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 NetApp popolare file system ONTAP. 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 SSD (Solid State Drive) 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 puoi creare istantanee, clonare e replicare i tuoi file con un semplice clic. Inoltre, FSx per 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 duraturo con backup completamente gestiti e supporto per il disaster recovery interregionale. Per semplificare la protezione e la protezione dei dati, FSx for ONTAP supporta le più diffuse applicazioni antivirus e di sicurezza dei dati.

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

Essendo un servizio completamente gestito, FSx for ONTAP semplifica il lancio 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 archiviazione dei file completamente gestita con:

- Support per set di dati su scala petabyte in un unico namespace
- Fino a decine di gigabyte al secondo () di velocità effettiva per file system GBps
- Accesso multiprotocollo ai dati tramite i protocolli Network File System (NFS), Server Message Block (SMB), Internet Small Computer Systems Interface (iSCSI) e Non-Volatile Memory Express () NVMe
- 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
- Supporto per due opzioni di tipo di rete, IPv4 -only e dual-stack (che supporta entrambe IPv4 e IPv6), per accedere e gestire il file system
- Support per la SnapMirrorfunzionalità NetApp di replica
- Support per NetApp la soluzione di FlexCache caching locale
- Support per l'accesso e la gestione tramite operazioni native AWS o NetApp strumenti e API
  - Console di gestione AWS, AWS Command Line Interface (AWS CLI) e SDKs
  - NetApp CLI ONTAP, API REST e console NetApp

Sicurezza e protezione dei dati

Il modello di responsabilità condivisa viene utilizzato in relazione aSicurezza in Amazon FSx per NetApp ONTAP. Amazon FSx offre diversi livelli di sicurezza e conformità per facilitare la protezione dei dati.

FSx for ONTAP supporta le seguenti funzionalità di protezione dei dati, sicurezza e controllo degli accessi:

- Crittografia dei dati inattivi per i dati del file system e i backup utilizzando AWS KMS keys
- Crittografia dei dati in transito utilizzando:
  - Kerberos SMB
  - IPSEC
  - Crittografia basata su N
- Scansione antivirus su richiesta
- Autenticazione e autorizzazione tramite Microsoft Active Directory
- Controllo dell'accesso ai file
- NetAppSnapLockWORM con modalità di conservazione Compliance ed Enterprise

Per ulteriori informazioni, consultare Protezione dei dati in Amazon FSx per NetApp ONTAP e Protezione dei dati.

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 Protezione dei dati.

Strumenti di monitoraggio

Gli strumenti di monitoraggio includono CloudWatchCloudTrail, eventi ONTAP EMS, NetAppData Infrastructure Insights e NetAppHarvest.

Prezzi di FSx 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 di cui effettui il provisioning superiore a tre (per IOPS al mese) IOPS/GB
- Capacità di throughput (per megabyte al secondo [] -mese) MBps
- 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.

FSx per ONTAP su AWS re:Post

Se riscontri problemi durante l'utilizzo di Amazon FSx, usali AWS re:Postper ottenere risposte alle tue domande su FSx for ONTAP.

Sei un FSx utente Amazon per la prima volta?

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

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

Come funziona Amazon FSx for NetApp ONTAP

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

Argomenti

FSx per i file system ONTAP

Un file system è la risorsa principale FSx per ONTAP, analogamente 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 ONTAP FSx.

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 ONTAP FSx di prima generazione e i file system Multi-AZ di seconda generazione supportano una coppia HA. I file system Single-AZ di seconda generazione supportano fino a 12 coppie HA. Per ulteriori informazioni, consulta Gestione delle 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 si accede 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 SVMs.

È possibile iscriversi SVMs 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 ONTAP.

Volumi

FSx i volumi for ONTAP sono risorse virtuali utilizzate per organizzare e raggruppare i dati. I volumi sono contenitori logici ospitati su e SVMs 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

FSx i volumi for ONTAP sono dotati di thin provisioning, il che significa che consumano solo la capacità di archiviazione per i dati in essi contenuti. 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 FSx volumi ONTAP.

Livelli di storage

Il file system An 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, progettato 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 FSx per i livelli di storage ONTAP. È possibile aumentare la capacità di archiviazione SSD del file system man mano che le esigenze di archiviazione crescono. Sui file system di seconda generazione, puoi anche ridurre la capacità di archiviazione SSD quando cambiano i requisiti di archiviazione ad alte prestazioni, ottimizzando i costi di archiviazione. Per ulteriori informazioni, consulta Capacità di storage del file system e IOPS.

Tiering di dati

Il data tiering è il processo mediante il quale Amazon FSx for NetApp 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 volumi di 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 Efficienza dello storage.

Accesso ai dati archiviati sui file system ONTAP FSx

Puoi accedere ai tuoi dati su FSx volumi 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 a blocchi Non-Volatile Memory Express (NVMe) e Internet Small Computer Systems Interface (iSCSI). Per ulteriori informazioni, consulta Accesso ai dati di FSx for ONTAP.

Gestione delle risorse ONTAP FSx

Esistono diversi modi per interagire con il file system FSx for ONTAP e gestirne le risorse. Puoi gestire le tue risorse FSx for ONTAP utilizzando sia gli strumenti di gestione di ONTAP che quelli AWS di NetApp ONTAP:

- AWS strumenti di gestione
  - La Console di gestione AWS
  - Il AWS Command Line Interface (AWS CLI)

  - L' FSx API Amazon e SDKs
  - AWS CloudFormation
- NetApp strumenti di gestione:
  - NetApp Console
  - La CLI NetApp di ONTAP
  - L'API REST NetApp ONTAP

Per ulteriori informazioni, consulta Amministrazione delle risorse.

Guida introduttiva ad Amazon FSx for NetApp ONTAP

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

1. Registrati Account AWS e crea un utente amministrativo nell'account.
2. Crea un file system Amazon FSx for NetApp ONTAP utilizzando la FSx console Amazon.
3. Installa il tuo file system da un'istanza Amazon EC2 Linux.
4. Eliminare tutte le risorse create.

Argomenti

Configurazione 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 https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

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

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

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

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

1. Accedi Console di gestione AWScome 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 Accedere come utente root nella 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 il Centro identità IAM.

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

2. Nel Centro identità IAM, assegna l'accesso amministrativo a un utente.

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

Accesso come utente amministratore

- Per accedere come utente del Centro identità IAM, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente del Centro identità IAM.

  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.

Assegnazione dell'accesso ad altri utenti

1. Nel Centro identità IAM, crea un set di autorizzazioni conforme alla best practice per l'applicazione di autorizzazioni con il privilegio minimo.

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

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

Approfondimenti

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

Crea un file system Amazon FSx for NetApp ONTAP

La FSx console Amazon 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, usa l'opzione Quick create.

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, è possibile creare volumi aggiuntivi SVMs in base alle esigenze, tra cui una SVM unita a un Active Directory per consentire l'accesso dai client Windows e macOS tramite il protocollo Server Message Block (SMB). È inoltre possibile aggiungere ulteriori coppie ad alta disponibilità (HA) a seconda del tipo di distribuzione scelto e del numero di coppie HA aggiunte al momento della creazione.

> **Note**
>
> FSx per i file system ONTAP creati con l'opzione di creazione rapida, utilizza un tipo di rete di. `IPv4` Per creare un file system con un tipo di rete di `Dual-stack` (che supporta entrambi IPv4 e IPv6), utilizzate l'opzione di creazione Standard.

Per informazioni sull'utilizzo dell'opzione di creazione Standard per creare un file system con una configurazione personalizzata e sull'utilizzo dell'API AWS CLI and, vedereCreazione di file system.

Per creare il file system

1. Apri la FSx console Amazon 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, scegliete 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, durabilità e opzioni di implementazione.

> **Note**
>
> FSx Per impostazione predefinita, viene scelta la generazione di file system ONTAP di ultima generazione disponibile per l'utente Regione AWS . È possibile specificare la generazione del file system (se disponibile Regioni AWS) con l'opzione di creazione Standard. Per ulteriori informazioni, consulta Creazione di file system.

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 1.048.576. 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 fornisce FSx automaticamente la capacità di throughput consigliata in base allo storage SSD. Puoi anche scegliere la velocità effettiva del tuo file system (fino a 73.728 a MBps seconda del tipo di implementazione e della quantità di coppie HA).
9. Per il Virtual Private Cloud (VPC), scegli l'Amazon VPC che desideri associare al tuo file system.
10. (Solo Multi-AZ) L'intervallo di indirizzi IP degli 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 IPv4 indirizzi non allocato 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 endpoint IPv4 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 ne ospita 10 SVMs 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 IPv4 indirizzi fluttuante all'esterno del tuo VPC: scegli questa opzione per fare in modo che FSx Amazon 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 di creazione standard. L'intervallo di indirizzi IP che scegli può essere interno o esterno all'intervallo di IPv4 indirizzi del VPC, purché non si sovrapponga a nessuna sottorete e purché non sia già utilizzato da un altro file system con lo stesso VPC e le stesse tabelle di routing. Ti consigliamo di utilizzare un intervallo compreso nell'intervallo di indirizzi IP del VPC.

> **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 dei file system

11. Per l'efficienza dello storage, scegli Abilitato per attivare le funzionalità di efficienza dello storage ONTAP (compressione, deduplicazione e compattazione) o Disabilitato per disattivarle.
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.

Creazione di una SVM aggiunta a Microsoft Active Directory

Dopo aver creato il file system, puoi crearne altri SVMs uniti a Microsoft Active Directory per consentire l'accesso SMB dai client Windows e macOS. FSx for ONTAP si integra con per Gestione dei segreti AWS gestire in modo sicuro le credenziali dell'account del servizio di accesso al dominio Microsoft Active Directory.

Per creare una SVM aggiunta a Microsoft Active Directory

1. Nella FSx console Amazon, scegli Storage virtual machines dal riquadro di navigazione a sinistra.
2. Scegli Crea macchina virtuale di archiviazione.
3. Per File system, seleziona il file system che hai creato.
4. Per Storage virtual machine name, inserisci un nome per la tua SVM.
5. Per la configurazione di Microsoft Active Directory, scegli Unisciti a Microsoft Active Directory.
6. Per le credenziali dell'account del servizio di accesso al dominio, scegli Gestito in Secrets Manager (impostazione predefinita) per utilizzare Secrets Manager per la gestione sicura delle credenziali.

   > **Note**
   >
   > L'utilizzo di Secrets Manager elimina la necessità di archiviare credenziali in testo semplice e fornisce una gestione centralizzata delle credenziali. Per ulteriori informazioni, consulta Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.

7. Per Secret, scegli un segreto esistente da Secrets Manager che contenga le credenziali dell'account del servizio di accesso al dominio oppure scegli Crea nuovo segreto per crearne uno.
8. Completa i restanti campi di configurazione di Microsoft Active Directory in base alle esigenze del tuo ambiente.
9. Scegli Crea macchina virtuale di archiviazione.

La SVM verrà creata e aggiunta a Microsoft Active Directory utilizzando le credenziali archiviate in Secrets Manager. Ora puoi creare condivisioni e volumi SMB su questo SVM per l'accesso ai client Windows e macOS.

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, sostituiscila *`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 per 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 da montare. Puoi trovare il nome DNS NFS nella FSx console Amazon scegliendo Storage virtual machines, quindi scegliendo la SVM su cui esiste il volume che stai montando. Il nome DNS NFS si trova nel pannello Endpoints.
   - *`volume-junction-path`*— Il percorso di giunzione del volume che state montando. Puoi trovare il percorso di giunzione di un volume nella FSx console Amazon nel pannello Riepilogo della pagina dei dettagli del volume.
   - *`mount-point`*— Il nome della directory che hai creato sulla tua 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 seguente comando 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.

Pulizia 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, interrompi l'istanza. Per ulteriori informazioni, consulta Terminazione dell'istanza nella Guida per l'utente di Amazon EC2.
2. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
3. Sulla FSx console Amazon, elimina tutti i tuoi volumi FSx for ONTAP che non sono volumi root della tua SVM. Per ulteriori informazioni, consulta Eliminazione di volumi.
4. Elimina tutti i tuoi FSx for ONTAP. SVMs Per ulteriori informazioni, consulta Eliminazione di macchine virtuali di archiviazione (SVM).
5. Sulla FSx console Amazon, elimina il tuo 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. Mentre Amazon FSx elimina 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 IDs di controllo per i backup che desideri eliminare, quindi scegli Elimina backup.

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

Disponibilità entro Regione AWS

I file system Amazon FSx for NetApp ONTAP sono disponibili nei seguenti paesi Regioni AWS, con il supporto per il tipo di distribuzione indicato per ogni regione:

Regione AWS	Single-AZ 1	Multi-AZ 1	AZ singolo 2	Multi-AZ 2		
Stati Uniti orientali (Virginia settentrionale)	✓	✓	✓	✓		
Stati Uniti orientali (Ohio)	✓	✓	✓	✓		
Stati Uniti occidentali (California settentrionale)	✓	✓	✓	✓		
US West (Oregon)	✓	✓	✓	✓		
AWS GovCloud (Stati Uniti orientali)	✓	✓				
AWS GovCloud (Stati Uniti occidentali)	✓	✓				

Regione AWS	Single-AZ 1	Multi-AZ 1	AZ singolo 2	Multi-AZ 2		
Africa (Città del Capo)	✓	✓				
Asia Pacifico (Hong Kong)	✓	✓				
Asia Pacifico (Tokyo)	✓	✓	✓	✓		
Asia Pacifico (Seoul)	✓	✓	✓	✓		
Asia Pacifico (Osaka-Locale)	✓	✓				
Asia Pacifico (Mumbai)	✓	✓	✓	✓		
Asia Pacifico (Hyderabad)	✓	✓				
Asia Pacifico (Singapore)	✓	✓	✓	✓		

Regione AWS	Single-AZ 1	Multi-AZ 1	AZ singolo 2	Multi-AZ 2		
Asia Pacifico (Sydney)	✓	✓	✓	✓		
Asia Pacifico (Giacarta)	✓	✓				
Asia Pacifico (Melbourne)	✓	✓				
Asia Pacifico (Malesia)	✓	✓				
Asia Pacifico (Taipei)	✓	✓				
Asia Pacifico (Tailandia)	✓	✓				
Canada (Centrale)	✓	✓	✓	✓		
Canada occidentale (Calgary)	✓	✓				
Europa (Francoforte)	✓	✓	✓	✓		

Regione AWS	Single-AZ 1	Multi-AZ 1	AZ singolo 2	Multi-AZ 2		
Europa (Zurigo)	✓	✓	✓	✓		
Europa (Stoccolma)	✓	✓	✓	✓		
Europa (Milano)	✓	✓				
Europa (Spagna)	✓	✓	✓	✓		
Europa (Irlanda)	✓	✓	✓	✓		
Europe (London)	✓	✓				
Europa (Parigi)	✓	✓				
Israele (Tel Aviv)	✓	✓				
Messico (centrale)	✓	✓				
Medio Oriente (EAU)	✓	✓				
Medio Oriente (Bahrein)	✓	✓				

Regione AWS	Single-AZ 1	Multi-AZ 1	AZ singolo 2	Multi-AZ 2		
Sud America (San Paolo)	✓	✓				

Accesso ai dati di FSx for ONTAP

Puoi accedere ai tuoi FSx file system Amazon 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) per il supporto dello storage a blocchi condiviso.
- `Nvme`— Per la connessione utilizzando il Non-Volatile Memory Express (NVMe) over TCP/IP per il supporto dello storage a blocchi condiviso.
- `Management`— Per la gestione SVMs tramite l'interfaccia a riga di comando o l'API NetApp ONTAP o la console NetApp

> **Note**
>
> Il protocollo iSCSI è disponibile su tutti i file system con 6 o meno coppie di coppie ad alta disponibilità (HA). Il NVMe/TCP protocollo è disponibile sui file system di seconda generazione con 6 o meno coppie HA.

