggiunta di una SVM a un AD autogestito non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx non è in grado di comunicare con Active Directory. Per risolvere questo problema, assicurati che il traffico di rete sia consentito tra Amazon FSx e i controller di dominio. Quindi riprova a unire la tua SVM ad Active Directory.

Per risolvere il problema, procedere come segue:

1. Esamina i requisiti descritti in Requisiti relativi alla configurazione della rete e apporta le modifiche necessarie per abilitare le comunicazioni di rete tra Amazon FSx e il tuo AD.

2. Una volta che Amazon FSx è in grado di comunicare con il tuo AD, segui la procedura descritta in Unire una SVM a un Active Directory utilizzando l'API e AWS Management ConsoleAWS CLI e riprova a collegare la SVM all'AD.

Amazon FSx non riesce a connettersi ad Active Directory a causa di requisiti di porta o autorizzazioni per account di servizio non soddisfatti

L'aggiunta di una SVM a un AD autogestito non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx non è in grado di stabilire una connessione con Active Directory. Ciò è dovuto al fatto che i requisiti di porta per Active Directory non sono soddisfatti o l'account di servizio fornito non dispone delle autorizzazioni per aggiungere la macchina virtuale di storage al dominio con l'unità organizzativa specificata. Per risolvere questo problema, aggiorna la configurazione di Active Directory della tua macchina virtuale di storage dopo aver risolto eventuali problemi di autorizzazioni con porte e account di servizio, come consigliato nella guida per l'utente di Amazon FSx.

Per risolvere il problema, procedere come segue:

1. Esamina i requisiti descritti in Requisiti relativi alla configurazione della rete e apporta le modifiche necessarie per soddisfare i requisiti di rete e assicurati che le comunicazioni siano abilitate sulle porte richieste
2. Rivedi i requisiti degli account di servizio descritti inRequisiti degli account di servizio Active Directory. Assicurati che l'account di servizio disponga delle autorizzazioni delegate necessarie per aggiungere la tua SVM al dominio AD utilizzando l'unità organizzativa specificata.
3. Dopo aver apportato modifiche alle autorizzazioni della porta o all'account di servizio, seguite la procedura descritta in Unire una SVM a un Active Directory utilizzando l'API e AWS Management ConsoleAWS CLI e riprovate ad aggiungere la SVM all'AD.

Amazon FSx non può connettersi ai controller di dominio Active Directory perché le credenziali dell'account di servizio non sono valide

L'aggiunta di una SVM alla tua Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx non è in grado di stabilire una connessione con i controller di dominio Active Directory perché le credenziali dell'account di servizio fornite non sono valide. Per risolvere questo problema,

aggiorna la configurazione di Active Directory della macchina virtuale di storage con un account di servizio valido.

Per risolvere questo problema, utilizzare la procedura descritta in Aggiornamento di una configurazione SVM Active Directory esistente utilizzando l'API AWS Management Console, e AWS CLI Per aggiornare le credenziali dell'account di servizio SVM. Quando inserite il nome utente dell'account di servizio, assicuratevi di includere solo il nome utente (ad esempio,`ServiceAcct`) e di non includere alcun prefisso di dominio (ad esempio,`corp.com\ServiceAcct`) o suffisso di dominio (ad esempio,). `ServiceAcct@corp.com` Non utilizzate il nome distinto (DN) quando inserite il nome utente dell'account di servizio (ad esempio,`CN=ServiceAcct,OU=example,DC=corp,DC=com`).

Amazon FSx non può connettersi ai controller di dominio Active Directory a causa di credenziali dell'account di servizio insufficienti

L'aggiunta di una SVM alla tua Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx non è in grado di stabilire una connessione con i controller di dominio Active Directory. Ciò è dovuto al fatto che i requisiti di porta per Active Directory non sono stati soddisfatti o l'account di servizio fornito non dispone dell'autorizzazione per aggiungere la macchina virtuale di storage al dominio con l'unità organizzativa specificata.

Per risolvere questo problema, assicurati di aver delegato le autorizzazioni richieste all'account di servizio che hai fornito. L'account di servizio deve essere in grado di creare ed eliminare oggetti informatici nell'unità organizzativa del dominio a cui si sta entrando a far parte del file system. L'account di servizio deve inoltre disporre almeno delle autorizzazioni per eseguire le seguenti operazioni:

- Reimpostare le password
- Impedisci agli account di leggere e scrivere dati
- Capacità convalidata di scrittura sull'hostname DNS
- Capacità convalidata di scrivere sul nome principale del servizio
- Capacità di creare ed eliminare oggetti informatici
- Capacità convalidata di leggere e scrivere le restrizioni relative all'account

Per ulteriori informazioni sulla creazione di un account di servizio con le autorizzazioni corrette, consulta Requisiti degli account di servizio Active Directory e. Delega delle autorizzazioni al tuo account di servizio Amazon FSx

Amazon FSx non è in grado di comunicare con i server DNS o i controller di dominio Active Directory

L'aggiunta di una SVM alla tua Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx non è in grado di comunicare con Active Directory. Questo perché Amazon FSx non può raggiungere i server DNS forniti o i controller di dominio per il tuo dominio. Per risolvere questo problema, aggiorna la configurazione Active Directory della tua macchina virtuale di storage con server DNS validi e una configurazione di rete che consenta il flusso del traffico dalla macchina virtuale di storage al controller di dominio.

Per risolvere questo problema, utilizzare la procedura seguente:

1. Se solo alcuni controller di dominio in Active Directory sono raggiungibili, ad esempio a causa di limitazioni geografiche o firewall, puoi aggiungere controller di dominio preferiti. Utilizzando questa opzione, Amazon FSx tenta di contattare i controller di dominio preferiti. Aggiungi i controller di dominio preferiti utilizzando il comando `vserver cifs domain preferred-dc add` NetApp ONTAP CLI, come segue:

   a. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

      ```
      [~]$ ssh fsxadmin@management_endpoint_ip
      ```

      Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

   b. Immettete il seguente comando, dove:

      - `-vserver vserver_name`specifica il nome della macchina virtuale di archiviazione (SVM).
      - `-domain domain_name`specifica il nome completo di Active Directory (FQDN) del dominio a cui appartengono i controller di dominio specificati.