Argomenti

- Montaggio di volumi su client macOS
- Provisioning di iSCSI per Linux
- Provisioning di iSCSI per Windows
- Provisioning di NVMe /TCP per Linux
- Accesso ai dati tramite punti di accesso Amazon S3
- Accesso ai dati da altri servizi AWS

Client supportati

FSx i file system 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 scollega FSx automaticamente qualsiasi indirizzo IP elastico, che è un indirizzo IP pubblico raggiungibile da Internet, che viene collegato all'interfaccia di rete elastica di un file system.

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

- Istanze Amazon Elastic Compute Cloud (Amazon EC2) che eseguono Linux con supporto NFS o SMB, Microsoft Windows e macOS. Per ulteriori informazioni, consulta, e. Montaggio di volumi su client Linux Montaggio di volumi su client Microsoft Windows Montaggio di volumi su client macOS
- 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 for ONTAP.
- Amazon Elastic Kubernetes Service — Per ulteriori informazioni, consulta il driver CSI di Amazon for ONTAP nella FSx Guida NetApp 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 Usare Amazon WorkSpaces con FSx per 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 (VMs) in esecuzione nel VMware cloud su ambienti. AWS Per ulteriori informazioni, consulta Configurare Amazon FSx for NetApp ONTAP come storage esterno e VMware cloud on AWS with Amazon FSx for NetApp ONTAP Deployment Guide.

Una volta montati, FSx i file system di ONTAP appaiono 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.

Utilizzo dei protocolli di storage a blocchi

Amazon FSx for NetApp ONTAP supporta Internet Small Computer Systems Interface (iSCSI) e Non-Volatile Memory Express NVMe () su TCP NVMe/TCP) block storage protocols. In Storage Area Network (SAN) environments, storage systems are targets that have storage target devices. For iSCSI, the storage target devices are referred to as logical units (LUNs). For NVMe/TCP (, i dispositivi di storage di destinazione sono denominati namespace.

Si utilizza l'interfaccia logica iSCSI (LIF) di una SVM per connettersi sia NVMe allo storage a blocchi iSCSI che a quello iSCSI.

È possibile configurare lo storage creando LUNs per iSCSI e creando namespace per. NVMe LUNs e gli host accedono quindi ai namespace utilizzando i protocolli iSCSI o TCP.

Per ulteriori informazioni sulla configurazione di iSCSI NVMe/TCP e dello storage a blocchi, vedere:

- Provisioning di iSCSI per Linux
- Provisioning di iSCSI per Windows
- Provisioning di NVMe /TCP per Linux

Accesso ai dati dall'interno di Cloud AWS

Ogni FSx file system Amazon è associato a un Virtual Private Cloud (VPC). Puoi accedere al file system FSx for ONTAP da qualsiasi punto del VPC del file system, indipendentemente dalla zona di disponibilità. Puoi accedere al tuo file system anche da altri VPCs che possono trovarsi in AWS

account diversi o. Regioni AWS Oltre ai requisiti descritti nelle seguenti sezioni per l'accesso alle FSx risorse 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

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. Tutti SVMs i volumi associati al file system Amazon FSx for NetApp 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.

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 FSx console Amazon, 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 del file system FSx for ONTAP da AWS posizioni esterne al VPC di distribuzione 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 su Amazon per i file system Multi-AZ di FSx Amazon NetApp per ONTAP 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 ONTAP FSx.

Questi indirizzi IP mobili vengono creati nelle tabelle di routing VPC associate al file system e si trovano all'interno dei file system `EndpointIPv4AddressRange` `EndpointIPv6AddressRange` o specificati durante la creazione. L'intervallo di indirizzi IP dell'endpoint utilizza i seguenti intervalli di indirizzi, a seconda di come viene creato un file system:

- I file system dual-stack Multi-AZ creati con la console Amazon FSx o l' FSx API Amazon per impostazione predefinita utilizzano un intervallo di indirizzi IP /118 disponibile selezionato FSx da

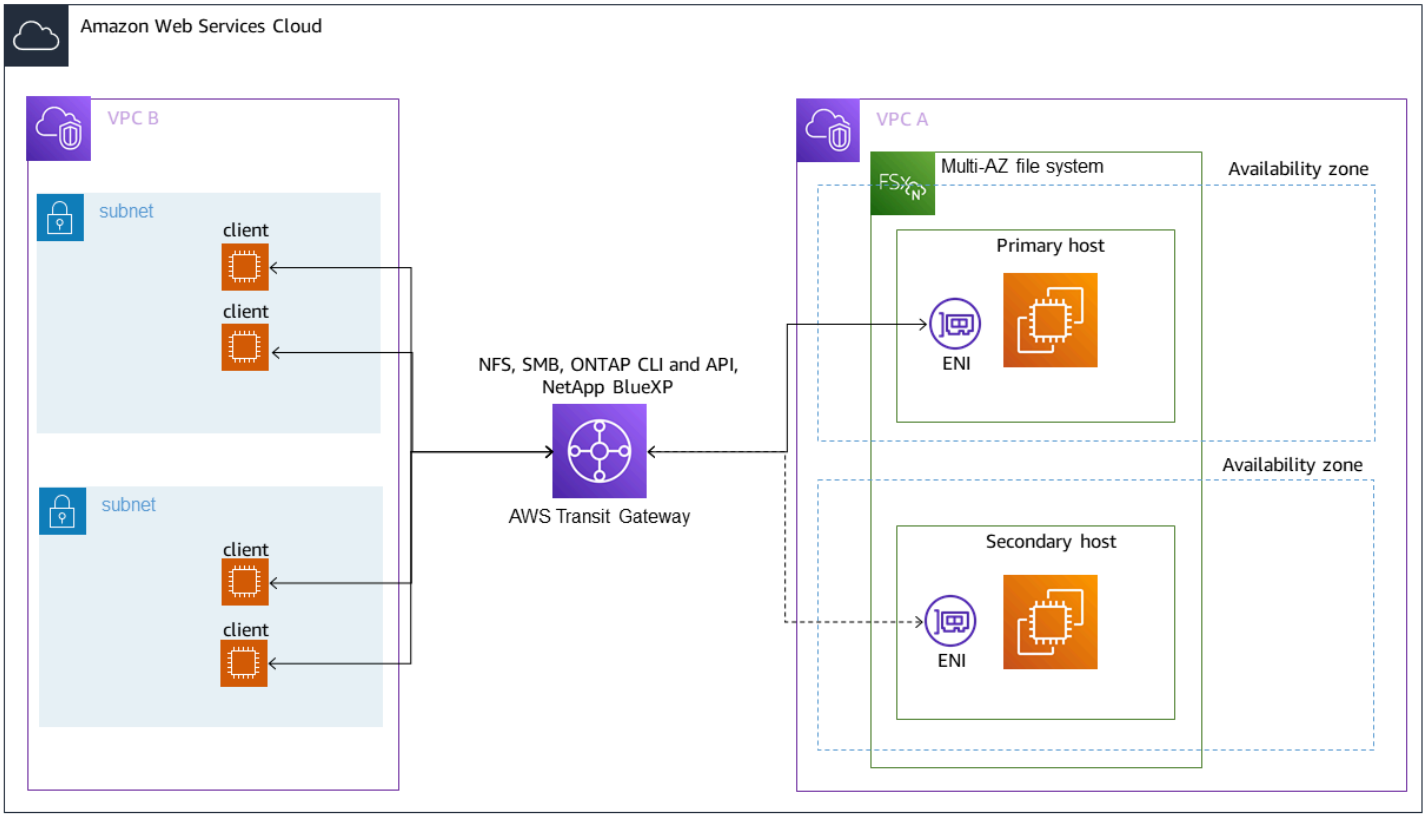
Amazon tra uno degli intervalli CIDR del VPC. Puoi avere indirizzi IP degli endpoint sovrapposti per i file system distribuiti nelle stesse VPC/route tabelle, purché non si sovrappongano a nessuna sottorete.

- Per impostazione predefinita, IPv4 i file system Multi-AZ creati utilizzando la FSx console Amazon utilizzano gli ultimi 64 indirizzi IP dell'intervallo CIDR primario del VPC per l'intervallo di indirizzi IP degli endpoint del file system.

  Per impostazione predefinita, i IPv4 file system Multi-AZ creati utilizzando l' FSx API o AWS CLI Amazon utilizzano un intervallo di indirizzi IP all'interno del blocco di `198.19.0.0/16` indirizzi per l'intervallo di indirizzi IP dell'endpoint.
- Per entrambi i tipi di rete, puoi anche specificare il tuo intervallo di indirizzi IP quando utilizzi l'opzione di creazione Standard. 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 e purché non sia già utilizzato da un altro file system con lo stesso VPC e le stesse tabelle di routing. Per questa opzione, ti consigliamo di utilizzare un intervallo che si trova all'interno dell'intervallo di indirizzi IP del VPC.

AWS Transit GatewaySupporta solo il routing verso indirizzi IP mobili, noto anche come peering transitivo. Peering VPC e Site-to-Site VPN non supportano 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 dei file system

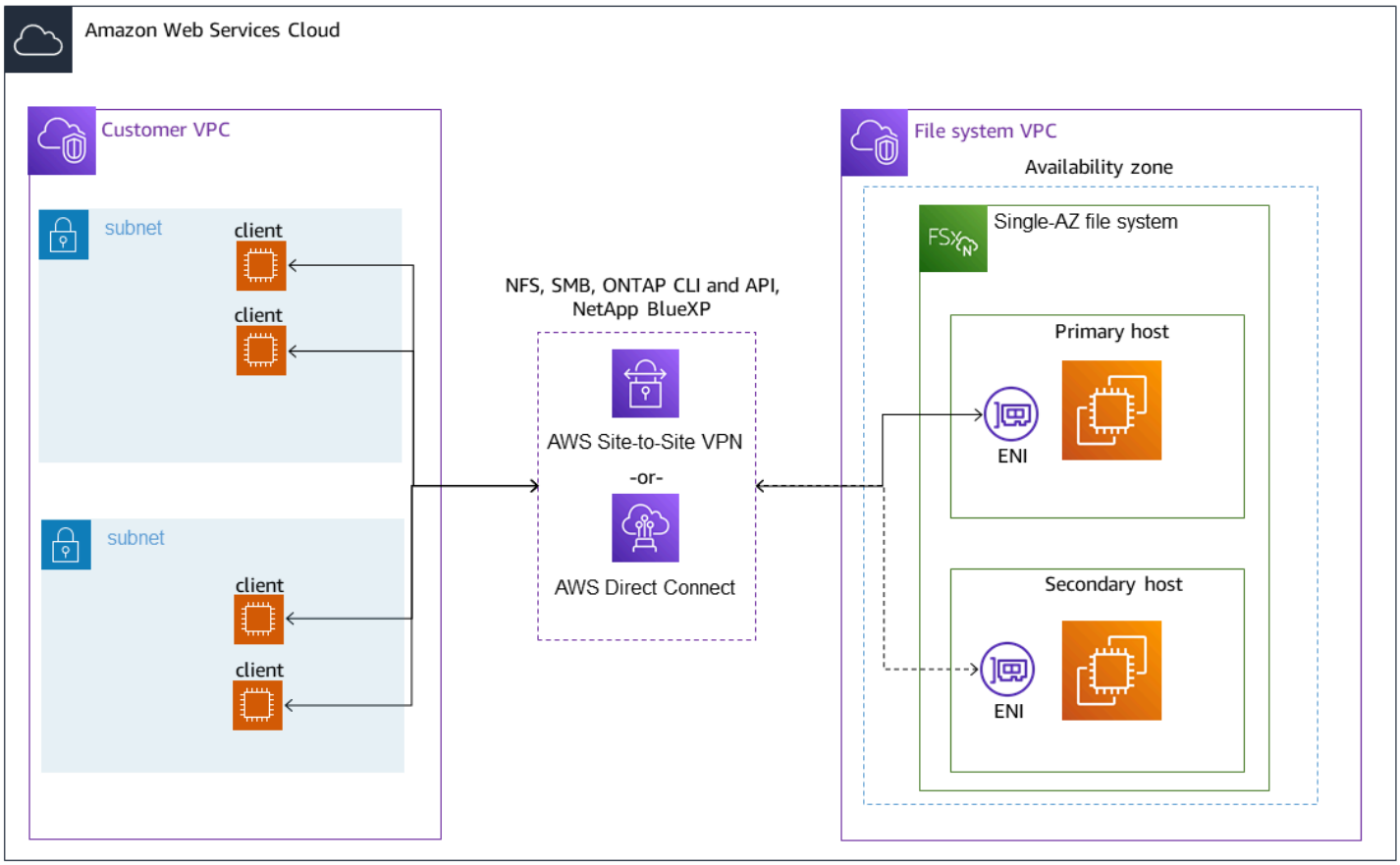
Per informazioni su quando è necessario utilizzare Transit Gateway per accedere al file system FSx for ONTAP, vedereQuando è richiesto il Transit Gateway?.

Amazon FSx gestisce le tabelle di routing VPC per i file system Multi-AZ utilizzando l'autenticazione basata su tag. Queste tabelle di routing sono contrassegnate con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Durante la creazione o l'aggiornamento FSx per l'utilizzo di file system ONTAP Multi-AZ, si CloudFormation consiglia di aggiungere il `Key: AmazonFSx; Value: ManagedByAmazonFSx` tag manualmente.

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

Gli endpoint utilizzati FSx per accedere ai file system 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 Site-to-Site VPN AWS Transit Gateway

Il diagramma seguente illustra l'utilizzo Site-to-Site VPN o 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 FSx tramite NFS, SMB o l'API REST NetApp ONTAP, CLI. oppure NetApp Console	Solo se: • Accesso da una rete peer-to-peer (ad esempio locale), e • Non si accede FSx tramite un'istanza NetApp FlexCache o Global File Cache
Accesso ai dati tramite iSCSI	No
Accesso ai dati tramite NVMe	No
Unire una SVM a un Active Directory	No
SnapMirror	No
FlexCache Memorizzazione nella cache	No
Cache globale dei file	No

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

È possibile utilizzare il peering VPC o accedere AWS Transit Gateway agli endpoint del file system, NVMe iSCSI e intercluster dall'esterno del VPC di implementazione del file system. È possibile utilizzare il peering VPC per instradare traffico, NVMe iSCSI e intercluster tra. VPCs Una connessione peering VPC è una connessione di rete tra due VPCs e viene utilizzata per instradare il traffico tra di loro utilizzando indirizzi o privati IPv4 . IPv6 Puoi utilizzare il peering VPC per connetterti VPCs 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 Site-to-Site VPNe Direct Connect; linee guida più specifiche sui casi d'uso sono disponibili nelle sezioni seguenti. Oltre a tutti i requisiti elencati di seguito per l'accesso a diverse risorse FSx for ONTAP da locali, 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 Gruppi di sicurezza Amazon VPC.

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

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

Accesso ai file system Multi-AZ dall'ambiente locale

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 le zone di disponibilità per i 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 indirizzi IP mobili, è necessario utilizzarli insieme o per accedere AWS Transit Gatewaya queste interfacce da una rete locale. AWS Direct Connect Site-to-Site VPN Gli indirizzi IP mobili utilizzati per queste interfacce rientrano nel `EndpointIPv4AddressRange` o `EndpointIPv6AddressRange` specificati durante la creazione del file system Multi-AZ. L'intervallo di indirizzi IP dell'endpoint utilizza i seguenti intervalli di indirizzi, a seconda di come viene creato un file system:

- I file system dual-stack Multi-AZ creati con la console Amazon FSx o l' FSx API Amazon per impostazione predefinita utilizzano un intervallo di indirizzi IP /118 disponibile selezionato FSx da Amazon tra uno degli intervalli CIDR del VPC. Puoi avere indirizzi IP degli endpoint sovrapposti per i file system distribuiti nelle stesse VPC/route tabelle, purché non si sovrappongano a nessuna sottorete.
- Per impostazione predefinita, IPv4 i file system Multi-AZ creati utilizzando la FSx console Amazon utilizzano gli ultimi 64 indirizzi IP dell'intervallo CIDR primario del VPC per l'intervallo di indirizzi IP degli endpoint del file system.