- `-preferred-dc IP_address,…` specifica uno o più indirizzi IP dei controller di dominio preferiti, come elenco delimitato da virgole, in ordine di preferenza.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_name -
domain domain_name -preferred-dc IP_address, …+
```

Il comando seguente aggiunge i controller di dominio 172.17.102.25 e 172.17.102.24 all'elenco dei controller di dominio preferiti utilizzati dal server SMB su SVM vs1 per gestire l'accesso esterno al dominio cifs.lab.example.com.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
 cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. Verifica se il tuo controller di dominio può essere risolto con DNS. Utilizza il comando `vserver services access-check dns forward-lookup` NetApp ONTAP CLI per restituire l'indirizzo IP di un nome host in base alla ricerca sul server DNS specificato o alla configurazione DNS del vserver.

   a. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx NetApp for ONTAP eseguendo il comando seguente. Sostituisci *`management_endpoint_ip`* con l'indirizzo IP della porta di gestione del file system.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   Per ulteriori informazioni, consulta Gestione dei file system con la ONTAP CLI.

   b. Accedere alla modalità avanzata CLI di ONTAP utilizzando il seguente comando.

   ```
   FsxId123456789::> set adv
   ```

   c. Immettete il seguente comando, dove:

   - `-vserver vserver_name`specifica il nome della macchina virtuale di archiviazione (SVM).
   - `-hostname host_name`specifica il nome host da cercare sul server DNS.
   - `-node node_name` specifica il nome del nodo su cui viene eseguito il comando.
   - `-lookup-type`specifica il tipo di indirizzo IP da cercare sul server DNS, l'impostazione predefinita è. `all`

```
FsxId123456789::> vserver services access-check dns forward-lookup \
-vserver vserver_name -node node_name \
-domains domain_name -name-servers dns_server_ip_address \
-hostname host_name
```

3. Rivedi le informazioni di cui hai bisogno per unire una SVM a un AD.
4. Rivedi i requisiti di rete quando unisci una SVM a un AD.
5. Utilizzate la procedura descritta in Requisiti relativi alla configurazione della rete per aggiornare la configurazione AD della SVM utilizzando gli indirizzi IP corretti per i server AD DNS.

Amazon FSx non è in grado di comunicare con Active Directory a causa di un nome di dominio Active Directory non valido.

L'aggiunta di una SVM alla tua Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx ha rilevato che il nome di dominio completo fornito non è valido. Per risolvere questo problema, aggiorna la configurazione di Active Directory della tua macchina virtuale di storage con un FQDN che rispetti i requisiti di configurazione.

Per risolvere questo problema, utilizzare la seguente procedura:

1. Esamina i requisiti del nome di dominio Active Directory locale descritti in Informazioni necessarie per aggiungere un SVM a un Active Directory Assicurati che l'AD a cui stai tentando di aderire soddisfi tale requisito.
2. Utilizza la procedura descritta in Unire una SVM a un Active Directory utilizzando l'API e AWS Management ConsoleAWS CLI e riprova a unire il tuo SVM a un AD. Assicurati di utilizzare il formato corretto per l'FQDN del dominio AD.

L'account di servizio non può accedere al gruppo di amministratori specificato nella configurazione SVM Active Directory

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx non è in grado di applicare la configurazione di Active Directory. Questo perché il gruppo di amministratori che hai fornito non esiste o non è accessibile all'account di servizio che hai fornito. Per risolvere questo problema, assicuratevi che la configurazione di rete consenta il traffico dall'SVM ai controller di dominio e ai server DNS di Active Directory. Aggiorna quindi la configurazione di Active Directory della SVM, fornendo i server DNS di Active Directory e specificando un gruppo di amministratori nel dominio accessibile all'account di servizio fornito.

Per risolvere il problema, procedere come segue:

1. Consultate le informazioni su come fornire un gruppo di dominio per eseguire azioni amministrative sul vostro SVM. Assicurati di utilizzare il nome corretto del gruppo AD Domain Administrators.
2. Utilizzate la procedura descritta in Unire una SVM a un Active Directory utilizzando l'API e AWS Management ConsoleAWS CLI e riprovate ad aggiungere il vostro SVM a un AD.

Amazon FSx non può connettersi ai controller di dominio Active Directory perché l'unità organizzativa specificata non esiste o non è accessibile

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon FSx non è in grado di stabilire una connessione con Active Directory. Questo perché l'unità organizzativa specificata non esiste o non è accessibile all'account di servizio fornito. Per risolvere questo problema, aggiorna la configurazione di Active Directory della macchina virtuale di archiviazione, specificando un'unità organizzativa a cui l'account di servizio dispone delle autorizzazioni per aderire.

Per risolvere il problema, procedere come segue:

1. Rivedi i prerequisiti per unire una SVM a un AD.
2. Rivedi le informazioni di cui hai bisogno per aggiungere una SVM a un AD.
3. Riprova a unire SVM all'AD utilizzando questa procedura con l'unità organizzativa corretta.

Non è possibile eliminare una macchina virtuale o un volume di archiviazione

Ogni file system FSx for ONTAP può contenere una o più macchine virtuali di storage (SVM) e ogni SVM può contenere uno o più volumi. Quando si elimina una risorsa, è necessario innanzitutto assicurarsi che tutti i relativi elementi secondari siano stati eliminati. Ad esempio, prima di eliminare una SVM, è necessario eliminare tutti i volumi non root nella SVM.

> **Important**
>
> Puoi eliminare le macchine virtuali di storage solo utilizzando la console, l'API e la CLI di Amazon FSx. Puoi eliminare i volumi utilizzando la console, l'API o la CLI di Amazon FSx solo se sul volume sono abilitati i backup Amazon FSx.

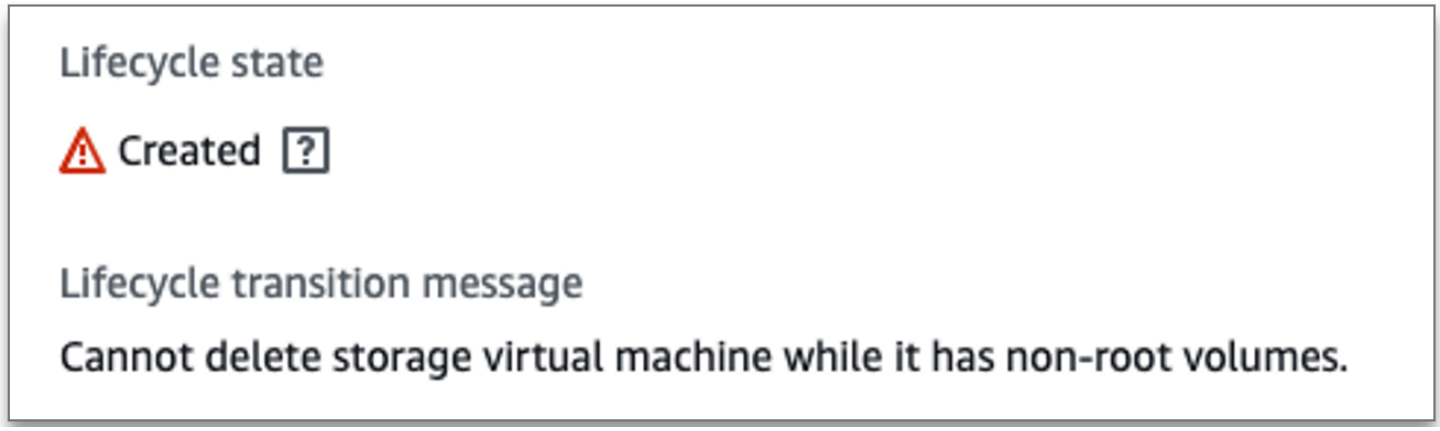
Per proteggere i dati e la configurazione, Amazon FSx impedisce l'eliminazione di SVM e volumi in determinate circostanze. Se tenti di eliminare una SVM o un volume e la richiesta di eliminazione non ha esito positivo, Amazon FSx ti fornisce informazioni nella console AWS Command Line Interface ,AWS CLI() e AWS nell'API sul motivo per cui la risorsa non è stata eliminata. Dopo aver risolto la causa dell'errore di eliminazione, puoi ripetere la richiesta di eliminazione.

Argomenti

Identificazione delle eliminazioni non riuscite

Quando elimini una SVM o un volume Amazon FSx, in genere vedi la transizione `Lifecycle` dello stato della risorsa fino a `DELETING` pochi minuti prima che la risorsa scompaia dalla console, dalla CLI e dall'API di Amazon FSx.

Se tenti di eliminare una risorsa e le relative transizioni di `Lifecycle` stato da a `DELETING` e viceversa`CREATED`, questo comportamento indica che la risorsa non è stata eliminata correttamente. In questo caso, Amazon FSx riporta un'icona di avviso nella console accanto allo stato del `CREATED` ciclo di vita. Scegliendo l'icona di avviso viene visualizzato il motivo dell'eliminazione non riuscita, come mostrato nell'esempio seguente.



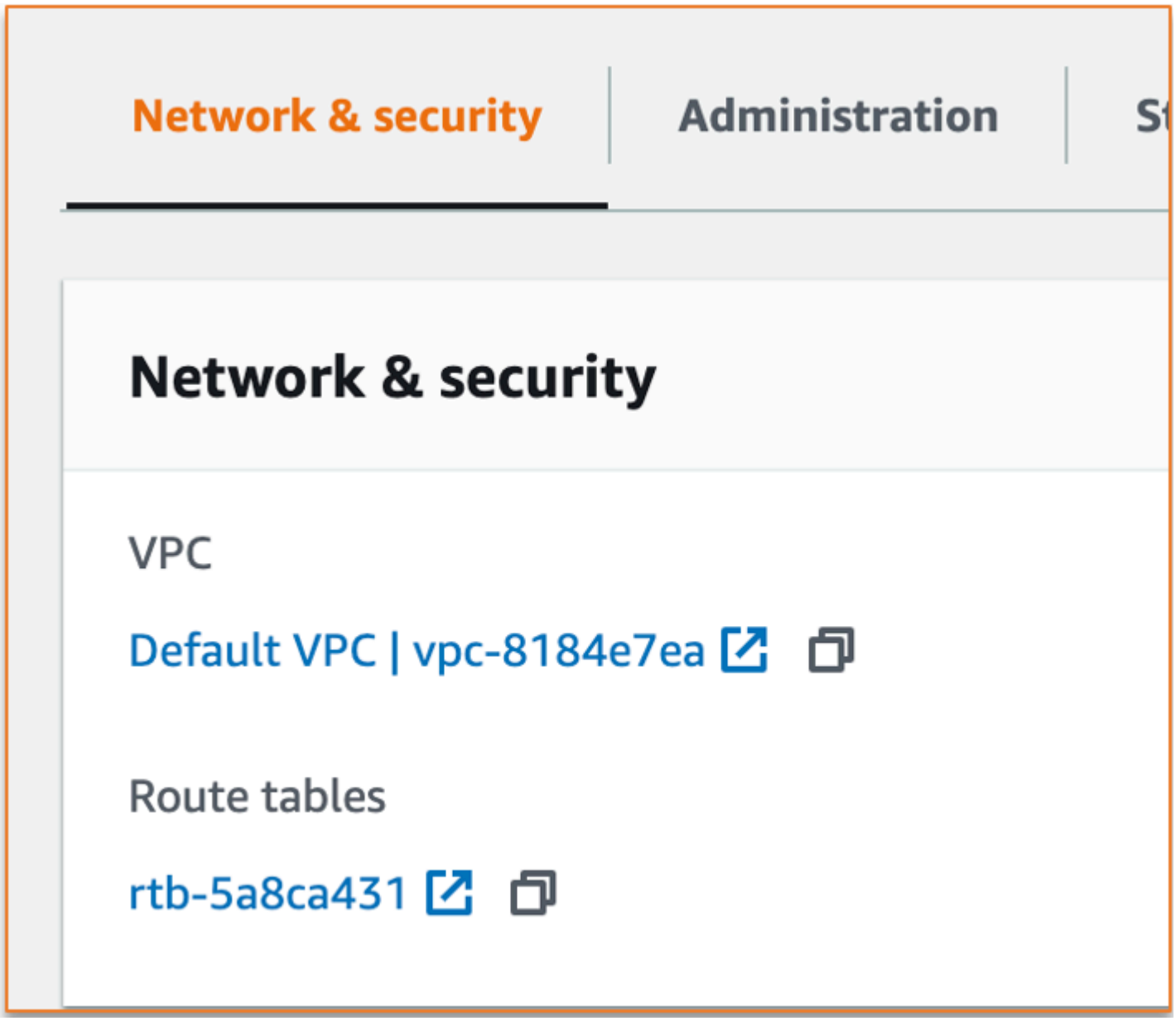
I motivi più comuni per cui Amazon FSx impedisce l'eliminazione di SVM e volumi sono descritti nelle sezioni seguenti, con step-by-step istruzioni su come risolvere questi problemi.

Eliminazione SVM: tabelle di routing inaccessibili

Ogni file system FSx for ONTAP crea una o più voci della tabella di routing per fornire failover e failback automatici tra le zone di disponibilità. Per impostazione predefinita, queste voci della tabella di routing vengono create nella tabella di routing predefinita del VPC. Facoltativamente, è possibile specificare una o più tabelle di routing non predefinite in cui è possibile creare interfacce FSx for ONTAP. Amazon FSx `AmazonFSx` assegna un tag a ogni tabella di routing associata a un file system e, se questo tag viene rimosso, può impedire ad Amazon FSx di eliminare risorse. Se si verifica questa situazione, viene visualizzato quanto segue: `LifecycleTransitionReason`