  Per impostazione predefinita, i IPv4 file system Multi-AZ creati utilizzando l' FSx API o AWS CLI Amazon utilizzano un intervallo di indirizzi IP all'interno del blocco di `198.19.0.0/16` indirizzi per l'intervallo di indirizzi IP dell'endpoint.
- Per entrambi i tipi di rete, puoi anche specificare il tuo intervallo di indirizzi IP quando utilizzi l'opzione di creazione Standard. 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 e purché non sia già utilizzato da un altro file system con lo stesso VPC e le stesse tabelle di routing. Per questa opzione, ti consigliamo di utilizzare un intervallo che si trova all'interno dell'intervallo di indirizzi IP del VPC.

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 ONTAP FSx.

> **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 ulteriori informazioni, consulta Configura il routing per accedere ai file system Multi-AZ dall'ambiente locale.

Accesso ai file system Single-AZ dall'ambiente locale

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

FSx gli endpoint intercluster di for ONTAP sono dedicati alla replica del traffico tra i file system ONTAP, incluse le distribuzioni locali e per NetApp ONTAP. NetApp FSx Il traffico di replica include SnapMirror e FlexClone le relazioni tra le macchine virtuali di storage (SVMs) 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 instradare il traffico intercluster tra locali e. Cloud AWS Tuttavia, i client locali devono comunque utilizzare Site-to-Site VPN o Direct Connect stabilire una connessione sicura al tuo VPC.

Per ulteriori informazioni, consulta Configura il routing per accedere ai file system Multi-AZ dall'ambiente locale.

Configura il routing per accedere ai file system Multi-AZ dall'esterno del tuo VPC

Se disponi di un file system Multi-AZ con un `EndpointIPv4AddressRange` o `EndpointIPv6AddressRange` che non rientra nell'intervallo di indirizzi IP 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 i file system Multi-AZ con un intervallo di indirizzi IP dell'endpoint compreso nell'intervallo di indirizzi IP del tuo VPC.

Per configurare il routing utilizzando AWS Transit Gateway

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli il FSx file system ONTAP per il quale stai configurando l'accesso da una rete peer.
3. In Rete e sicurezza copia 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-to-peer.

Per aggiungere la tabella delle rotte al file system, consulta. Aggiornamento dei 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.

Configura il routing per accedere ai file system Multi-AZ dall'ambiente locale

AWS Transit Gateway Per configurare l'accesso ai file system Multi-AZ dall'ambiente locale

Se disponi di un file system Multi-AZ con un `EndpointIPv4AddressRange` o `EndpointIPv6AddressRange` 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.

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

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli il FSx file system ONTAP per il quale stai configurando l'accesso da una rete peer.
3. In Rete e sicurezza, copia l'endpoint IPv4 o l'intervallo di indirizzi. IPv6
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-to-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. Se disponi di sottoreti di allegati Transit Gateway separate, devi anche associare le tabelle di routing per tali sottoreti ad FSx Amazon in modo che vengano aggiornate con gli indirizzi degli endpoint Amazon FSx .

Per aggiungere una tabella di routing al tuo file system, consulta. Aggiornamento dei file system

Montaggio di volumi su client Linux

È consigliabile che i volumi da montare con i client Linux abbiano un'impostazione di stile di sicurezza di`UNIX`. Per ulteriori informazioni, consulta Gestione dei FSx volumi ONTAP.

> **Note**
>
> Per impostazione predefinita, FSx per ONTAP i montaggi NFS sono montaggi. `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 dell'SVM anziché il relativo nome DNS. Consigliamo di utilizzare il nome DNS per montare i client su file system di seconda generazione 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 di seconda generazione, 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**
>
> FSx per i file system ONTAP non supportano il montaggio automatico utilizzando istanze `/etc/fstab` Mac di Amazon EC2.

> **Note**
>
> Prima di 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 file system.

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 di volumi 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 FSx macchine virtuali di archiviazione ONTAP Per ulteriori informazioni sull'utilizzo dei gruppi di lavoro, vedere. Configurazione di un server SMB in un gruppo di lavoro
- Il volume da allegare deve avere un'impostazione di stile di sicurezza di. NTFS Per ulteriori informazioni, consulta Stile di sicurezza del volume.

Per montare un volume 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 FSx macchine virtuali di archiviazione 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. Eseguire il seguente 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 di seconda generazione 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 di volumi 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 di seconda generazione 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 dell'SVM anziché il relativo nome DNS. Consigliamo di utilizzare il nome DNS per montare i client su file system di seconda generazione 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 dell'SVM anziché il relativo nome DNS. Consigliamo di utilizzare il nome DNS per montare i client su file system di seconda generazione 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
```

Provisioning di iSCSI per Linux

FSx for ONTAP supporta il protocollo iSCSI. È necessario eseguire il provisioning di iSCSI sia sul client Linux che sul file system per utilizzare il protocollo iSCSI per il trasporto dei dati tra i client e il file system. Il protocollo iSCSI è disponibile su tutti i file system con 6 o meno coppie ad alta disponibilità (HA).

Il processo di configurazione di iSCSI su FSx Amazon NetApp for ONTAP prevede tre passaggi principali, descritti nelle seguenti procedure:

1. Installa e configura il client iSCSI sull'host Linux.
2. Configurare iSCSI sulla SVM del file system.
   - Creare un gruppo di iniziatori iSCSI.
   - Mappare il gruppo di iniziatori sul LUN.
3. Montare un LUN iSCSI sul client Linux.

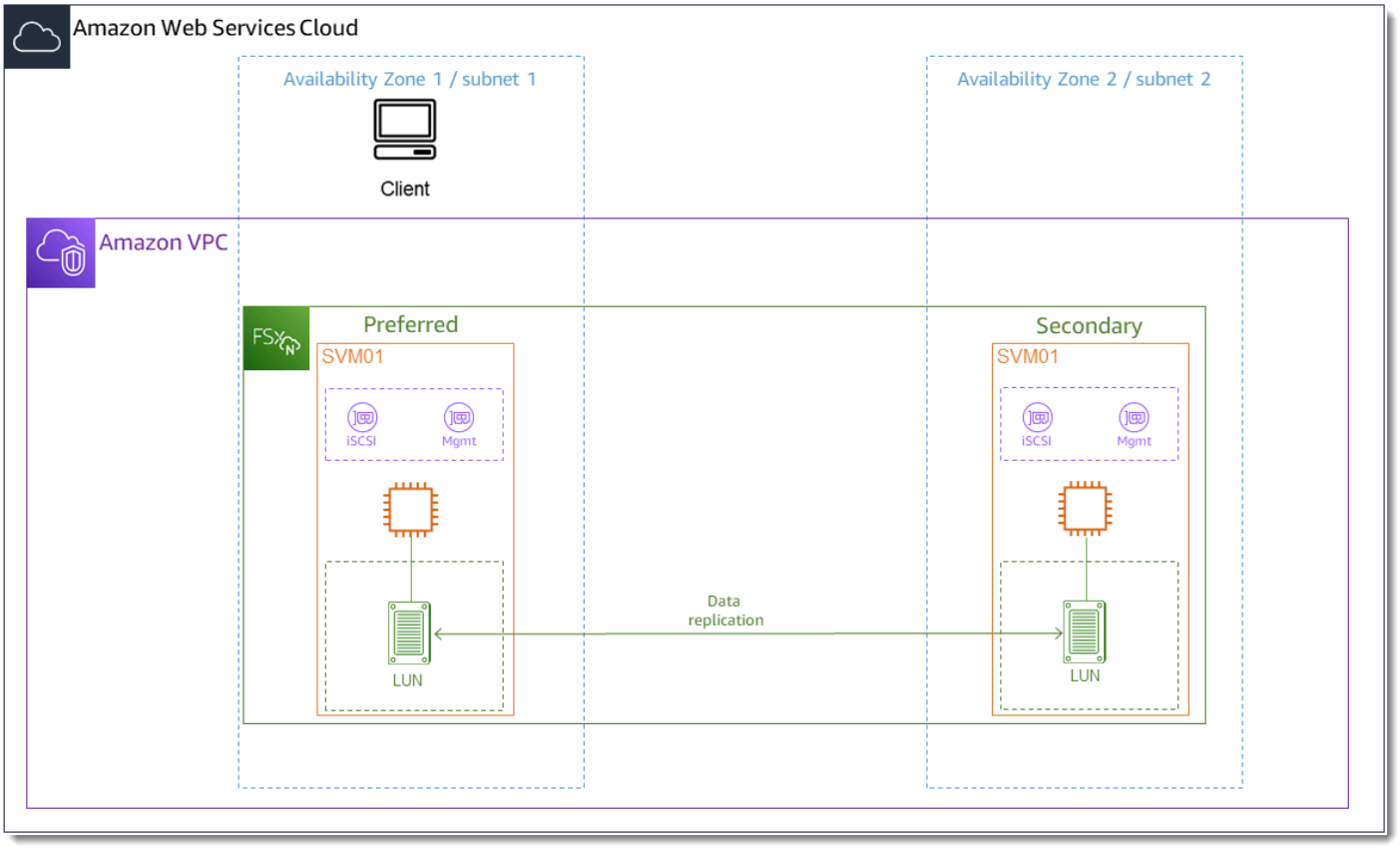
Prima di iniziare

Prima di iniziare il processo di configurazione del file system per iSCSI, è necessario completare i seguenti elementi.

- Creane uno FSx per il file system ONTAP. Per ulteriori informazioni, consulta Creazione di file system.

- Creare un LUN iSCSI sul file system. Per ulteriori informazioni, consulta Creazione di un LUN iSCSI.
- Crea un' EC2 istanza che esegue Amazon Linux 2 Amazon Machine Image (AMI) nello stesso VPC del file system. Questo è l'host Linux su cui configurare iSCSI e accedere ai dati dei file.

  Oltre all'ambito di queste procedure, se l'host si trova in un altro VPC, è possibile utilizzare il peering VPC o concedere altri VPCs accessi AWS Transit Gateway agli endpoint iSCSI del volume. Per ulteriori informazioni, consulta Accesso ai dati dall'esterno del VPC di implementazione.
- Configurare i gruppi di sicurezza VPC dell'host Linux per consentire il traffico in entrata e in uscita come descritto in. Controllo degli accessi ai file system con Amazon VPC
- Ottieni le credenziali per ONTAP utente con `fsxadmin` privilegi che utilizzerai per accedere a ONTAP CLI. Per ulteriori informazioni, consulta ONTAPruoli e utenti.
- L'host Linux che configurerai per iSCSI e utilizzerai per accedere al file system FSx for ONTAP si trova nello stesso VPC e. Account AWS
- È consigliabile che l' EC2 istanza si trovi nella stessa zona di disponibilità della sottorete preferita del file system, come illustrato nella figura seguente.



Se la tua EC2 istanza esegue un'AMI Linux diversa da Amazon Linux 2, alcune delle utilità utilizzate in queste procedure ed esempi potrebbero essere già installate e potresti utilizzare comandi diversi per installare i pacchetti richiesti. Oltre all'installazione dei pacchetti, i comandi usati in questa sezione sono validi per altri EC2 sistemi Linux AMIs.

Argomenti

Installare e configurare iSCSI sull'host 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 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 all'interfaccia della NetApp riga di comando ONTAP FSx sul file system 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 su LUNs iSCSI e controlla a quali iniziatori (client) hanno accesso. LUNs 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 disponibile il LUNs mappato a questo igroup per 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. Se non lo avete fatto, consultate step-by-step le istruzioni Creazione di un LUN iSCSI per farlo.

   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

Il processo di montaggio del LUN iSCSI sul client Linux prevede tre passaggi:

1. Individuazione dei nodi iSCSI di destinazione
2. Partizionamento del LUN iSCSI
3. Montaggio del LUN iSCSI sul client

Queste sono trattate nelle seguenti procedure.

Per individuare i nodi iSCSI di destinazione

1. Sul client Linux, utilizzare il comando seguente per individuare i nodi iSCSI di destinazione utilizzando l'`iscsi_1`indirizzo IP. *`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) Per ottenere un throughput superiore a quello del client EC2 singolo Amazon (massimo 5 Gbps (~625 MBps) sul tuo LUN iSCSI, segui le procedure descritte nella sezione Larghezza di banda di EC2 rete delle istanze Amazon nella Amazon Elastic Compute Cloud User Guide for Linux Instances per stabilire sessioni aggiuntive per una maggiore velocità di trasmissione.

   Il comando seguente stabilisce 8 sessioni per iniziatore per nodo ONTAP in ogni zona di disponibilità, consentendo al client di gestire fino a 40 Gbps (5.000 MBps) 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. Gli iSCSI LUNs vengono presentati 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 NetApp ONTAP.
   - `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. È possibile creare più partizioni utilizzando un valore inferiore all'ultimo settore (`20971519`in questo esempio).

> **Note**
>
> Il `Last sector` valore varia in base alla dimensione del LUN iSCSI (10 GB 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. *`partition_name`*Ha il formato *`<device_name><partition_number>`*. 1è stato utilizzato come numero di partizione utilizzato nel `fdisk` comando del 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. Crea una directory *`directory_path`* come punto di montaggio per il tuo file system.

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

2. Montate il file system usando il seguente comando.

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

3. (Facoltativo) Se desideri assegnare a un utente specifico la proprietà della directory di montaggio, sostituiscila *username* con il nome utente del proprietario.

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

4. (Facoltativo) Verificate 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.

Provisioning di iSCSI per Windows

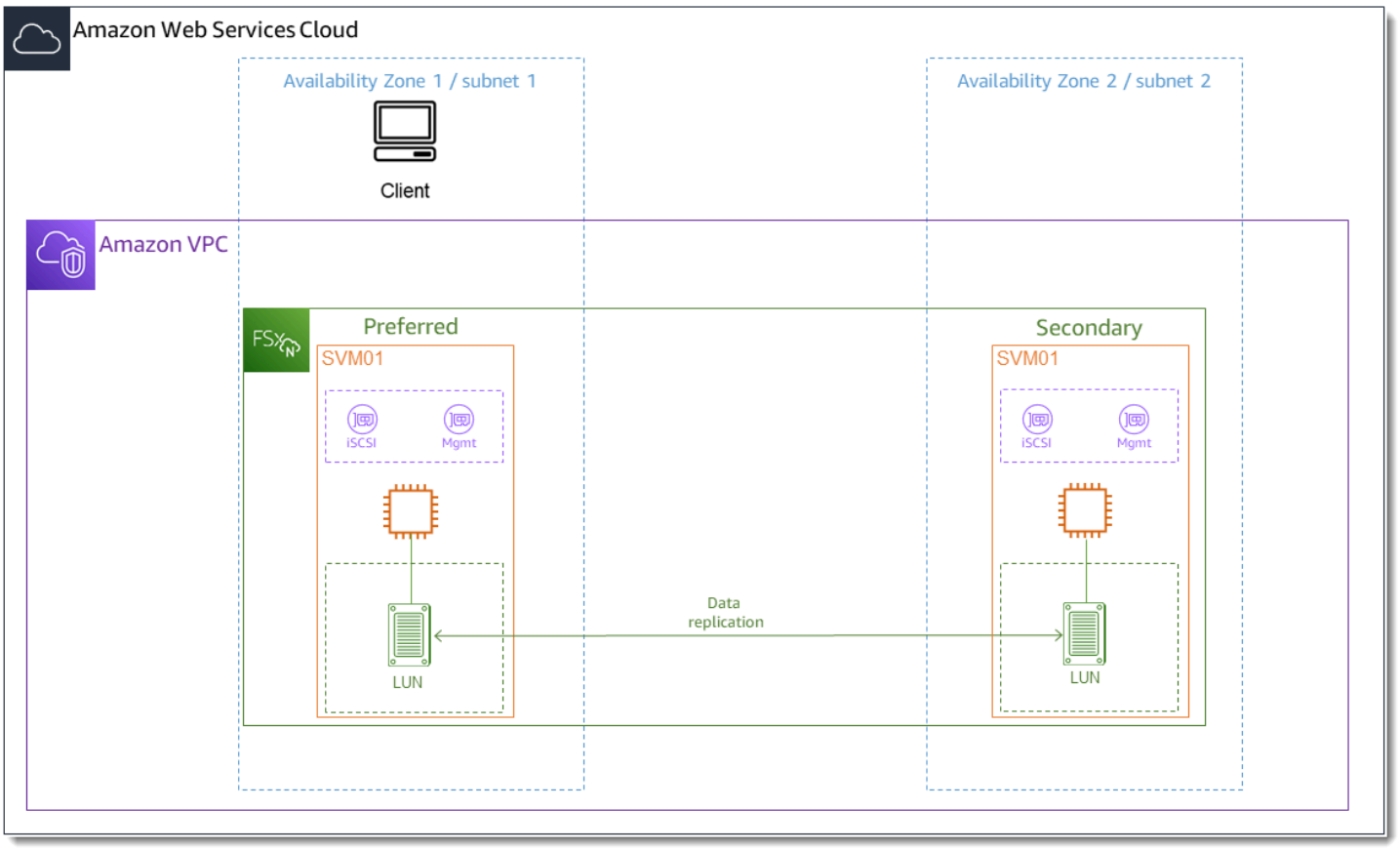
FSx for ONTAP supporta il protocollo iSCSI. È necessario eseguire il provisioning di iSCSI sia sul client Windows che sull'SVM e sul volume per utilizzare il protocollo iSCSI per il trasporto dei dati tra i client e il file system. Il protocollo iSCSI è disponibile su tutti i file system con 6 o meno coppie ad alta disponibilità (HA).

Gli esempi presentati in queste procedure mostrano come effettuare il provisioning del protocollo iSCSI sul client e FSx per il file system ONTAP e utilizzare 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 altri accessi AWS Transit Gateway agli endpoint VPCs iSCSI. Per ulteriori informazioni, consulta Accesso ai dati dall'esterno del VPC di implementazione.

  Si consiglia 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 for ONTAP utilizzando FSx 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. Per accedere alla ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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. Utilizzando la ONTAP CLI lun igroup create, crea il gruppo di iniziatori o. `igroup` Un gruppo di iniziatori esegue il mapping su LUNs iSCSI e controlla a quali iniziatori (client) hanno accesso. LUNs 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
```

Per rendere `igroup` disponibile la LUNs mappatura su questo a più host, è possibile specificare più nomi di iniziatori separati da virgole utilizzando il comando CLI. `lun igroup create`ONTAP

3. Conferma che `igroup` è stato creato correttamente utilizzando il comando ONTAPCLI lun igroup show:

```
::> 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
```

Con i `igroup` file creati, sei pronto per crearli LUNs e mapparli 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 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 Gbps (MBps5.000) di throughput aggregato verso il LUN iSCSI. Le 8 sessioni garantiscono che un singolo client sia in grado di gestire l'intera capacità di throughput di 4.000 unità per il massimo livello di capacità di MBps throughput ONTAP. FSx Facoltativamente, puoi modificare il numero di sessioni impostando un numero superiore o inferiore di sessioni (ogni sessione fornisce fino a MBps 625 di velocità effettiva) modificando la variabile. `RecommendedConnectionCount` 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.

```
Write-Host "Starting iSCSI connection setup..."
     $TargetPortalAddresses = @("iscsi_1","iscsi_2"); $LocaliSCSIAddress = "ec2_ip"
     $RecommendedConnectionCount = 8

     Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
```

```
        New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
    }

    New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

    $currentMPIOSettings = Get-MPIOSetting
    if ($currentMPIOSettings.PathVerificationState -ne 'Enabled') {
        Write-Host "Setting MPIO path verification state to Enabled"; Set-
MPIOSetting -NewPathVerificationState Enabled
    } else { Write-Host "MPIO path verification state already Enabled" }

    $portalConnectionCounts = @{}
    foreach ($TargetPortalAddress in $TargetPortalAddresses)
 { $portalConnectionCounts[$TargetPortalAddress] = 0 }

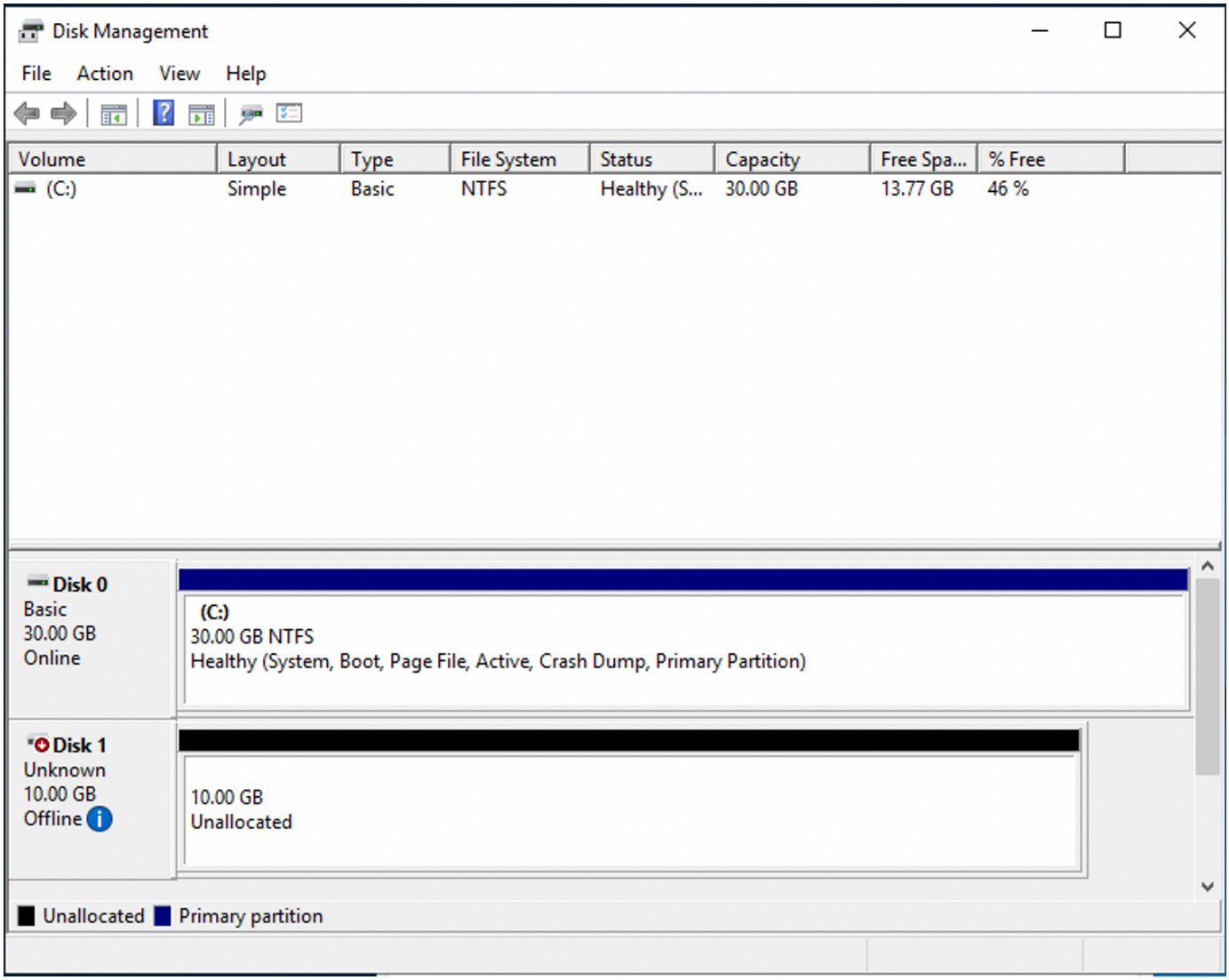
    $sessions = Get-IscsiSession
    if ($sessions) {
        foreach ($session in $sessions) {
            if ($session.IsConnected) {
                $targetPortal = (Get-IscsiTargetPortal -iSCSISession
 $session).TargetPortalAddress
                if ($portalConnectionCounts.ContainsKey($targetPortal))
 { $portalConnectionCounts[$targetPortal]++ }
            }
        }
    }

    foreach ($TargetPortalAddress in $TargetPortalAddresses) {
        $existingCount = $portalConnectionCounts[$TargetPortalAddress];
 $remainingConnections = $RecommendedConnectionCount - $existingCount
        Write-Host "Portal $TargetPortalAddress has $existingCount
 existing connections, $remainingConnections remaining (max recommended:
 $RecommendedConnectionCount)"
        if ($remainingConnections -gt 0) {
            Write-Host "Creating $remainingConnections connections for portal
 $TargetPortalAddress"
            1..$remainingConnections | ForEach-Object {
                Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true
            }
        } else { Write-Host "Maximum connections (8) reached for portal
 $TargetPortalAddress" }
```

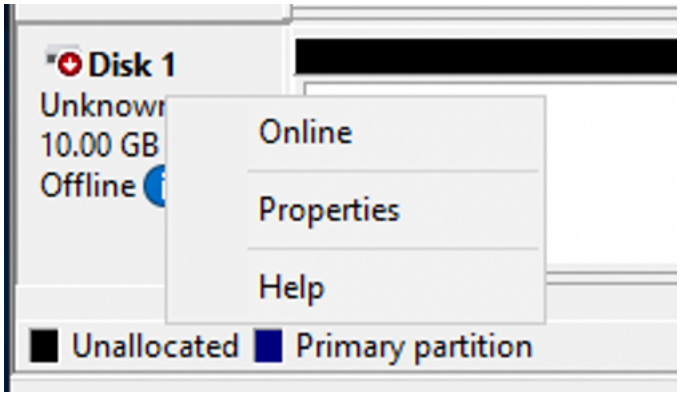
```
    }

    Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

3. Avvia l'applicazione Windows Disk Management. Aprire la finestra di dialogo Windows Esegui, quindi immettere `diskmgmt.msc` e premere 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 appare 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. Scarica 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.

MPIO Load Balance Policy is set to Round Robin (RR).
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
```

Provisioning di NVMe /TCP per Linux

FSx per ONTAP supporta Non-Volatile Memory Express over TCP (NVMe/TCP) block storage protocol. With NVMe/TCP, si utilizza il ONTAP CLI per fornire namespace e sottosistemi e quindi mappare i namespace ai sottosistemi, in modo analogo al modo in cui LUNs vengono forniti e mappati ai gruppi di iniziatori (igroup) per iSCSI. Il protocollo NVMe /TCP è disponibile sui file system di seconda generazione con 6 o meno coppie ad alta disponibilità (HA).

> **Note**
>
> FSx per i file system ONTAP utilizza gli endpoint iSCSI di un SVM per i protocolli di storage a blocchi NVMe iSCSI e /TCP.

Il processo di configurazione di NVMe /TCP su Amazon FSx for NetApp ONTAP prevede tre passaggi principali, descritti nelle seguenti procedure:

1. Installa e configura il NVMe client sull'host Linux.
2. Configura NVMe sulla SVM del file system.
   - Crea un NVMe namespace.
   - Crea un sottosistema NVMe .
   - Mappa lo spazio dei nomi sul sottosistema.
   - Aggiungere il client NQN al sottosistema.
3. Monta un NVMe dispositivo sul client Linux.

Prima di iniziare

Prima di iniziare il processo di configurazione del file system per NVMe /TCP, è necessario completare i seguenti elementi.

- Crea un file system FSx per ONTAP. Per ulteriori informazioni, consulta Creazione di file system.
- Crea un' EC2 istanza che esegue Red Hat Enterprise Linux (RHEL) 9.3 nello stesso VPC del file system. Questo è l'host Linux su cui configurerete NVMe e accederete ai dati dei file usando NVMe /TCP per Linux.

  Oltre all'ambito di queste procedure, se l'host si trova in un altro VPC, è possibile utilizzare il peering VPC o concedere altri VPCs accessi AWS Transit Gateway agli endpoint iSCSI del volume. Per ulteriori informazioni, consulta Accesso ai dati dall'esterno del VPC di implementazione.
- Configurare i gruppi di sicurezza VPC dell'host Linux per consentire il traffico in entrata e in uscita come descritto in. Controllo degli accessi ai file system con Amazon VPC
- Ottieni le credenziali per ONTAP utente con `fsxadmin` privilegi che utilizzerai per accedere a ONTAP CLI. Per ulteriori informazioni, consulta ONTAPruoli e utenti.

- L'host Linux per cui configurerai NVMe e utilizzerai per accedere al file system FSx for ONTAP si trova nello stesso Account AWS VPC e.
- È consigliabile che l' EC2 istanza si trovi nella stessa zona di disponibilità della sottorete preferita del file system.

Se l' EC2 istanza esegue un'AMI Linux diversa da RHEL 9.3, alcune delle utilità utilizzate in queste procedure ed esempi potrebbero essere già installate e potresti utilizzare comandi diversi per installare i pacchetti richiesti. Oltre all'installazione dei pacchetti, i comandi usati in questa sezione sono validi per altri sistemi Linux. EC2 AMIs

Argomenti

Installazione e configurazione NVMe sull'host Linux

Per installare il NVMe client

1. Connect alla propria istanza Linux utilizzando un client SSH. Per ulteriori informazioni, consulta Connect alla tua istanza Linux da Linux o macOS tramite SSH.
2. Installa `nvme-cli` utilizzando il seguente comando:

```
~$ sudo yum install -y nvme-cli
```

3. Carica il `nvme-tcp` modulo sull'host:

```
$ sudo modprobe nvme-tcp
```

4. Ottieni il nome NVMe qualificato (NQN) dell'host Linux utilizzando il seguente comando:

```
$ cat /etc/nvme/hostnqn
nqn.2014-08.org.nvmexpress:uuid:9ed5b327-b9fc-4cf5-97b3-1b5d986345d1
```

   Registra la risposta per utilizzarla in un passaggio successivo.

Configura NVMe sul file system FSx for ONTAP

Per configurare NVMe sul file system

Connect alla CLI NetApp ONTAP FSx sul file system for ONTAP su cui intendi creare il/i NVMe dispositivo/i.

1. Per accedere a ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 un nuovo volume sulla SVM che stai utilizzando per accedere all' NVMe interfaccia.

   ```
   ::> vol create -vserver fsx -volume nvme_vol1 -aggregate aggr1 -size 1t
        [Job 597] Job succeeded: Successful
   ```

3. Crea lo spazio dei NVMe nomi ns_1 utilizzando il comando vserver nvme namespace create NetApp ONTAP CLI. Un namespace esegue il mapping agli iniziatori (client) e controlla quali iniziatori (client) hanno accesso ai dispositivi. NVMe

   ```
   ::> vserver nvme namespace create -vserver fsx -path /vol/nvme_vol1/ns_1 -size 100g
    -ostype linux
   Created a namespace of size 100GB (107374182400).
   ```

4. Crea il NVMe sottosistema utilizzando il comando vserver nvme subsystem create NetApp ONTAP CLI.

   ```
   ~$ vserver nvme subsystem create -vserver fsx -subsystem sub_1 -ostype linux
   ```

5. Mappa lo spazio dei nomi sul sottosistema appena creato.

   ```
   ::> vserver nvme subsystem map add -vserver fsx -subsystem sub_1 -path /vol/
   nvme_vol1/ns_1
   ```

6. Aggiungi il client al sottosistema utilizzando il NQN recuperato in precedenza.

```
::> vserver nvme subsystem host add -subsystem sub_1 -host-nqn
 nqn.2014-08.org.nvmexpress:uuid:ec21b083-1860-d690-1f29-44528e4f4e0e -vserver fsx
```

Se desideri rendere i dispositivi mappati su questo sottosistema disponibili a più host, puoi specificare più nomi di iniziatori in un elenco separato da virgole. Per ulteriori informazioni, consulta vserver nvme subsystem host add nei documenti ONTAP. NetApp

7. Conferma che lo spazio dei nomi esista usando il comando: vserver nvme namespace show

```
::> vserver nvme namespace show -vserver fsx -instance
Vserver Name: fsx
            Namespace Path: /vol/nvme_vol1/ns_1
                      Size: 100GB
                 Size Used: 90.59GB
                   OS Type: linux
                   Comment:
                Block Size: 4KB
                     State: online
         Space Reservation: false
Space Reservations Honored: false
              Is Read Only: false
             Creation Time: 5/20/2024 17:03:08
            Namespace UUID: c51793c0-8840-4a77-903a-c869186e74e3
                 Vdisk ID: 80d42c6f00000000187cca9
      Restore Inaccessible: false
   Inconsistent Filesystem: false
       Inconsistent Blocks: false
                   NVFail: false
Node Hosting the Namespace: FsxId062e9bb6e05143fcb-01
               Volume Name: nvme_vol1
                Qtree Name:
          Mapped Subsystem: sub_1
            Subsystem UUID: db526ec7-16ca-11ef-a612-d320bd5b74a9
              Namespace ID: 00000001h
              ANA Group ID: 00000001h
              Vserver UUID: 656d410a-1460-11ef-a612-d320bd5b74a9
                Vserver ID: 3
              Volume MSID: 2161388655
              Volume DSID: 1029
                 Aggregate: aggr1
            Aggregate UUID: cfa8e6ee-145f-11ef-a612-d320bd5b74a9
 Namespace Container State: online
```

```
        Autodelete Enabled: false
          Application UUID: -
               Application: -
  Has Metadata Provisioned: true

1 entries were displayed.
```

8. Utilizzate il network interface show -vservercomando per recuperare gli indirizzi delle interfacce di archiviazione a blocchi per la SVM in cui avete creato i vostri dispositivi. NVMe

```
::> network interface show -vserver svm_name -data-protocol nvme-tcp
            Logical               Status     Network            Current
        Current Is
Vserver     Interface             Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------            ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.16.19/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.26.134/20
 FSxId0123456789abcdef8-02  e0e     true
2 entries were displayed.
```

> **Note**
>
> Il `iscsi_1` LIF viene utilizzato sia per NVMe iSCSI che per /TCP.