```
Amazon FSx is unable to complete the requested storage virtual machine
operation because of an inability to access one or more of the route tables
associated with your file system. Please contact AWS Support.
```

Puoi trovare le tabelle di routing del tuo file system nella console Amazon FSx accedendo alla pagina di riepilogo del file system, nella scheda Rete e sicurezza:



Scegliendo il link alle tabelle delle rotte si accede alle tabelle delle rotte. Successivamente, verificate che ciascuna delle tabelle di routing associate al vostro file system sia etichettata con questa coppia chiave-valore:

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

Se questo tag non è presente, ricrealo e poi prova a eliminare nuovamente l'SVM.

Eliminazione SVM: relazione tra pari

Se stai tentando di eliminare una SVM o un volume che fa parte di una relazione tra pari, devi prima eliminare la relazione peer prima di eliminare l'SVM o il volume. Questo requisito impedisce che le SVM peerizzate diventino malsane. Se la SVM non può essere eliminata a causa di una relazione tra pari, viene visualizzato quanto segue: `LifecycleTransitionReason`

Amazon FSx non è in grado di eliminare la macchina virtuale di storage perché fa parte di una relazione peer o di transizione SVM. Elimina la relazione e riprova.

È possibile eliminare le relazioni tra pari SVM tramite la CLI ONTAP. Per accedere alla CLI di ONTAP, segui i passaggi indicati in. Gestione dei file system con la ONTAP CLI Utilizzando la CLI di ONTAP, procedi nel seguente modo.

1. Verificate le relazioni tra pari SVM utilizzando il comando seguente. *svm_name*Sostituiscilo con il nome del tuo SVM.

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

   Se questo comando ha esito positivo, verrà visualizzato un output simile al seguente:

   ```
               Peer        Peer                           Peering        Remote
   Vserver     Vserver     State        Peer Cluster      Applications   Vserver
   ----------- ----------- ------------ ----------------- -------------- ---------
   svm_name    test2       peered       FsxId02d81fef0d84734b6
                                                          snapmirror     fsxDest
   svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                          snapmirror     fsxDest
   ```