In questo esempio, l'indirizzo IP di iscsi_1 è 172.31.16.19 e iscsi_2 è 172.31.26.134.

NVMe Monta un dispositivo sul tuo client Linux

Il processo di montaggio del NVMe dispositivo sul client Linux prevede tre passaggi:

1. Alla scoperta dei NVMe nodi
2. Partizionamento del dispositivo NVMe
3. Montaggio del NVMe dispositivo sul client

Queste sono trattate nelle seguenti procedure.

Per scoprire i NVMe nodi di destinazione

1. Sul tuo client Linux, usa il seguente comando per scoprire i NVMe nodi di destinazione. Sostituisci `iscsi_1` l'indirizzo IP di *`iscsi_1_IP`* with e *`client_IP`* l'indirizzo IP del client.

   > **Note**
   >
   > `iscsi_1`e `iscsi_2` LIFs vengono utilizzati sia per iSCSI che per lo storage. NVMe

   ```
   ~$ sudo nvme discover -t tcp -w client_IP -a iscsi_1_IP
   ```

   ```
   Discovery Log Number of Records 4, Generation counter 11
   =====Discovery Log Entry 0======
   trtype:  tcp
   adrfam:  ipv4
   subtype: current discovery subsystem
   treq:    not specified
   portid:  0
   trsvcid: 8009
   subnqn:  nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
   traddr:  172.31.26.134
   eflags:  explicit discovery connections, duplicate discovery information
   sectype: none
   =====Discovery Log Entry 1======
   trtype:  tcp
   adrfam:  ipv4
   subtype: current discovery subsystem
   treq:    not specified
   portid:  1
   trsvcid: 8009
   subnqn:  nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
   traddr:  172.31.16.19
   eflags:  explicit discovery connections, duplicate discovery information
   sectype: none
   ```

2. (Facoltativo) Per ottenere un throughput superiore a quello del client EC2 singolo Amazon (massimo 5 Gbps (~625 MBps) sul tuo NVMe dispositivo di file, segui le procedure descritte nella

sezione Larghezza di banda di rete delle EC2 istanze Amazon nella Amazon Elastic Compute Cloud User Guide for Linux Instances per stabilire sessioni aggiuntive.

3. Accedi agli iniziatori di destinazione con un timeout di perdita del controller di almeno 1800 secondi, utilizzando nuovamente l'indirizzo IP di e l'indirizzo IP `iscsi_1` del client per. *`iscsi_1_IP client_IP`* I NVMe dispositivi vengono presentati come dischi disponibili.

```
~$ sudo nvme connect-all -t tcp -w client_IP -a iscsi_1 -l 1800
```

4. Utilizzate il comando seguente per verificare che lo NVMe stack abbia identificato e unito le sessioni multiple e configurato il multipathing. Il comando restituisce `Y` se la configurazione ha avuto successo.

```
~$ cat /sys/module/nvme_core/parameters/multipath
Y
```

5. Utilizzate i seguenti comandi per verificare che l'impostazione NVMe -oF `model` sia impostata su `NetApp ONTAP Controller` e che il bilanciamento del carico `iopolicy` sia impostato su `round-robin` per il rispettivo ONTAP namespace per distribuire l'I/O su tutti i percorsi disponibili

```
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/model
Amazon Elastic Block Store
NetApp ONTAP Controller
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/iopolicy
numa
round-robin
```

6. Utilizzate il comando seguente per verificare che i namespace vengano creati e rilevati correttamente sull'host:

```
~$ sudo nvme list
Node                  Generic               SN                   Model
                        Namespace  Usage                      Format           FW
 Rev
--------------------- --------------------- --------------------
 ---------------------------------------- ---------- --------------------------
 ---------------- --------
/dev/nvme0n1          /dev/ng0n1            vol05955547c003f0580 Amazon Elastic
 Block Store               0x1         25.77  GB /  25.77  GB    512   B +  0 B
 1.0
```

```
/dev/nvme2n1          /dev/ng2n1            lWB12JWY/XLKAAAAAAAC NetApp ONTAP
 Controller                  0x1        107.37  GB / 107.37  GB      4 KiB +  0 B
 FFFFFFFF
```

Il nuovo dispositivo nell'output è. `/dev/nvme2n1` Questo schema di denominazione può variare a seconda dell'installazione Linux in uso.

7. Verifica che lo stato del controller di ogni percorso sia attivo e abbia lo stato di multipathing ANA (Asymmetric Namespace Access) corretto:

```
~$ nvme list-subsys /dev/nvme2n1
nvme-subsys2 -
 NQN=nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:subsystem.rhel
               hostnqn=nqn.2014-08.org.nvmexpress:uuid:ec2a70bf-3ab2-6cb0-
f997-8730057ceb24
               iopolicy=round-robin
\
 +- nvme2 tcp
 traddr=172.31.26.134,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
 live non-optimized
 +- nvme3 tcp
 traddr=172.31.16.19,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
 live optimized
```

In questo esempio, lo NVMe stack ha rilevato automaticamente il file LIF alternativo del file system, 172.31.26.134. `iscsi_2`

8. Verificate che NetApp il plug-in visualizza i valori corretti per ciascuno ONTAP dispositivo namespace:

```
~$ sudo nvme netapp ontapdevices -o column
Device           Vserver                   Namespace Path
           NSID UUID                                   Size
---------------- ------------------------
 ------------------------------------------------- ----
 ------------------------------------ ---------
/dev/nvme2n1     fsx                       /vol/nvme_vol1/ns_1
           1    0441c609-3db1-4b0b-aa83-790d0d448ece   107.37GB
```

Per partizionare il dispositivo

1. Usa il comando seguente per verificare che sia presente il percorso del tuo device_name`nvme2n1`.

```
~$ ls /dev/mapper/nvme2n1
/dev/nvme2n1
```

2. Partiziona il disco usando. `fdisk` Inserirai un prompt interattivo. Inserisci le opzioni nell'ordine mostrato. È possibile creare più partizioni utilizzando un valore inferiore all'ultimo settore (`20971519`in questo esempio).

> **Note**
>
> Il `Last sector` valore varierà a seconda delle dimensioni del NVMe dispositivo (100 GiB in questo esempio).

```
~$ sudo fdisk /dev/mapper/nvme2n1
```

Viene avviato il prompt `fsdisk` interattivo.

```
Welcome to fdisk (util-linux 2.37.4).
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 (256-26214399, default 256):
Last sector, +sectors or +size{K,M,G,T,P} (256-26214399, default
 26214399): 20971519

Created a new partition 1 of type 'Linux' and of size 100 GiB.
```

```
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/nvme2n1` diventa disponibile. *`partition_name`*Ha il formato *`<device_name><partition_number>`*. 1è stato utilizzato come numero di partizione nel `fdisk` comando del passaggio precedente.

3. Crea il tuo file system utilizzando `/dev/nvme2n1` come percorso.

```
~$ sudo mkfs.ext4 /dev/nvme2n1
```

Il sistema risponde con il seguente output:

```
mke2fs 1.46.5 (30-Dec-2021)
Found a dos partition table in /dev/nvme2n1
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 372fb2fd-ae0e-4e74-ac06-3eb3eabd55fb
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

Per montare il NVMe dispositivo sul client Linux

1. Crea una directory *`directory_path`* come punto di montaggio per il tuo file system sull'istanza Linux.

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

2. Monta il file system usando il seguente comando.

```
~$ sudo mount -t ext4 /dev/nvme2n1 /directory_path/mount_point
```

3. (Facoltativo) Se desideri assegnare a un utente specifico la proprietà della directory di montaggio, sostituiscila *username* con il nome utente del proprietario.

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

4. (Facoltativo) Verificate 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!
```

Hai creato e montato correttamente un NVMe dispositivo sul tuo client Linux.

Accesso ai dati tramite punti di accesso Amazon S3

Puoi anche utilizzare i punti di accesso S3 per accedere ai dati dei file archiviati sui FSx file system Amazon come se fossero in S3, consentendoti di utilizzarli con applicazioni e servizi che funzionano con S3 senza modifiche alle applicazioni o spostando i dati dallo storage dei file. I punti di accesso Amazon S3 sono endpoint S3 che si collegano ai bucket S3 o FSx ai volumi ONTAP e OpenZFS. FSx I punti di accesso Amazon S3 semplificano la gestione dell'accesso ai dati per qualsiasi applicazione o AWS servizio compatibile con S3. Con i punti di accesso S3, i clienti con set di dati condivisi, tra cui data lake, archivi multimediali e contenuti generati dagli utenti, possono facilmente controllare e scalare l'accesso ai dati per centinaia di applicazioni, team o individui creando punti di accesso personalizzati con nomi e autorizzazioni personalizzati per ciascuno.

I punti di accesso S3 collegati ai volumi Amazon FSx for NetApp ONTAP supportano l'accesso in lettura e scrittura ai dati dei file utilizzando operazioni sugli oggetti S3 (ad esempio `GetObject`Put`Object`, e`ListObjectsV2`) su un endpoint Amazon S3.

Ogni punto di accesso S3 collegato a un file system FSx for ONTAP ha una policy sul punto di accesso AWS Identity and Access Management (IAM) e un utente del file system UNIX o Windows associato che viene utilizzato per autorizzare tutte le richieste effettuate tramite il punto di accesso. Per ogni richiesta, S3 valuta innanzitutto tutte le policy pertinenti, incluse quelle relative all'utente, all'access point, all'endpoint VPC S3 e alle policy di controllo del servizio, per autorizzare la richiesta. Una volta autorizzata da S3, la richiesta viene autorizzata dal file system, che valuta se l'utente del file system associato al punto di accesso S3 è autorizzato ad accedere ai dati sul file system. Puoi configurare un punto di accesso per accettare richieste solo da un cloud privato virtuale (VPC) per limitare l'accesso ai dati di Amazon S3 a una rete privata. Amazon S3 applica Block public access

per impostazione predefinita per tutti i punti di accesso collegati a un volume FSx for ONTAP e non è possibile modificare o disabilitare questa impostazione.

Utilizza la FSx console Amazon, la CLI e l'API per creare un punto di accesso S3 e collegarlo a un volume FSx for ONTAP. Il punto di accesso ti consente di accedere ai dati dei tuoi file utilizzando l'API S3, anche se i dati continuano a risiedere nel tuo file system FSx for ONTAP e puoi continuare a utilizzare i protocolli NFS e SMB per accedere ai tuoi dati insieme all'API S3.

I punti di accesso Amazon S3 FSx per i sistemi file ONTAP offrono una latenza nell'intervallo di decine di millisecondi, coerente con l'accesso ai bucket S3. Il throughput e le richieste al secondo che puoi inviare a un FSx file system Amazon tramite l'API S3 dipendono dal throughput assegnato al file system. Per ulteriori informazioni sulle funzionalità prestazionali del file system, consulta Amazon FSx per le prestazioni di NetApp ONTAP

Argomenti

Regioni AWS con punti di accesso Amazon S3 per FSx ONTAP

I punti di accesso Amazon S3 FSx per ONTAP sono supportati nei seguenti paesi Regioni AWS: Africa (Città del Capo), Asia Pacifico (Hong Kong, Hyderabad, Giacarta, Melbourne, Mumbai, Osaka, Seoul, Singapore, Sydney, Tokyo), Canada (Centrale), Canada occidentale (Calgary), Europa (Francoforte, Irlanda, Londra, Milano, Parigi, Spagna, Stoccolma, Zurigo), Israele (Tel Aviv), Medio Oriente (Bahrein, Emirati Arabi Uniti), Sud America (San Paolo), Stati Uniti orientali (Virginia settentrionale, Ohio) e Stati Uniti occidentali (California settentrionale, Oregon).

Regole di denominazione, restrizioni e limitazioni dei punti di accesso

Quando crei un punto di accesso S3, scegli un nome per esso. I seguenti argomenti forniscono informazioni sulle regole di denominazione dei punti di accesso S3, nonché sulle restrizioni e limitazioni.

Argomenti

Regole di denominazione dei punti di accesso

Quando crei un access point S3 ne scegli il nome. Non è necessario che i nomi dei punti di accesso siano univoci tra Account AWS o Regioni AWS. Lo stesso Account AWS può creare punti di accesso con lo stesso nome in modi diversi Regioni AWS o due punti di accesso diversi Account AWS possono utilizzare lo stesso nome di punto di accesso. Tuttavia, all'interno di Regione AWS una singola persona non Account AWS possono esserci due punti di accesso con lo stesso nome.

I nomi dei punti di accesso S3 non possono terminare con il suffisso`-ext-s3alias`, che è riservato agli alias dei punti di accesso. Per un elenco completo delle regole di denominazione dei punti di accesso, consulta Regole di denominazione per i punti di accesso Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.

Restrizioni e limitazioni degli access point.

I punti di accesso S3 collegati FSx ai volumi ONTAP hanno le seguenti restrizioni, che non si applicano ai punti di accesso collegati ai bucket S3:

- Puoi creare un punto di accesso S3 solo nello stesso Regione AWS volume FSx for ONTAP a cui lo stai collegando.
- Lo stesso Account AWS deve possedere il file system FSx for ONTAP e il punto di accesso S3. Puoi creare solo punti di accesso S3 collegati ai volumi ONTAP FSx di tua proprietà. Non puoi creare un punto di accesso S3 collegato a un volume di proprietà di un altro. Account AWS
- Puoi creare e collegare punti di accesso S3 solo ai file system ONTAP che FSx eseguono NetApp ONTAP versione 9.17.1 e successive.

Per un elenco completo di tutte le restrizioni e limitazioni dei punti di accesso, consulta Restrizioni e limitazioni per i punti di accesso nella Guida per l'utente di Amazon Simple Storage Service.

Riferimento ai punti di accesso con ARNs alias dei punti di accesso o virtual-hosted-style URIs

Dopo aver creato un punto di accesso collegato a un volume FSx for ONTAP, puoi accedere ai dati tramite l'API AWS CLI e S3, oltre a servizi e applicazioni compatibili con S3 AWS e di terze parti. Quando fai riferimento a un punto di accesso in un'applicazione Servizio AWS o, puoi utilizzare l'Amazon Resource Name (ARN), l'alias del punto di accesso o l'URI in stile hosting virtuale.

Argomenti

- Punto di accesso ARNs
- Alias del punto di accesso
- URI virtual-hosted-style

Punto di accesso ARNs

I punti di accesso hanno Amazon Resource Names (ARNs). Gli access point ARNs sono simili al bucket S3 ARNs, ma vengono digitati e codificati in modo esplicito il punto di accesso Regione AWS e l' Account AWS ID del proprietario del punto di accesso. Per ulteriori informazioni ARNs, consulta Identify AWS resources with Amazon Resource Names (ARNs) nella Guida per l'AWS Identity and Access Management utente.

I punti di accesso ARNs hanno il seguente formato:

```
arn:aws::s3:region:account-id:accesspoint/resource
```

`arn:aws:s3:us-west-2:777777777777:accesspoint/test`rappresenta il punto di accesso denominato*test*, di proprietà dell'account 7777 nella regione*us-west-2*.

ARNs per oggetti e file a cui si accede tramite un punto di accesso, utilizzare il seguente formato:

```
arn:aws::s3:region:account-id:accesspoint/access-point-name/object/resource
```

`arn:aws:s3:us-west-2:111122223333:accesspoint/test/object/lions.jpg`rappresenta il file*lions.jpg*, accessibile tramite il punto di accesso denominato*test*, di proprietà dell'account 111122223333 nella regione. *us-west-2*

Per ulteriori informazioni sul punto di accesso ARNs, consulta Access point ARNs nella Guida per l'utente di Amazon Simple Storage Service.

Alias del punto di accesso

Quando crei un punto di accesso, Amazon S3 genera automaticamente un alias del punto di accesso che puoi utilizzare ovunque sia possibile utilizzare i nomi dei bucket S3 per accedere ai dati.

Un alias del punto di accesso non può essere modificato. Per un punto di accesso collegato a un volume FSx for ONTAP, l'alias del punto di accesso è composto dalle seguenti parti:

```
access point prefix-metadata-ext-s3alias
```

Di seguito vengono illustrati l'ARN e l'alias del punto di accesso per un punto di accesso S3 collegato a un volume FSx for ONTAP, restituito come parte della risposta a un comando CLI. `describe-s3-access-point-attachments` FSx Il punto di accesso in questo esempio è denominato. `my-ontap-ap`

```
...
        "S3AccessPoint": {
            "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-ontap-ap",
            "Alias": "my-ontap-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias",
...
```

> **Note**
>
> Il `-ext-s3alias` suffisso è riservato agli alias dei punti di accesso S3 collegati a un volume FSx for ONTAP e non può essere utilizzato per i nomi dei punti di accesso.

Puoi utilizzare l'alias del punto di accesso anziché un ARN del punto di accesso Amazon S3 in alcune operazioni del piano dati S3. Per un elenco delle operazioni supportate, consulta. Compatibilità dei punti di accesso

Per un set completo di limitazioni degli alias dei punti di accesso, consulta Limitazioni degli alias dei punti di accesso nella Guida per l'utente di Amazon Simple Storage Service.

URI virtual-hosted-style

Gli access point supportano virtual-host-style solo l'indirizzamento. In un URI in stile host virtuale, il nome del punto di accesso Regione AWS fa parte del nome di dominio contenuto nell'URL. Account AWSPer visualizzare l'URI S3 per un punto di accesso collegato a un volume FSx for ONTAP, nella pagina dei dettagli del punto di accesso sotto Dettagli del punto di accesso S3, scegli il nome del punto di accesso elencato per il punto di accesso S3. Verrai indirizzato alla pagina dei dettagli del punto di accesso nella console Amazon S3. Puoi trovare l'URI S3 in Proprietà.

Per ulteriori informazioni, consulta l'URI in stile hosting virtuale nella Guida per l'utente di Amazon Simple Storage Service.

Compatibilità dei punti di accesso

Puoi utilizzare i punti di accesso per accedere ai dati archiviati su un volume FSx for ONTAP utilizzando il seguente Amazon APIs S3 per l'accesso ai dati. Tutte le operazioni elencate di seguito possono accettare sia alias di punti di accesso che di punti ARNs di accesso.

La tabella seguente è un elenco parziale delle operazioni Amazon S3 e indica se sono compatibili con i punti di accesso. La tabella mostra quali operazioni sono supportate dai punti di accesso che utilizzano un volume FSx for ONTAP come origine dati.

Operazioni S3	Punto di accesso collegato a un volume FSx for ONTAP
`AbortMultipartUpload`	Supportata
`CompleteMultipartUpload`	Supportata
`CopyObject` (solo copie della stessa Regione)	Supportato, se l'origine e la destinazione si trovano all'interno dello stesso punto di accesso
`CreateMultipartUpload`	Supportata
`DeleteObject`	Supportato
`DeleteObjects`	Supportato
`DeleteObjectTagging`	Supportata

Operazioni S3	Punto di accesso collegato a un volume FSx for ONTAP
GetBucketAcl	Non supportata
GetBucketCors	Non supportato
GetBucketLocation	Supportata
GetBucketNotificationConfiguration	Non supportata
GetBucketPolicy	Non supportato
GetObject	Supportata
GetObjectAcl	Non supportata
GetObjectAttributes	Supportata
GetObjectLegalHold	Non supportata
GetObjectRetention	Non supportato
GetObjectTagging	Supportato
HeadBucket	Supportato
HeadObject	Supportato
ListMultipartUploads	Supportato
ListObjects	Supportato
ListObjectsV2	Supportata
ListObjectVersions	Non supportata
ListParts	Supportata
Presign	Non supportata

Operazioni S3	Punto di accesso collegato a un volume FSx for ONTAP
PutObject	Supportata
PutObjectAcl	Non supportata
PutObjectLegalHold	Non supportata
PutObjectRetention	Non supportato
PutObjectTagging	Supportata
RestoreObject	Non supportata
UploadPart	Supportata
UploadPartCopy (solo copie della stessa Regione)	Supportato, se l'origine e la destinazione si trovano all'interno dello stesso punto di accesso

Le limitazioni all'utilizzo delle operazioni di Amazon S3 sono le seguenti:

- La dimensione massima degli oggetti è di 5 GB per i caricamenti, ma puoi scaricare oggetti più grandi
- `FSX_ONTAP`è l'unica classe di archiviazione supportata
- SSE-FSX è l'unica modalità di crittografia lato server supportata
- Le seguenti funzionalità di Amazon S3 non sono supportate: liste di controllo degli accessi (ACLs) diverse da Requester Pays`bucket-owner-full-control`, Object Versioning, Object Lock, Object Lifecycle, Hosting di siti Web statici (ad es. reindirizzamento di siti Web), autenticazione a più fattori (MFA) e scritture condizionali

Per esempi di utilizzo dei punti di accesso per eseguire operazioni di accesso ai dati sui file, consulta. Utilizzo dei punti di accesso

Oggetto ETag

Il tag dell'entità è un hash dell'oggetto. ETag Riflette le modifiche solo al contenuto di un oggetto, non ai relativi metadati. Non ETag è un MD5 riassunto dei dati dell'oggetto.

Checksum dell'oggetto

Puoi utilizzare i valori di checksum per verificare l'integrità dei dati che carichi. Quando carichi dati e specifichi un algoritmo di checksum, l' AWS SDK utilizza l'algoritmo di checksum scelto per calcolare un valore di checksum prima della trasmissione dei dati. Amazon S3 calcola quindi in modo indipendente un checksum dei dati e lo convalida rispetto al valore di checksum fornito. Gli oggetti vengono accettati solo dopo aver confermato che l'integrità dei dati è stata mantenuta durante il transito verso Amazon S3. A differenza dei checksum per gli oggetti nei bucket Amazon S3 General Purpose, il valore del checksum non viene memorizzato nel volume NetApp for ONTAP come metadati FSx dell'oggetto e come oggetto stesso. Ciò significa che i valori del checksum non vengono restituiti nella risposta e non vengono utilizzati per verificare l'integrità dell'oggetto durante il download.

Crittografia lato server con Amazon FSx (SSE-FSX)

Tutti i FSx file system di Amazon hanno la crittografia configurata per impostazione predefinita e sono crittografati a riposo con chiavi gestite tramite AWS Key Management Service. I dati vengono crittografati e decrittografati automaticamente sul file system man mano che i dati vengono scritti e letti dal file system. Questi processi vengono gestiti in modo trasparente da Amazon. FSx

Caricamento in più parti

Il caricamento in più parti consente di caricare un singolo oggetto come un insieme di parti. Ciascuna parte è una parte contigua dei dati dell'oggetto. È possibile caricare queste parti di oggetto in modo indipendente e in qualsiasi ordine. Il caricamento multiparte tiene conto delle seguenti considerazioni quando si utilizzano punti di accesso S3 con for ONTAP: FSx

- Le parti associate ai caricamenti multiparte in corso (ovvero caricamenti incompleti) non sono incluse nei backup di volume ONTAP. FSx
- Lo spazio di archiviazione utilizzato associato al caricamento multiparte in corso (ovvero caricamento incompleto) non si riflette nella metrica della capacità di archiviazione del volume di destinazione, ma si riflette nella CloudWatch metrica della capacità di `StorageUsed` archiviazione del file system principale. `StorageUsed` CloudWatch
- Una volta completata un'operazione di caricamento in più parti, i metadati della parte associata non vengono più memorizzati con l'oggetto. Ciò significa che non è possibile recuperare i metadati delle parti dell'oggetto utilizzando `GetObjectAttributes` o scaricare una singola parte di un oggetto in base al numero di parte dell'oggetto letto.

Elenco di controllo degli accessi (ACL)

Le liste di controllo degli accessi di Amazon S3 (ACLs) consentono di gestire l'accesso a bucket e oggetti. I punti di accesso S3 supportano FSx solo il valore ACL. `bucket-owner-full-control` L'utilizzo di qualsiasi altro valore ACL genererà un'eccezione. `InvalidArgument`

Gestione dell'accesso ai punti di accesso

Puoi configurare ogni punto di accesso S3 con autorizzazioni e controlli di rete distinti che S3 applica per qualsiasi richiesta effettuata utilizzando quel punto di accesso. I punti di accesso S3 supportano le policy relative alle risorse AWS Identity and Access Management (IAM) che puoi utilizzare per controllare l'uso del punto di accesso in base alla risorsa, all'utente o ad altre condizioni. Affinché un'applicazione o un utente possa accedere ai file tramite un punto di accesso, sia il punto di accesso che il volume sottostante devono consentire la richiesta. Per ulteriori informazioni, consulta Politiche dei punti di accesso IAM.

I punti di accesso Amazon S3 FSx per ONTAP utilizzano un modello di autorizzazione a doppio livello che combina le autorizzazioni AWS IAM con le autorizzazioni a livello di file system. Questo approccio garantisce che le richieste di accesso ai dati siano autorizzate correttamente sia a livello di AWS servizio che a livello di file system sottostante.

Affinché un'applicazione o un utente possa accedere correttamente ai dati tramite un punto di accesso, sia la policy del punto di accesso S3 che il volume sottostante FSx per ONTAP devono consentire la richiesta.

Argomenti

- Identità e autorizzazione dell'utente del file system
- Autorizzazione della richiesta API S3
- Blocco dell'accesso pubblico di S3
- Politiche dei punti di accesso IAM

Identità e autorizzazione dell'utente del file system

Quando crei un punto di accesso S3 per un volume FSx for ONTAP, specifichi un'identità del file system che verrà utilizzata per autorizzare tutte le richieste di file system effettuate tramite quel punto di accesso. Questa identità del file system determina il livello di accesso concesso ai file e alle directory sottostanti in base al modello di autorizzazione del file system. L'utente del file system è

un account utente sul FSx file system Amazon sottostante. Se l'utente del file system ha accesso in sola lettura, vengono autorizzate solo le richieste di lettura effettuate utilizzando il punto di accesso e le richieste di scrittura vengono bloccate. Se l'utente del file system dispone di accesso in lettura/scrittura, sono autorizzate sia le richieste di lettura che quelle di scrittura al volume allegato effettuate utilizzando il punto di accesso.

L'identità del file system può essere di due tipi:

- Identità UNIX: utilizzate un'identità UNIX (nome utente) per accedere ai volumi con lo stile di sicurezza UNIX
- Identità Windows: utilizza un'identità Windows (dominio e nome utente) per accedere ai volumi con lo stile di sicurezza NTFS.

Quando specifichi un'identità UNIX o Windows, tutte le operazioni dell'API S3 eseguite tramite il punto di accesso sono autorizzate utilizzando le autorizzazioni dell'utente sul file system.

L'identità del file system associata al punto di accesso determina il livello di accesso a file e directory. Ad esempio, se si associa il punto di accesso all'identità UNIX radice (UID 0), che in genere dispone di autorizzazioni complete di accesso ai file sul file system, tutte le operazioni sui file sarebbero autorizzate. Al contrario, se si associa il punto di accesso a un'identità utente limitata, le operazioni sui file sarebbero limitate a ciò a cui l'utente può accedere in base al modello di autorizzazione del file system.

È necessario utilizzare il tipo di identità del file system UNIX per i volumi con stile di sicurezza UNIX e il tipo di identità Windows per i volumi con stile di sicurezza NTFS. Questo allineamento garantisce che il modello di autorizzazione corrisponda alla configurazione di sicurezza del volume.

Per i volumi in stile di sicurezza UNIX, il file system utilizza i bit di modalità o per controllare l'accesso. NFSv4 ACLs Per i volumi in stile di sicurezza NTFS, il file system utilizza Windows per controllare l'accesso. ACLs

> **Important**
>
> Il collegamento di un punto di accesso S3 a un volume FSx for ONTAP non modifica il comportamento del volume quando si accede direttamente al volume tramite NFS o SMB. Tutte le operazioni esistenti sul volume continueranno a funzionare come prima. Le restrizioni incluse in una policy sui punti di accesso S3 si applicano solo alle richieste effettuate utilizzando il punto di accesso.

Autorizzazione della richiesta API S3

Quando effettui una richiesta API S3 tramite un punto di accesso collegato a un volume FSx for NetApp ONTAP, Amazon S3 valuta le autorizzazioni IAM del principale chiamante rispetto alla policy delle risorse IAM del punto di accesso. Il chiamante principale IAM deve disporre delle autorizzazioni necessarie concesse tramite le proprie politiche basate sull'identità e la politica delle risorse del punto di accesso deve inoltre consentire l'azione richiesta.

Amazon S3 valuta tutte le policy pertinenti, incluse le policy degli utenti, le policy dei punti di accesso, le policy degli endpoint VPC e le politiche di controllo del servizio, per determinare se autorizzare la richiesta.

Puoi anche configurare un punto di accesso S3 per accettare solo le richieste da uno specifico cloud privato virtuale (VPC) per limitare l'accesso ai dati. Per ulteriori informazioni, consulta Creazione di access point limitati a un cloud privato virtuale.

Blocco dell'accesso pubblico di S3

I punti di accesso Amazon S3 collegati a un volume FSx for ONTAP vengono configurati automaticamente con l'accesso pubblico a blocchi abilitato, che non è possibile modificare.

Politiche dei punti di accesso IAM

I punti di accesso Amazon S3 supportano politiche di risorse AWS Identity and Access Management (IAM) che consentono di controllare l'uso del punto di accesso in base alla risorsa, all'utente o ad altre condizioni. Affinché un'applicazione o un utente possano accedere agli oggetti tramite un punto di accesso, sia il punto di accesso che l'origine dati sottostante devono consentire la richiesta.

L'`s3:PutAccessPointPolicy`autorizzazione è necessaria per creare una policy opzionale per i punti di accesso.

Dopo aver collegato un access point S3 a un FSx volume Amazon, tutte le operazioni esistenti sul volume continueranno a funzionare come prima. Le limitazioni incluse in una policy di access point si applicano solo alle richieste effettuate tramite quell'access point. Per maggiori informazioni, consulta Configurazione delle policy IAM per l'utilizzo dei punti di accesso nella Guida per l'utente di Amazon Simple Storage Service.

Puoi configurare una policy per i punti di accesso quando crei un punto di accesso collegato a un volume FSx for ONTAP utilizzando la FSx console Amazon. Per aggiungere, modificare o eliminare

una politica del punto di accesso su un punto di accesso S3 esistente, puoi utilizzare la console S3, la CLI o l'API.

Creazione di un access point

Puoi creare e gestire punti di accesso S3 che si collegano ai FSx volumi Amazon utilizzando la FSx console Amazon, la CLI, l'API e Supported. SDKs

> **Note**
>
> Poiché potresti voler pubblicizzare il nome del tuo punto di accesso S3 in modo che altri utenti possano utilizzarlo, evita di includere informazioni sensibili nel nome del punto di accesso S3. I nomi dei punti di accesso vengono pubblicati in un database accessibile pubblicamente noto come sistema dei nomi di dominio (DNS). Per ulteriori informazioni sui nomi dei punti di accesso, consulta. Regole di denominazione dei punti di accesso

Autorizzazioni richieste

Le seguenti autorizzazioni sono necessarie per creare un punto di accesso S3 collegato a un volume Amazon FSx :

- `fsx:CreateAndAttachS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:GetAccessPoint`

L'`s3:PutAccessPointPolicy`autorizzazione è necessaria per creare una policy di Access Point opzionale utilizzando la console Amazon FSx o S3. Per ulteriori informazioni, consulta Politiche dei punti di accesso IAM.

Per creare un punto di accesso, consulta i seguenti argomenti.

Argomenti

- Creazione di access point
- Creazione di access point limitati a un cloud privato virtuale

Creazione di access point

> **Important**
>
> Per collegare un access point S3 a un volume FSx for ONTAP, il volume deve essere montato (avere un percorso di giunzione). Consulta la documentazione di ONTAP per maggiori dettagli.

Il volume FSx for ONTAP deve essere già presente nel tuo account quando crei un punto di accesso S3 per il tuo volume.

Per creare il punto di accesso S3 collegato a un volume FSx for ONTAP, specificate le seguenti proprietà:

- Nome del punto di accesso. Per informazioni sulle regole di denominazione dei punti di accesso, consulta. Regole di denominazione dei punti di accesso
- L'identità dell'utente del file system da utilizzare per autorizzare le richieste di accesso ai file effettuate utilizzando il punto di accesso. Specificate in UNIX o Windows il nome utente POSIX che desiderate includere. Per ulteriori informazioni, consulta Identità e autorizzazione dell'utente del file system.
- La configurazione di rete del punto di accesso determina se il punto di accesso è accessibile da Internet o se l'accesso è limitato a uno specifico cloud privato virtuale (VPC). Per ulteriori informazioni, consulta Creazione di access point limitati a un cloud privato virtuale.

Per creare un punto di accesso S3 collegato a un FSx volume (console) FSx

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nella barra di navigazione nella parte superiore della pagina, scegli quello Regione AWS in cui desideri creare un punto di accesso. Il punto di accesso deve essere creato nella stessa regione del volume associato.
3. Nel riquadro di navigazione a sinistra, scegli Volumi.
4. Nella pagina Volumi, scegli FSx il volume ONTAP a cui desideri collegare il punto di accesso.
5. Visualizza la pagina Crea punto di accesso S3 scegliendo Crea punto di accesso S3 dal menu Azioni.

6. Per il nome del punto di accesso, inserisci il nome del punto di accesso. Per ulteriori informazioni sulle linee guida e le restrizioni relative ai nomi dei punti di accesso, vedereRegole di denominazione dei punti di accesso.

   I dettagli sull'origine dei dati vengono compilati con le informazioni del volume scelto nel passaggio 3.

7. L'identità utente del file system viene utilizzata da Amazon FSx per autenticare le richieste di accesso ai file effettuate utilizzando questo punto di accesso. Assicurati che l'utente del file system specificato disponga delle autorizzazioni corrette sul volume FSx for ONTAP.

   Per il tipo di identità utente del file system, seleziona UNIX o Windows.

8. Per Nome utente, immettere il nome utente dell'utente.

9. Nel pannello di configurazione della rete, scegli se il punto di accesso è accessibile da Internet o se l'accesso è limitato a uno specifico cloud privato virtuale.

   Per Origine di rete, scegli Internet per rendere il punto di accesso accessibile da Internet oppure scegli Virtual private cloud (VPC) e inserisci l'ID VPC da cui desideri limitare l'accesso al punto di accesso.

   Per ulteriori informazioni sulle origini della rete per i punti di accesso, consulta Creazione di access point limitati a un cloud privato virtuale.

10. (Facoltativo) In Access Point Policy - opzionale, specifica una policy opzionale per il punto di accesso. Assicurati di risolvere eventuali avvisi, errori e suggerimenti relativi alle policy. Per ulteriori informazioni sulla specificazione di una policy per i punti di accesso, consulta Configurazione delle policy IAM per l'utilizzo dei punti di accesso nella Amazon Simple Storage Service User Guide.

11. Scegli Crea punto di accesso per rivedere la configurazione degli allegati del punto di accesso.

Per creare un punto di accesso S3 collegato a un FSx volume (CLI)

Il comando di esempio seguente crea un punto di accesso denominato *my-ontap-ap* che è collegato al volume FSx for ONTAP *fsvol-0123456789abcdef9* nell'account. *111122223333*