```
2 entries were displayed.
```

2. Eliminare ogni relazione tra pari SVM utilizzando il comando seguente. Sostituisci *svm_name* e *remote_svm_name* con i tuoi valori effettivi.

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

Se questo comando ha esito positivo, verrà visualizzato il seguente risultato:

```
Info: 'vserver peer delete' command is successful.
```

Eliminazione di SVM o volume: SnapMirror

Proprio come non è possibile eliminare una SVM con una relazione tra pari senza prima eliminare la relazione tra pari (vediEliminazione SVM: relazione tra pari), non è possibile eliminare una SVM che ha una SnapMirror relazione senza prima eliminare la relazione. SnapMirror Per eliminare la SnapMirror relazione, utilizza la CLI di ONTAP per eseguire le seguenti operazioni sul file system di destinazione della SnapMirror relazione. Per accedere alla CLI di ONTAP, segui i passaggi indicati in. Gestione dei file system con la ONTAP CLI

> **Note**
>
> I backup Amazon FSx vengono utilizzati SnapMirror per creare point-in-time backup incrementali dei volumi del file system. Non puoi eliminare questa SnapMirror relazione per i tuoi backup nella CLI di ONTAP. Tuttavia, questa relazione viene eliminata automaticamente quando si elimina un volume tramite AWS CLI, API o console.

1. Elenca SnapMirror le tue relazioni nel file system di destinazione utilizzando il comando seguente. Sostituiscilo *svm_name* con il nome del tuo SVM.

```
FsxId123456789abcdef::> snapmirror show -vserver svm_name
```

Se questo comando ha esito positivo, verrà visualizzato un output simile al seguente:

```
Source            Destination    Mirror  Relationship   Total             Last
Path        Type  Path           State   Status         Progress  Healthy Updated
```

```
----------- ---- ------------    ------- -------------- --------- ------- --------
sourceSvm:sourceVol
            XDP  destSvm:destVol Snapmirrored
                                      Idle           -         true    -
```

2. Eliminate la SnapMirror relazione eseguendo il comando seguente sul file system di destinazione.

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

Eliminazione SVM: LIF compatibile con Kerberos

Se state tentando di eliminare una SVM dotata di un'interfaccia logica (LIF) con Kerberos abilitato, dovete prima disabilitare Kerberos su quella LIF prima di eliminare l'SVM.

È possibile disabilitare Kerberos su un LIF tramite la CLI ONTAP. Per accedere alla CLI di ONTAP, segui i passaggi indicati in. Gestione dei file system con la ONTAP CLI

1. Accedere alla modalità diagnostica nella CLI di ONTAP utilizzando il comando seguente.

```
FsxId123456789abcdef::> set diag
```

Quando viene richiesto di continuare, immettere. **y**

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

2. Verificate su quali interfacce è abilitato Kerberos. *svm_name*Sostituiscilo con il nome della tua SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Se questo comando ha esito positivo, verrà visualizzato un output simile al seguente:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
```

```
svm_name        nfs_smb_management_1
                              10.19.153.48    enabled
5 entries were displayed.
```

3. Disattivate Kerberos LIF utilizzando il seguente comando. *svm_name*Sostituiscilo con il nome del tuo SVM. Dovrai fornire il nome utente e la password di Active Directory che hai usato per aggiungere questa SVM ad Active Directory.

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

Se questo comando ha esito positivo, verrà visualizzato il seguente output. Fornisci il nome utente e la password di Active Directory che hai usato per aggiungere questa SVM ad Active Directory. Quando ti viene richiesto di continuare, inserisci. **y**

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *************

Warning: This command deletes the service principal name from the machine account
 on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. Verificate che Kerberos sia disabilitato sulla SVM utilizzando il comando seguente. *svm_name*Sostituiscilo con il nome del tuo SVM.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

Se questo comando ha esito positivo, verrà visualizzato un output simile al seguente:

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    disabled
5 entries were displayed.
```

5. Se l'interfaccia è mostrata come`disabled`, prova a eliminare nuovamente l'SVM tramite la AWS CLI, l'API o la console.

   Se non siete riusciti a eliminare il LIF utilizzando i comandi precedenti, potete forzare l'eliminazione del LIF Kerberos utilizzando il comando seguente. Sostituiscilo con il nome del tuo SVM. *svm_name*

   > **Important**
   >
   > Il comando seguente può collocare l'oggetto computer della SVM su Active Directory.

   ```
   FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
    nfs_smb_management_1 -force true
   ```

   Se questo comando ha esito positivo, verrà visualizzato un output simile al seguente. Quando ti viene richiesto di continuare, inserisci**y**.

   ```
   (vserver nfs kerberos interface disable)

   Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver
    "svm_name" will be deleted.
   The corresponding account on the KDC will not be deleted. Do you want to continue?
    {y|n}: y
   ```

Eliminazione SVM: altro motivo

Le SVM FSx for ONTAP creano un oggetto computer in Active Directory quando entrano a far parte di Active Directory. In alcuni casi, potresti voler annullare manualmente l'iscrizione a una SVM da Active Directory utilizzando la CLI di ONTAP. Per accedere alla CLI di ONTAP, segui i passaggi indicati, accedendo alla CLI ONTAP Gestione dei file system con la ONTAP CLI a livello di file system con le credenziali. `fsxadmin` Utilizzando la CLI ONTAP, procedi nel seguente modo per annullare l'accesso a una SVM da Active Directory.

> **Important**
>
> Questa procedura può bloccare l'oggetto computer della SVM su Active Directory.

1. Accedere alla modalità avanzata nella CLI di ONTAP utilizzando il comando seguente.

```
FsxId123456789abcdef::> set adv
```

Dopo aver eseguito questo comando, vedrai questo output. Entra **y** per continuare.

```
Warning: These advanced commands are potentially dangerous; use them only when
      directed to do so by NetApp personnel.
      Do you want to continue? {y|n}: y
```

2. Eliminare il DNS per Active Directory utilizzando il seguente comando. *svm_name*Sostituiscilo con il nome del tuo SVM.

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
 delete -vserver svm_name -lif nfs_smb_management_1
```

> **Note**
>
> Se il record DNS è già stato eliminato o se il server DNS non è raggiungibile, questo comando ha esito negativo. Se ciò accade, continua con il passaggio successivo.