```
$ aws fsx create-and-attach-s3-access-point --name my-ontap-ap --type ONTAP --ontap-configuration \
   VolumeId=fsvol-0123456789abcdef9,FileSystemIdentity='{Type=UNIX,UnixUser={Name=ec2-user}}' \
```

```
    --s3-access-point VpcConfiguration='{VpcId=vpc-0123467},Policy=access-point-policy-
json
```

In caso di richiesta riuscita, il sistema risponde restituendo il nuovo allegato del punto di accesso S3.

```
$ {
  {
     "S3AccessPointAttachment": {
        "CreationTime": 1728935791.8,
        "Lifecycle": "CREATING",
        "LifecycleTransitionReason": {
            "Message": "string"
        },
        "Name": "my-ontap-ap",
        "OntapConfiguration": {
            "VolumeId": "fsvol-0123456789abcdef9",
            "FileSystemIdentity": {
                "Type": "UNIX",
                "UnixUser": {
                    "Name": "ec2-user"
                }
            }
        },
        "S3AccessPoint": {
            "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/my-ontap-ap",
            "Alias": "my-ontap-ap-aqfqprnstn7aefdfbarligizwgyfouse1a-ext-s3alias",
            "VpcConfiguration": {
                "VpcId": "vpc-0123467"
        }
     }
  }
}
```

Creazione di access point limitati a un cloud privato virtuale

Quando crei un punto di accesso, puoi scegliere di renderlo accessibile da Internet oppure puoi specificare che tutte le richieste effettuate tramite quel punto di accesso devono provenire da uno specifico Amazon Virtual Private Cloud. Un access point accessibile da Internet ha l'origine di rete `Internet`. Può essere utilizzato da qualsiasi punto di Internet, fatte salve eventuali altre restrizioni di accesso in vigore per il punto di accesso, il bucket sottostante o FSx il volume Amazon e le risorse correlate, come gli oggetti richiesti. Un punto di accesso accessibile solo da uno specifico Amazon

VPC ha un'origine di rete di VPC e Amazon S3 rifiuta qualsiasi richiesta effettuata al punto di accesso che non provenga da tale Amazon VPC.

> **Important**
>
> Puoi specificare l'origine di rete di un access point solo quando crei l'access point. Dopo aver creato l'access point, non è più possibile modificare l'origine di rete.

Per limitare un punto di accesso all'accesso solo ad Amazon VPC, includi il `VpcConfiguration` parametro nella richiesta di creazione del punto di accesso. Nel `VpcConfiguration` parametro, specifichi l'ID Amazon VPC che desideri utilizzare per l'access point. Se viene effettuata una richiesta tramite il punto di accesso, la richiesta deve provenire da Amazon VPC o Amazon S3 la rifiuterà.

Puoi recuperare l'origine di rete di un punto di accesso utilizzando AWS CLI, AWS SDKs o REST. APIs Se per un punto di accesso è specificata una configurazione Amazon VPC, la sua origine di rete è. VPC In caso contrario, l'origine della rete dell'access point è `Internet`.

Example

Esempio: creare un punto di accesso limitato all'accesso ad Amazon VPC

L'esempio seguente crea un punto di accesso denominato `example-vpc-ap` bucket `amzn-s3-demo-bucket` in account `123456789012` che consente l'accesso solo da `vpc-1a2b3c` Amazon VPC. L'esempio verifica quindi che il nuovo access point abbia l'origine di rete VPC.

AWS CLI

```
$ aws fsx create-and-attach-s3-access-point --name example-vpc-ap --type ONTAP --
ontap-configuration \

 VolumeId=fsvol-0123456789abcdef9,FileSystemIdentity='{Type=UNIX,UnixUser={Name=ec2-
user}}' \
   --s3-access-point VpcConfiguration='{VpcId=vpc-id},Policy=access-point-policy-
json
```

```
$ {
  {
     "S3AccessPointAttachment": {
        "Lifecycle": "CREATING",
```

```
        "CreationTime": 1728935791.8,
        "Name": "example-vpc-ap",
        "OntapConfiguration": {
            "VolumeId": "fsvol-0123456789abcdef9",
            "FileSystemIdentity": {
                "Type": "UNIX",
                "UnixUser": {
                    "Name": "my-unix-user"
                }
            }
        },
        "S3AccessPoint": {
            "ResourceARN": "arn:aws:s3:us-east-1:111122223333:accesspoint/example-
vpc-ap",
            "Alias": "access-point-abcdef0123456789ab12jj77xy51zacd4-ext-s3alias",
            "VpcConfiguration": {
                "VpcId": "vpc-1a2b3c"
            }
        }
    }
  }
```

Per utilizzare un punto di accesso con un Amazon VPC, devi modificare la politica di accesso per il tuo endpoint Amazon VPC. Gli endpoint Amazon VPC consentono al traffico di fluire dal tuo Amazon VPC ad Amazon S3. Dispongono di politiche di controllo degli accessi che controllano il modo in cui le risorse all'interno di Amazon VPC possono interagire con Amazon S3. Le richieste dal tuo Amazon VPC ad Amazon S3 hanno successo tramite un punto di accesso solo se la policy degli endpoint di Amazon VPC consente l'accesso sia al punto di accesso che al bucket sottostante.

> **Note**
>
> Per rendere le risorse accessibili solo all'interno di un Amazon VPC, assicurati di creare una zona ospitata privata per il tuo endpoint Amazon VPC. Per utilizzare una zona ospitata privata, modifica le impostazioni di Amazon VPC in modo che gli attributi di rete Amazon VPC siano `enableDnsHostnames` impostati `enableDnsSupport` su. `true`

La seguente dichiarazione politica di esempio configura un endpoint Amazon VPC per consentire le chiamate verso un punto `GetObject` di accesso denominato. `example-vpc-ap`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
    {
        "Principal": "*",
        "Action": [
            "s3:GetObject"
        ],
        "Effect": "Allow",
        "Resource": [
            "arn:aws:s3:us-east-1:123456789012:accesspoint/example-vpc-ap/object/
*"
        ]
    }]
}
```

> **Note**
>
> La dichiarazione `Resource` in questo esempio utilizza un Amazon Resource Name (ARN) per specificare l'access point.

Per ulteriori informazioni sulle politiche degli endpoint di Amazon VPC, consulta Gateway endpoints for Amazon S3 nella Amazon VPC User Guide.

Gestione dei punti di accesso Amazon S3

Questa sezione spiega come gestire e utilizzare i punti di accesso Amazon S3 utilizzando l'API Console di gestione AWS AWS Command Line Interface, o.

Argomenti

- Elenco degli allegati dei punti di accesso S3
- Visualizzazione dei dettagli dei punti di accesso
- Eliminazione di un allegato al punto di accesso S3

Elenco degli allegati dei punti di accesso S3

Questa sezione spiega come elencare il punto di accesso S3 utilizzando l'API Console di gestione AWS AWS Command Line Interface, o REST.

Per elencare tutti i punti di accesso S3 collegati a un volume FSx for ONTAP (console Amazon FSx)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione sul lato sinistro della console, scegli Volumi.
3. Nella pagina Volumes, scegli il volume ONTAP per cui desideri visualizzare gli allegati del punto di accesso.
4. Nella pagina dei dettagli del volume, scegli S3 per visualizzare un elenco di tutti i punti di accesso S3 collegati al volume.

Per elencare tutti i punti di accesso S3 collegati a un volume FSx for ONTAP ()AWS CLI

Il comando di `describe-s3-access-point-attachments`esempio seguente mostra come utilizzare AWS CLI per elencare gli allegati dei punti di accesso S3.

Il comando seguente elenca tutti i punti di accesso S3 collegati ai volumi sul file system FSx for ONTAP fs-0abcdef123456789.

```
aws fsx describe-s3-access-point-attachments --filter {[Name: file-system-id, Values:
{[fs-0abcdef123456789]}}
```

Il comando seguente elenca i punti di accesso S3 collegati a un volume for ONTAP [vol-9abcdef123456789]. FSx

```
aws fsx describe-s3-access-point-attachments --filter {[Name: volume-id, Values:
{[vol-9abcdef123456789]}}
```

Per ulteriori informazioni ed esempi, consulta list-access-points nella documentazione di riferimento dei comandi della AWS CLI .

Visualizzazione dei dettagli dei punti di accesso

Questa sezione spiega come visualizzare i dettagli dei punti di accesso S3 utilizzando l' Console di gestione AWS API o REST. AWS Command Line Interface

Per visualizzare i dettagli dei punti di accesso S3 collegati a un volume FSx for ONTAP (console Amazon FSx)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa al volume collegato al punto di accesso di cui desideri visualizzare i dettagli.
3. Scegli S3 per visualizzare l'elenco dei punti di accesso collegati al volume.
4. Scegli il punto di accesso di cui desideri visualizzare i dettagli.
5. Nel riepilogo degli allegati del punto di accesso S3, visualizza i dettagli e le proprietà di configurazione per il punto di accesso selezionato.

   Per l'allegato del punto di accesso sono elencate anche la configurazione dell'identità utente del file system e la politica di autorizzazione del punto di accesso S3.
6. Per visualizzare la configurazione S3 del punto di accesso nella console Amazon S3, scegli il nome del punto di accesso S3 visualizzato sotto il punto di accesso S3. Ti porta alla pagina dei dettagli del punto di accesso nella console Amazon S3.

Eliminazione di un allegato al punto di accesso S3

Questa sezione spiega come eliminare i punti di accesso S3 utilizzando l'API Console di gestione AWS AWS Command Line Interface, o REST.

Le `s3control:DeleteAccessPoint` autorizzazioni `fsx:DetatchAndDeleteS3AccessPoint` e sono necessarie per eliminare un allegato del punto di accesso S3.

Per eliminare un punto di accesso S3 collegato a un volume FSx for ONTAP (console Amazon FSx)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa al volume a cui è allegato l'allegato del punto di accesso S3 che desideri eliminare.
3. Scegli S3 per visualizzare l'elenco dei punti di accesso S3 collegati al volume.
4. Seleziona l'allegato del punto di accesso S3 che desideri eliminare.
5. Scegli Elimina.
6. Conferma di voler eliminare il punto di accesso S3 e scegli Elimina.