3. Disabilita il DNS utilizzando il seguente comando. *svm_name*Sostituiscilo con il nome del tuo SVM.

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
vserver svm_name -is-enabled false -use-secure false
```

Se questo comando ha esito positivo, verrà visualizzato il seguente risultato:

```
Warning: DNS updates for Vserver "svm_name" are now disabled.
     Any LIFs that are subsequently modified or deleted
     can result in a stale DNS entry on the DNS server,
     even when DNS updates are enabled again.
```

4. Annulla l'accesso al dispositivo da Active Directory. *svm_name*Sostituiscilo con il nome del tuo SVM.

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

Dopo aver eseguito questo comando, vedrai il seguente output, dove *CORP.EXAMPLE.COM* viene sostituito dal nome del tuo dominio. Quando richiesto, inserisci il nome utente e la password. Quando ti viene chiesto se desideri eliminare il server, inserisci**y**.

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
     Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
 server.
     Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

Eliminazione del volume: FlexCache relazione

Non è possibile eliminare i volumi che sono i volumi di origine di una FlexCache relazione a meno che non si elimini prima la relazione nella cache. Per determinare quali volumi hanno una FlexCache relazione, puoi utilizzare la CLI di ONTAP. Per accedere alla CLI di ONTAP, segui i passaggi indicati in. Gestione dei file system con la ONTAP CLI

1. Verifica le FlexCache relazioni utilizzando il comando seguente.

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. Eliminare eventuali relazioni nella cache utilizzando il comando seguente. Sostituisci *dest_svm_name* e *dest_vol_name* con i tuoi valori effettivi.

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. Dopo aver eliminato la relazione con la cache, prova a eliminare nuovamente la SVM tramite la AWS CLI, l'API o la console.

I backup giornalieri automatici falliscono a causa dell'insufficiente capacità di volume

I backup giornalieri automatici del volume falliscono e viene visualizzato il seguente messaggio:

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

I backup giornalieri automatici non funzionano perché la capacità di archiviazione disponibile sul volume è insufficiente. Per mitigare questa condizione, è necessario liberare la capacità di archiviazione sul volume. È possibile eseguire questa operazione utilizzando una o più delle seguenti opzioni, a seconda della situazione:

- Aumentare la capacità di archiviazione del volume
- Aumenta la riserva di istantanee del volume
- Disattiva l'eliminazione automatica delle istantanee
- Non eliminare lo snapshot di backup utilizzando la CLI di ONTAP

La capacità di volume è insufficiente

Se lo spazio sui volumi sta esaurendo, puoi utilizzare le procedure mostrate qui per diagnosticare e risolvere la situazione.

Argomenti

- Determinate come viene utilizzata la capacità di storage del volume
- Aumento della capacità di archiviazione di un volume
- Utilizzo del dimensionamento automatico del volume
- Lo storage principale del file system è pieno
- Eliminazione di snapshot
- Aumento della capacità massima di file di un volume

Determinate come viene utilizzata la capacità di storage del volume

Puoi vedere come viene consumata la capacità di archiviazione del tuo volume utilizzando il comando `volume show-space` NetApp ONTAP CLI. Queste informazioni possono aiutarti a prendere

decisioni su come recuperare o conservare la capacità di archiviazione dei volumi. Per ulteriori informazioni, consulta Per monitorare la capacità di archiviazione di un volume (console).

Aumento della capacità di archiviazione di un volume

Puoi aumentare la capacità di storage di un volume utilizzando la console Amazon FSx e l'API AWS CLI Amazon FSx. Per ulteriori informazioni sull'aggiornamento di un volume con una maggiore capacità, consulta. Aggiornamento di un volume

In alternativa, puoi aumentare la capacità di archiviazione di un volume utilizzando il comando `volume modify` NetApp ONTAP CLI. Per ulteriori informazioni, consulta Per modificare la capacità di archiviazione di un volume (console).

Utilizzo del dimensionamento automatico del volume

È possibile utilizzare il dimensionamento automatico del volume in modo che un volume cresca automaticamente di una quantità specificata o raggiunga una dimensione specificata quando raggiunge una soglia di spazio utilizzata. È possibile eseguire questa operazione per i tipi di FlexVol volume, che è il tipo di volume predefinito per FSx for ONTAP, utilizzando il comando ONTAP `volume autosize` NetApp CLI. Per ulteriori informazioni, consulta Attivazione del dimensionamento automatico del volume.

Lo storage principale del file system è pieno

Se lo storage principale del file system FSx for ONTAP è pieno, non è possibile aggiungere altri dati ai volumi del file system, anche se un volume dimostra di avere una capacità di storage disponibile sufficiente. Puoi visualizzare la quantità di capacità di storage principale disponibile nella scheda Monitoraggio e prestazioni nella pagina dei dettagli del file system nella console Amazon FSx. Per ulteriori informazioni, consultare Monitoraggio dell'utilizzo dello storage SSD

Per risolvere questo problema, puoi aumentare le dimensioni del livello di storage principale del file system. Per ulteriori informazioni, consulta Aggiornamento dello storage SSD e degli IOPS del file system.

Eliminazione di snapshot

Le istantanee sono abilitate per impostazione predefinita sui volumi, utilizzando la politica di snapshot predefinita. Le istantanee vengono archiviate nella `.snapshot` directory alla radice di un volume. È possibile gestire la capacità di archiviazione dei volumi rispetto alle istantanee nei seguenti modi:

- Eliminazione manuale delle istantanee: recupera la capacità di archiviazione eliminando le istantanee manualmente.
- Crea una politica di eliminazione automatica delle istantanee: crea una politica che elimini le istantanee in modo più aggressivo rispetto alla politica predefinita delle istantanee.
- Disattiva le istantanee automatiche: conserva la capacità di archiviazione disattivando le istantanee automatiche.

Per ulteriori informazioni sull'eliminazione delle istantanee e sulla gestione delle politiche relative alle istantanee per conservare la capacità di storage, vedere. Eliminazione di snapshot

Aumento della capacità massima di file di un volume

Un volume FSx for ONTAP può esaurire la capacità dei file quando il numero di inode o puntatori di file disponibili è esaurito. Per impostazione predefinita, il numero di inode disponibili su un volume è 1 per ogni 32 KiB di dimensione del volume. Per ulteriori informazioni, consulta Capacità dei file di volume.

Il numero di inode in un volume aumenta proporzionalmente alla capacità di archiviazione del volume, fino a una soglia di 648 GiB. Per impostazione predefinita, i volumi con una capacità di archiviazione pari o superiore a 648 GiB hanno tutti lo stesso numero di inode, 21.251.126. Per visualizzare la capacità massima di file di un volume, vedere. Visualizzazione della capacità dei file di un volume

Se si crea un volume più grande di 648 GiB e si desidera avere più di 21.251.126 inode, è necessario aumentare manualmente il numero massimo di file sul volume. Se la capacità di archiviazione del volume sta esaurendo, puoi verificarne la capacità massima di file. Se si avvicina alla capacità dei file, puoi aumentarla manualmente. Per ulteriori informazioni, consulta Per aumentare il numero massimo di file su un volume (ONTAPCLI).

Risoluzione dei problemi di rete

Se si verificano problemi di rete, è possibile utilizzare le procedure illustrate di seguito per diagnosticare il problema.

Si desidera acquisire una traccia di pacchetto

Il tracciamento dei pacchetti è il processo di verifica del percorso di un pacchetto attraverso i livelli fino alla sua destinazione. Puoi controllare il processo di tracciamento dei pacchetti con i seguenti comandi NetApp ONTAP CLI:

- network tcpdump start— Avvia il tracciamento dei pacchetti
- network tcpdump show— Mostra le tracce dei pacchetti attualmente in esecuzione
- network tcpdump stop— Interrompe una traccia di pacchetti in esecuzione

Questi comandi sono disponibili per gli utenti che hanno il `fsxadmin` ruolo nel file system dell'utente.

Per acquisire una traccia di pacchetto dal file system

1. Per accedere tramite SSH alla NetApp CLI ONTAP del tuo file system, segui i passaggi documentati nella sezione della Guida per Utilizzo della CLI NetApp ONTAP l'utente di Amazon FSx for ONTAP. NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Immettere il livello di privilegio di diagnostica nella CLI di ONTAP utilizzando il comando seguente.

   ```
   ::> set diag
   ```

   Quando viene richiesto di continuare, immettere. y

   ```
   Warning: These diagnostic commands are for use by NetApp personnel only.
   Do you want to continue? {y|n}: y
   ```

3. Identificate la posizione sul file system in cui desiderate salvare la traccia dei pacchetti. Il volume deve essere online e deve essere montato nel namespace con un percorso di giunzione valido. Utilizzate il seguente comando per verificare i volumi che soddisfano questi criteri:

   ```
   ::*> volume show -junction-path !- -fields junction-path
   vserver volume    junction-path
   ------- --------- -------------
   fsx     test_vol1 /test_vol1
   fsx     test_vol2 /test_vol2
   fsx     test_vol2 /test_vol3
   ```

4. Avviate la traccia con gli argomenti minimi richiesti. Sostituisci quanto segue:

   - Sostituite *node_name* con il nome del nodo (ad esempio,). `FsxId01234567890abcdef-01`

- Sostituisci *svm_name con il nome* della tua macchina virtuale di archiviazione (ad esempio,). `fsx`
- *Sostituite junction_path_name con il nome del volume* (ad esempio,). `test-vol1`

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
 e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
 packet traces are occurring. Use the
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
 disable Snapshots on the
tcpdump destination volume.
```

> **Important**
>
> Le tracce dei pacchetti possono essere acquisite solo sull'interfaccia e nello `e0e` spazio IP. `Default` In FSx for ONTAP, tutto il traffico di rete utilizza l'interfaccia. `e0e`

Quando utilizzate il tracciamento dei pacchetti, tenete presente quanto segue:

- *Quando si avvia una traccia dei pacchetti, è necessario includere il percorso in cui si desidera memorizzare i file di traccia, in questo formato: /clus/ svm_name/junction-path-name*
- Facoltativamente, fornite il nome del file per la traccia del pacchetto. *Se il filter_name non è specificato, viene generato automaticamente nel formato: node-name _ port-name _ yyyymmdd_hhmmss .trc*
- Se vengono specificate tracce di rotolamento, al filter_name viene aggiunto un numero che indica la posizione nella sequenza di rotazione.
- L'ONTAP CLI accetta anche i seguenti -pass-through argomenti opzionali:

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
```

```
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
<filter-expression>
```

- Per informazioni sulle espressioni di filtro, vedere la pagina man di pcap-filter (7).

5. Visualizza le tracce in corso:

```
::*> debug network tcpdump show
Node                     IPspace  Port     Filename
-----------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. Interrompi la traccia:

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

7. Ritorna al livello di privilegi di amministratore:

```
::*> set -priv admin
::>
```

8. Accedi alle tracce dei pacchetti.

   Le tracce dei pacchetti sono archiviate nel volume specificato utilizzando il debug network tcpdump start comando ed è possibile accedervi tramite l'esportazione NFS o una condivisione SMB corrispondente a quel volume.

Per ulteriori informazioni sull'acquisizione delle tracce dei pacchetti, vedere Come usare debug network tcpdump in ONTAP 9.10+ nella Knowledge Base. NetApp

Cronologia dei documenti per Amazon FSx for ONTAP NetApp

- Versione API: 2018-03-01
- Ultimo aggiornamento della documentazione: 30 aprile 2024

La tabella seguente descrive le modifiche importanti alla Guida per l'utente di Amazon FSx NetApp ONTAP. Per ricevere notifiche sugli aggiornamenti della documentazione, è possibile sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Support aggiunto per il `fsxadmin-readonly` ruolo degli utenti amministratori del file system	Il `fsxadmin-readonly` ruolo è ora disponibile per gli utenti amministratori del ONTAP file system e può essere utilizzato per applicazioni di monitoraggio del file system comeNetApp Harvest. Per ulteriori informazioni, vedere Ruoli e utenti dell'amministratore del file system.	30 aprile 2024
Support aggiunto per l'autenticazione a chiave pubblica SSH per gli utenti amministrativi del dominio Windows	È ora possibile utilizzare l'autenticazione a chiave pubblica SSH con il file system di dominio Active Directory e gli utenti SVM. Per ulteriori informazioni, consulta https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/set-up-ad-auth.html.	30 aprile 2024

Support aggiunto per 12 coppie HA nei file system con scalabilità orizzontale	Amazon FSx for NetApp ONTAP ha aggiunto il supporto per 12 coppie HA in file system con scalabilità orizzontale. I file system con 12 coppie HA possono fornire fino a 72 GBps di capacità di throughput e 2.400.000 IOPS SSD in 12 coppie ad alta disponibilità (HA). Per ulteriori informazioni, consulta Coppie ad alta disponibilità (HA) e prestazioni Amazon FSx NetApp for ONTAP.	4 marzo 2024
Support aggiunto per la modalità di scrittura su cloud	Amazon FSx for NetApp ONTAP ha aggiunto il supporto per la modalità di scrittura su cloud per i volumi. Per ulteriori informazioni, consulta Abilitazione della modalità di scrittura su cloud su un volume.	6 febbraio 2024
Support aggiunto per il backup FlexGroup dei volumi con AWS Backup	È ora possibile AWS Backup utilizzarlo per eseguire il backup e il ripristino FlexGroup dei volumi sui file system FSx for ONTAP. Per ulteriori informazioni, consulta Using AWS Backup with Amazon FSx.	11 gennaio 2024

Amazon FSX ha aggiornato le politiche gestite di AmazonFSx FullAccess, AmazonFSx ConsoleFullAccess, AmazonF e SxReadOnlyAccess AmazonF SxConsole ReadOnlyAccess SxService RolePolicy AWS	Amazon FSX ha aggiornato le politiche AmazonFSx FullAccess, AmazonF, AmazonF SxConsoleFullAccess e AmazonF per SxReadOnlyAccess aggiungere l'autorizzazioneSxConsoleReadOnlyAccess. SxService RolePolicy `ec2:GetSecurityGroupsForVpc` Per ulteriori informazioni, consulta gli aggiornamenti di Amazon FSx alle policy AWS gestite.	9 gennaio 2024
Amazon FSx ha aggiornato le politiche gestite di AmazonF SxFullAccess e AmazonF SxConsoleFullAccess AWS	Amazon FSx ha aggiornato le politiche AmazonF SxFullAccess e AmazonF SxConsole FullAccess per aggiungere l'azione. `ManageCrossAccountDataReplication` Per ulteriori informazioni, consulta gli aggiornamenti di Amazon FSx alle policy AWS gestite.	20 dicembre 2023
Support aggiunto per metriche scalabili	FSx for ONTAP ora fornisce i CloudWatch parametri di Amazon per i file system con più coppie HA. Per ulteriori informazioni, consulta le metriche del file system con scalabilità orizzontale.	26 novembre 2023

Support aggiunto per file system con scalabilità orizzontale	Amazon FSx for NetApp ONTAP ha aggiunto il supporto per file system scalabili in grado di fornire fino a 36 GBps di capacità di throughput e 1.200.000 IOPS SSD su sei coppie ad alta disponibilità (HA). Per ulteriori informazioni, consulta Coppie ad alta disponibilità (HA) e prestazioni Amazon FSx NetApp for ONTAP.	26 novembre 2023
Support aggiunto per i FlexGroup volumi	Amazon FSx for NetApp ONTAP ha aggiunto il supporto per i volumi. FlexGroup Per ulteriori informazioni, consulta Volume styles.	26 novembre 2023
Supporto VPC condiviso aggiunto per i file system Multi-AZ	Gli account dei partecipanti possono ora creare file system Multi-AZ in un VPC condiviso con loro. Gli account proprieta ri possono gestire questa funzionalità nella console, nella CLI e nell'API di Amazon FSx. Per ulteriori informazi oni, vedere Creazione di file system FSx for ONTAP in sottoreti condivise	26 novembre 2023

Amazon FSx ha aggiornato le politiche gestite di AmazonF SxFullAccess e AmazonF SxConsoleFullAccess AWS	Amazon FSx ha aggiornato le politiche AmazonF SxFullAcc ess e AmazonF SxConsole FullAccess per aggiungere l'autorizzazione. `fsx:CopyS napshotAndUpdateVo lume` Per ulteriori informazi oni, consulta gli aggiornam enti di Amazon FSx alle policy AWS gestite.	26 novembre 2023
Amazon FSx ha aggiornato le politiche gestite di AmazonF SxFullAccess e AmazonF SxConsoleFullAccess AWS	Amazon FSX ha aggiornato le SxConsoleFullAccess politiche AmazonF SxFullAccess e AmazonF per aggiungere le autorizzazioni e. `fsx:Descr ibeSharedVPCConfig uration` `fsx:Updat eSharedVPCConfigur ation` Per ulteriori informazi oni, consulta gli aggiornam enti di Amazon FSx alle policy AWS gestite.	14 novembre 2023
Support aggiunto per la creazione di ruoli e utenti ONTAP aggiuntivi	Amazon FSx for NetApp ONTAP ora supporta la creazione di ruoli e utenti ONTAP aggiuntivi per definire le capacità e i privilegi degli utenti quando utilizzano la CLI di ONTAP e l'API REST. Per ulteriori informazioni, consulta Ruoli e utenti in Amazon FSx for NetApp ONTAP.	6 settembre 2023

Support aggiunto per CloudWatch metriche aggiuntive e una dashboard di monitoraggio migliorata	FSx for ONTAP offre ora metriche prestazionali aggiuntive e un dashboard di monitoraggio avanzato per una migliore visibilità sull'attività del file system. Per ulteriori informazioni, vedere Monitoraggio con. CloudWatch	17 agosto 2023
Amazon FSx ha aggiornato la policy gestita di SxService RolePolicy AWS AmazonF	Amazon FSx ha aggiornato l'`cloudwatch:PutMetricData` autorizzazione in AmazonF. SxServiceRolePolicy Per ulteriori informazioni, consulta gli aggiornamenti di Amazon FSx alle policy AWS gestite.	24 luglio 2023
Support aggiunto per l'utilizzo diretto NetApp di System Manager	È possibile gestire i file system FSx for ONTAP utilizzando System Manager direttamente da. NetApp BlueXP Per ulteriori informazioni, vedere Utilizzo di NetApp System Manager con BlueXP.	13 luglio 2023
Support aggiunto per il monitoraggio degli eventi EMS	È possibile monitorare gli eventi del file system FSx for ONTAP utilizzando il file system nativo di NetApp ONTAP. Events Management System (EMS) È possibile visualizzare gli eventi EMS utilizzando la CLI di NetApp ONTAP. Per ulteriori informazioni, consulta Monitoring FSx for ONTAP EMS events.	13 luglio 2023

Support aggiunto per SnapLock	FSx for ONTAP ora supporta i volumi. SnapLock SnapLockc onsente di proteggere i file passando allo stato WORM (Write Once, Read Many), che impedisce la modifica o l'eliminazione per un periodo di conservazione specifica to. FSx for ONTAP supporta le modalità di conservazione Compliance e Enterprise con. SnapLock Per ulteriori informazioni, vedere Working with. SnapLock	13 luglio 2023
Support aggiunto per la crittografia IPSec dei dati in transito	FSx for ONTAP ora supporta l'utilizzo della crittografia IPSec per crittografare i dati in transito tra file system e client connessi. Per ulteriori informazioni, vedere Configura zione di IPSec utilizzan do l'autenticazione PSK e Configurazione di IPSec utilizzando l'autenticazione dei certificati.	13 luglio 2023
La dimensione massima del volume è aumentata	FSx for ONTAP ha aggiornat o la dimensione massima di un volume da 100 TB a 300 TB. Per ulteriori informazioni, consulta Attivare il dimension amento automatico dei volumi.	13 luglio 2023

Amazon FSx ha aggiornato la policy gestita di SxFullAccess AWS AmazonF	Amazon FSx ha aggiornato la SxFullAccess policy di AmazonF per rimuovere l'`fsx:*`autorizzazione e aggiungere azioni specifiche. `fsx` Per ulteriori informazioni, consulta la politica di AmazonF. SxFullAccess	13 luglio 2023
Amazon FSx ha aggiornato la policy gestita di SxConsole FullAccess AWS AmazonF	Amazon FSx ha aggiornato la SxConsoleFullAccess policy di AmazonF per rimuovere l'`fsx:*`autorizzazione e aggiungere azioni specifiche. `fsx` Per ulteriori informazioni, consulta la politica di AmazonF. SxConsole FullAccess	13 luglio 2023
Support aggiunto per unire macchine virtuali di archiviazione esistenti a un Active Directory	È possibile unire le macchine virtuali di archiviazione esistenti a un Active Directory utilizzando AWS Management Console l'API AWS CLI e. Per ulteriori informazioni, vedere Aggiungere una SVM a un Active Directory.	13 giugno 2023

Support per la cache di lettura NVMe aggiunto per i file system Single-AZ	La cache di lettura NVMe è ora supportata per i file system Single-AZ creati dopo il 28 novembre 2022 con almeno 2 GBps di capacità di throughput nella regione Stati Uniti orientali (Ohio), nella regione Stati Uniti orientali (Virginia settentrionale), nella regione Stati Uniti occidentali (Oregon) ed Europa (Irlanda). Per ulteriori informazioni, consulta Impatto del tipo di implementazione sulle prestazioni.	28 novembre 2022
Support aggiunto per l'utilizzo di intervalli di indirizzi IP in-VPC per creare file system Multi-AZ	Ora puoi creare file system Multi-AZ FSx for ONTAP specificando gli endpoint che rientrano nell'intervallo di indirizzi IP del tuo VPC. Per ulteriori informazioni, vedere Creazione di FSx per i file system ONTAP.	28 novembre 2022
Support aggiunto per l'aggiornamento delle tabelle di routing VPC su file system Multi-AZ	È ora possibile associare (aggiungere) una nuova tabella di routing VPC a un file system Multi-AZ FSx for ONTAP esistente o dissociare (rimuovere) una tabella di routing VPC esistente da un file system Multi-AZ FSx for ONTAP esistente. Per ulteriori informazioni, vedere Aggiornamento di un file system.	28 novembre 2022

Support aggiunto per la crittografia dei dati in transito con AWS Nitro System	I dati in transito vengono crittografati automaticamente quando vi si accede da istanze Amazon EC2 supportate nella regione Stati Uniti orientali (Ohio), nella regione Stati Uniti orientali (Virginia settentrionale), nella regione Stati Uniti occidentali (Oregon) e in Europa (Irlanda). Per ulteriori informazioni, consulta Crittografia dei dati in transito con Nitro System. AWS	28 novembre 2022
Support aggiunto per la creazione di volumi DP	Ora puoi creare volumi DP (protezione dei dati) utilizzando la console Amazon FSx o l'API AWS CLI Amazon FSx. Puoi utilizzare i volumi DP come destinazione di una SnapVault relazione NetApp SnapMirror OR, quando desideri migrare o proteggere i dati di un singolo volume. Per ulteriori informazioni, consulta Tipi di volume.	28 novembre 2022
Support aggiunto per la copia dei tag di volume nei backup	Ora puoi abilitare `CopyTagsToBackups` l'API AWS CLI o Amazon FSx per copiare automaticamente i tag dai tuoi volumi ai backup. Per ulteriori informazioni, consulta Copiare i tag nei backup.	28 novembre 2022

Support aggiunto per la scelta di una policy di snapshot	Ora puoi scegliere tra tre policy di snapshot integrate durante la creazione o l'aggiornamento di un volume utilizzando la console AWS CLI Amazon FSx o l'API Amazon FSx. Puoi anche selezionare una policy di snapshot personalizzata che hai creato nella CLI ONTAP o nell'API REST. Per ulteriori informazioni, consulta le politiche relative agli snapshot.	28 novembre 2022
Support aggiunto per un'opzione di capacità di throughput aggiuntiva del file system	FSx for ONTAP ora supporta 4.096 MBps di capacità di throughput per i file system creati dopo il 28 novembre 2022 nella regione Stati Uniti orientali (Ohio), nella regione Stati Uniti orientali (Virginia settentrionale), nella regione Stati Uniti occidentali (Oregon) ed Europa (Irlanda) . Per ulteriori informazioni, consulta Impatto della capacità di throughput sulle prestazioni.	28 novembre 2022

Support aggiunto per IOPS SSD aggiuntivi	FSx for ONTAP ora supporta 160.000 IOPS SSD per file system creati dopo il 28 novembre 2022 nella regione Stati Uniti orientali (Ohio), nella regione Stati Uniti orientali (Virginia settentrionale), nella regione Stati Uniti occidentali (Oregon) ed Europa (Irlanda). Per ulteriori informazioni, consulta Impatto della capacità di throughput sulle prestazioni.	28 novembre 2022
Support aggiunto per l'utilizzo di FSx for ONTAP come datastore esterno per VMware Cloud on AWS	È possibile utilizzare FSx for ONTAP come datastore esterno per VMware Cloud on AWS Software-Defined Data Center (SDDC). Questo supporto aggiuntivo offre la flessibilità necessaria per aumentare o ridurre lo storage indipendentemente dalle risorse di elaborazione per VMware Cloud sui carichi di lavoro. AWS Per ulteriori informazioni, vedere Utilizzo di VMware Cloud with FSx for ONTAP.	30 agosto 2022

Aumenta automaticamente la capacità di storage di un file system	Utilizza un AWS CloudFormation modello personalizzabile AWS sviluppato per aumentare automaticamente la capacità di archiviazione del file system quando la quantità di capacità di archiviazione SSD utilizzata supera una soglia specificata. Per ulteriori informazioni, consulta Aumentare dinamicamente la capacità di archiviazione SSD.	3 giugno 2022
Amazon FSx è ora integrato con AWS Backup	Ora puoi utilizzarli AWS Backup per eseguire il backup e il ripristino dei file system FSx oltre a utilizzare i backup nativi di Amazon FSx. Per ulteriori informazioni, consulta Using AWS Backup with Amazon FSx.	18 maggio 2022
Support aggiunto per le implementazioni di file system ONTAP in una singola zona di disponibilità	È possibile creare FSx Single-AZ per i file system ONTAP, progettati per fornire disponibilità e durabilità elevate all'interno di una singola zona di disponibilità (AZ). Per ulteriori informazioni, vedere Scelta della distribuzione del file system.	13 aprile 2022

Support aggiunto per gli AWS PrivateLink endpoint VPC di interfaccia	Ora puoi utilizzare gli endpoint VPC dell'interfaccia per accedere all'API Amazon FSx 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 la modifica della capacità di throughput per i file system ONTAP esistenti	È ora possibile modificar e la capacità di throughput disponibile per i file system ONTAP esistenti. Per ulteriori informazioni, vedere Gestione della capacità di throughput.	30 marzo 2022
Support aggiunto per la capacità di archiviazione SSD e la scalabilità IOPS fornita	Ora puoi aumentare la capacità di archiviazione SSD e fornire IOPS per i file system FSx for ONTAP esistenti man mano che i requisiti di storage e IOPS evolvono. Per ulteriori informazioni, vedere Gestione della capacità di storage e provisioning degli IOPS.	25 gennaio 2022
Support aggiunto per i CloudWatch parametri di Amazon	Puoi monitorare il tuo file system utilizzando Amazon CloudWatch, che raccoglie ed elabora i dati grezzi da FSx for ONTAP in metriche leggibili quasi in tempo reale. Per ulteriori informazioni, consulta Monitoraggio con Amazon CloudWatch.	19 gennaio 2022

Support aggiunto per ulteriori opzioni di throughput del file system	FSx for ONTAP ora supporta le opzioni da 128 MB/s e 256 MB/s per il throughput del file system. Per ulteriori informazioni, consulta Impatto della capacità di throughput sulle prestazioni.	30 novembre 2021
Amazon FSx for NetApp ONTAP è ora disponibile a livello generale	FSx for ONTAP è un servizio completamente gestito che fornisce uno storage di file altamente affidabile, scalabile, performante e ricco di funzionalità basato sul file system ONTAP. NetApp Fornisce le caratteristiche, le prestazioni, le funzionalità e le API familiari dei NetApp file system con l'agilità, la scalabilità e la semplicità di un servizio completamente gestito. AWS	2 settembre 2021

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.