Per eliminare un punto di accesso S3 collegato a un volume FSx for ONTAP ()AWS CLI

- Per eliminare gli allegati di un punto di accesso S3, usa il comando CLI a 3 detach-and-delete-spunti di accesso (o l'operazione API AccessPoint S3 DetachAndDeleteequivalente), come mostrato nell'esempio seguente. Utilizza la `--name` proprietà per specificare il nome dell'allegato del punto di accesso S3 che desideri eliminare.

```
aws fsx detach-and-delete-s3-access-point \
    --region us-east-1 \
    --name my-ontap-ap
```

Utilizzo dei punti di accesso

Gli esempi seguenti mostrano come utilizzare i punti di accesso per accedere ai dati dei file archiviati su un volume FSx for ONTAP utilizzando l'API S3. Per un elenco completo delle operazioni dell'API Amazon S3 supportate dai punti di accesso collegati a un volume FSx for ONTAP, consulta. Compatibilità dei punti di accesso

> **Note**
>
> I file presenti nei FSx volumi ONTAP sono identificati con un. `StorageClass` `FSX_ONTAP`

Argomenti

- Scaricamento di un file utilizzando un punto di accesso S3
- Caricamento di un file utilizzando un punto di accesso S3
- Elencare i file utilizzando un punto di accesso S3
- Taggare un file utilizzando un punto di accesso S3
- Eliminazione di un file utilizzando un punto di accesso S3

Scaricamento di un file utilizzando un punto di accesso S3

Il comando di `get-object` esempio seguente mostra come è possibile utilizzare il AWS CLI per scaricare un file tramite un punto di accesso. È necessario includere un outfile, che è un nome di file per l'oggetto scaricato.

L'esempio richiede il file *my-image.jpg* tramite il punto di accesso *my-ontap-ap* e salva il file scaricato come*download.jpg*.

```
$ aws s3api get-object --key my-image.jpg --bucket my-ontap-ap-
hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias download.jpg
{
    "AcceptRanges": "bytes",
    "LastModified": "Mon, 14 Oct 2024 17:01:48 GMT",
    "ContentLength": 141756,
    "ETag": "\"00751974dc146b76404bb7290f8f51bb-1\"",
    "ContentType": "binary/octet-stream",
    "ServerSideEncryption": "SSE_FSX",
    "Metadata": {},
    "StorageClass": "FSX_ONTAP"
}
```

È inoltre possibile utilizzare l'API REST per scaricare un oggetto tramite un punto di accesso. Per ulteriori informazioni, consulta GetObject in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Caricamento di un file utilizzando un punto di accesso S3

Il comando di `put-object` esempio seguente mostra come utilizzare il AWS CLI per caricare un file tramite un punto di accesso. È necessario includere un outfile, che è un nome di file per l'oggetto caricato.

L'esempio carica il file *my-new-image.jpg* tramite il punto di accesso *my-ontap-ap* e salva il file caricato come. *my-new-image.jpg*

```
$ aws s3api put-object --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-
s3alias --key my-new-image.jpg --body  my-new-image.jpg
```

È inoltre possibile utilizzare l'API REST per caricare un oggetto tramite un punto di accesso. Per ulteriori informazioni, consulta PutObject in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Elencare i file utilizzando un punto di accesso S3

L'esempio seguente elenca i file tramite l'alias del punto di accesso *my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b*`-ext-s3alias` posseduto dall'ID dell'account *111122223333* in Region*us-east-2*.

```
$ aws s3api list-objects-v2 --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-
ext-s3alias
{
    "Contents": [
        {
            "Key": ".hidden-dir-with-data/file.txt",
            "LastModified": "2024-10-29T14:22:05.4359",
            "ETag": "\"88990077ab44cd55ef66aa77-1\"",
            "Size": 18,
            "StorageClass": "FSX_ONTAP"
        },
        {
            "Key": "documents/report.rtf",
            "LastModified": "2024-11-02T10:18:15.6621",
            "ETag": "\"ab12cd34ef56a89219zg6aa77-1\"",
            "Size": 1048576,
            "StorageClass": "FSX_ONTAP"
        },
    ]
}
```

Puoi anche utilizzare l'API REST per elencare i tuoi file. Per ulteriori informazioni, consulta ListObjectsV2 in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Taggare un file utilizzando un punto di accesso S3

Il comando di `put-object-tagging` esempio seguente mostra come è possibile utilizzare il AWS CLI per aggiungere un set di tag tramite un punto di accesso. Ogni tag è una coppia chiave-valore. Per ulteriori informazioni, consulta Categorizzazione dello storage mediante tag nella Guida per l'utente di Amazon Simple Storage Service.

L'esempio aggiunge un set di tag al file esistente `my-image.jpg` utilizzando il punto di accesso. *my-ontap-ap*

```
$ aws s3api put-object-tagging --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-
ext-s3alias --key my-image.jpg --tagging TagSet=[{Key="finance",Value="true"}]
```

È inoltre possibile utilizzare l'API REST per aggiungere un set di tag a un oggetto tramite un punto di accesso. Per ulteriori informazioni, consulta PutObjectTagging in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Eliminazione di un file utilizzando un punto di accesso S3

Il comando di `delete-object` esempio seguente mostra come è possibile utilizzare il AWS CLI per eliminare un file tramite un punto di accesso.

```
$ aws s3api delete-object --bucket my-ontap-ap-hrzrlukc5m36ft7okagglf3gmwluquse1b-ext-s3alias --key my-image.jpg
```

È inoltre possibile utilizzare l'API REST per eliminare un oggetto tramite un punto di accesso. Per ulteriori informazioni, consulta DeleteObject in Amazon Simple Storage Service API Reference (Guida di riferimento per l'API di Amazon Simple Storage Service).

Risoluzione dei problemi relativi ai punti di accesso S3

Questa sezione descrive i sintomi, le cause e le soluzioni in caso di problemi di accesso ai FSx dati dagli access point S3.

La creazione del punto di accesso S3 non è riuscita a causa di un errore di ricerca dell'identità utente del file system

Quando si crea e si collega un punto di accesso S3, è necessario fornire un `FileSystemIdentity`. L'utente è responsabile della configurazione dell'utente UNIX o Windows fornito all'interno di ONTAP.

Se `UnixUser`viene fornito un, ONTAP deve essere in grado di mappare il UnixUser nome a UNIX UID/. GIDs ONTAP determina come eseguire questa mappatura utilizzando la configurazione dello switch di servizio dei nomi.

```
> vserver services name-service ns-switch show
```

```
Vserver         Database       Order
--------------- ------------   ---------
svm_1           hosts          files,
                               dns
svm_1           group          files,
                               ldap
svm_1           passwd         files,
                               ldap
svm_1           netgroup       nis,
                               files
```

Assicurati di avere UnixUser una voce nei `group` database `passwd` e che utilizzi una fonte valida (`files`,`ldap`, ecc.). La `files` fonte può essere configurata utilizzando i `vserver services name-service unix-group` comandi `vserver services name-service unix-user` and. La `ldap` sorgente può essere configurata utilizzando il `vserver services name-service ldap` comando.

Se `WindowsUser`viene fornito un, ONTAP deve essere in grado di trovare il WindowsUser nome nel dominio Active Directory aggiunto.

Per confermare se un dato UnixUser o WindowsUser è mappato correttamente, `fsxadmin` puoi usare il seguente comando (sostituisci `-unix-user-name` con `-win-name` for WindowsUsers):

```
> vserver services access-check authentication show-creds -
node FsxId0fd48ff588b9d3eee-01 -vserver svm_name -unix-user-name root -show-partial-
unix-creds true
```

Esempio di output riuscito:

```
 UNIX UID: root

 GID: daemon
 Supplementary GIDs:
  daemon
```

Esempio di output non riuscito:

```
Error: Acquire UNIX credentials procedure failed
  [  2 ms] Entry for user-name: unmapped-user not found in the
           current source: FILES. Entry for user-name: unmapped-user
           not found in any of the available sources
**[     3] FAILURE: Unable to retrieve UID for UNIX user
**         unmapped-user

Error: command failed: Failed to resolve user name to a UNIX ID. Reason: "SecD Error:
 object not found".
```

Una mappatura utente errata può causare `Access Denied` errori da parte di S3. Di seguito sono riportati alcuni esempi di motivi di errore.

`Entry for user-name not found in the current source: LDAP`

Se sei `ns-switch` configurato per utilizzare una `ldap` fonte, assicurati che ONTAP sia configurato per utilizzare correttamente il tuo server LDAP. Per ulteriori informazioni NetApp, consulta il Rapporto tecnico per la configurazione di LDAP.

`RESULT_ERROR_DNS_CANT_REACH_SERVER` o `RESULT_ERROR_SECD_IN_DISCOVERY`

Questo errore indica un problema con la configurazione DNS del vserver in ONTAP. Esegui quanto segue per assicurarti che il DNS del tuo vserver sia configurato correttamente:

```
> dns check -vserver svm_name
```

`NT_STATUS_PENDING`

Questo errore indica un problema di comunicazione con il controller di dominio. La causa sottostante può essere dovuta alla mancanza di crediti SMB. Per ulteriori informazioni, consulta NetApp KB.

La creazione del punto di accesso S3 non è riuscita perché il volume non è montato.

I punti di accesso S3 possono essere collegati solo FSx ai volumi ONTAP montati (con percorsi di giunzione). Questo vale anche per i tipi di volumi DP (Data Protection). Per ulteriori informazioni, consulta la documentazione sul montaggio dei volumi ONTAP.

La creazione del punto di accesso S3 non è riuscita perché il protocollo S3 è disabilitato sulla SVM

I punti di accesso S3 richiedono che il protocollo S3 sia abilitato sulla Storage Virtual Machine (SVM). Per abilitare il protocollo S3, esegui il seguente comando nella CLI di ONTAP utilizzando: `fsxadmin`

```
> vserver add-protocols -vserver svm_name -protocols s3
```

Per verificare che il protocollo sia abilitato:

```
> vserver show -vserver svm_name -fields allowed-protocols,disallowed-protocols
```

Il file system non è in grado di gestire le richieste S3

Se il volume di richieste S3 per un particolare carico di lavoro supera la capacità del file system di gestire il traffico, potrebbero verificarsi errori di richiesta S3 (ad esempio,, `Internal Server Error` e). `503 Slow Down Service Unavailable` Puoi monitorare e generare allarmi in

modo proattivo sulle prestazioni del tuo file system utilizzando i CloudWatch parametri di Amazon (ad esempio `Network throughput utilization` e`CPU utilization`). Se osservi un peggioramento delle prestazioni, puoi risolvere il problema aumentando la capacità di throughput del file system.

Accesso negato con le autorizzazioni predefinite del punto di accesso S3 per i ruoli di servizio creati automaticamente

Alcuni AWS servizi integrati in S3 creeranno un ruolo di servizio personalizzato e personalizzeranno le autorizzazioni allegate in base al tuo caso d'uso specifico. Quando si specifica l'alias del punto di accesso S3 come risorsa S3, le autorizzazioni allegate possono includere il punto di accesso che utilizza un formato ARN bucket (ad esempio,) `arn:aws:s3:::my-fsx-ap-foo7detztxouyjpwtu8krroppxytruse1a-ext-s3alias` anziché il formato ARN del punto di accesso (ad esempio,). `arn:aws:s3:us-east-1:1234567890:accesspoint/my-fsx-ap` Per risolvere questo problema, modificare la politica in modo da utilizzare l'ARN del punto di accesso.

Accesso ai dati da altri servizi AWS

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

Argomenti

- Usare Amazon WorkSpaces con FSx per ONTAP
- Utilizzo di Amazon Elastic Container Service con FSx for ONTAP
- Utilizzo di Amazon Elastic VMware Service con FSx for ONTAP
- FSx Utilizzo del cloud con for ONTAP VMware

Usare Amazon WorkSpaces con FSx per ONTAP

FSx for ONTAP può essere utilizzato con Amazon per WorkSpaces fornire un dispositivo NAS (Network-Attached Storage) condiviso o per archiviare profili di roaming per gli 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 per fornire WorkSpaces al profilo di roaming e all'accesso alla cartella home un'esperienza coerente e fornire una cartella di team condivisa per WorkSpaces gli utenti Windows e Linux. 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
- Fornisci una cartella condivisa per accedere ai file comuni

Fornisci supporto per i profili di roaming

Puoi utilizzare 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 FSx file Amazon, consentendo la condivisione di documenti e impostazioni tra diverse WorkSpaces istanze e il backup automatico tramite i backup automatici FSx giornalieri di Amazon.

Passaggio 1: crea una posizione per la cartella del profilo per gli utenti del dominio utilizzando Amazon FSx

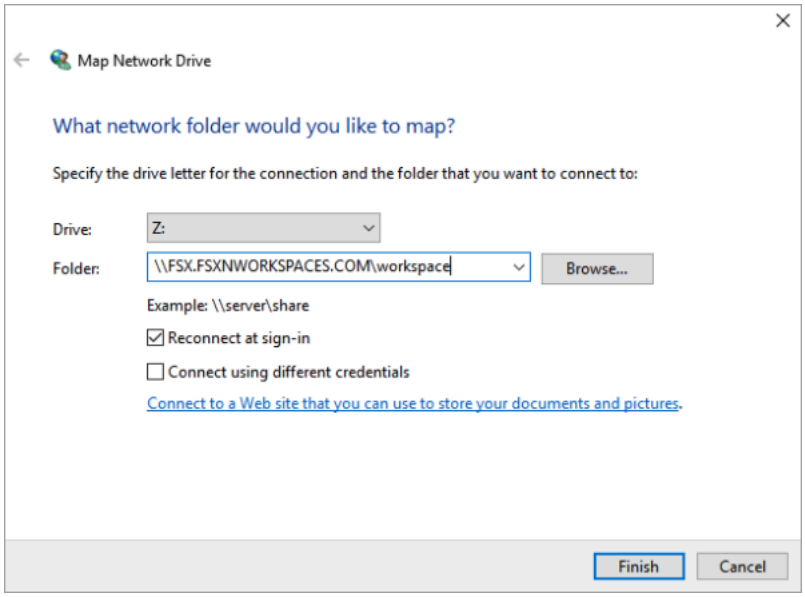
1. Crea un file system FSx for ONTAP utilizzando la FSx console Amazon. Per ulteriori informazioni, consulta Per creare un file system (console).

   > **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 per ONTAP sceglie un intervallo di indirizzi IP predefinito non utilizzato 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 da WorkSpaces, 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 FlexVol volume (console).
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' EC2 istanza Amazon che esegue Windows Server o da un WorkSpace. Per ulteriori informazioni, consulta Accesso ai dati di FSx for ONTAP.
6. Mappi la tua condivisione `Z:\` su un' WorkSpaces istanza Windows:



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 prova in modo che abbia un profilo di roaming sul tuo FSx file system Amazon. Nel tuo amministratore WorkSpaces, apri una PowerShell console e usa un comando

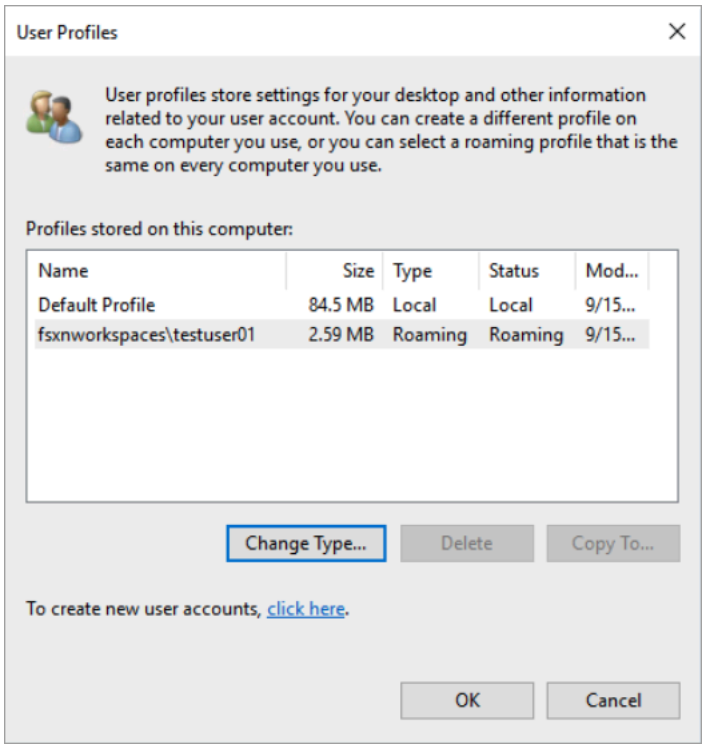
simile al seguente esempio (che utilizza la `profiles` cartella che hai creato in precedenza nel passaggio 1):

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

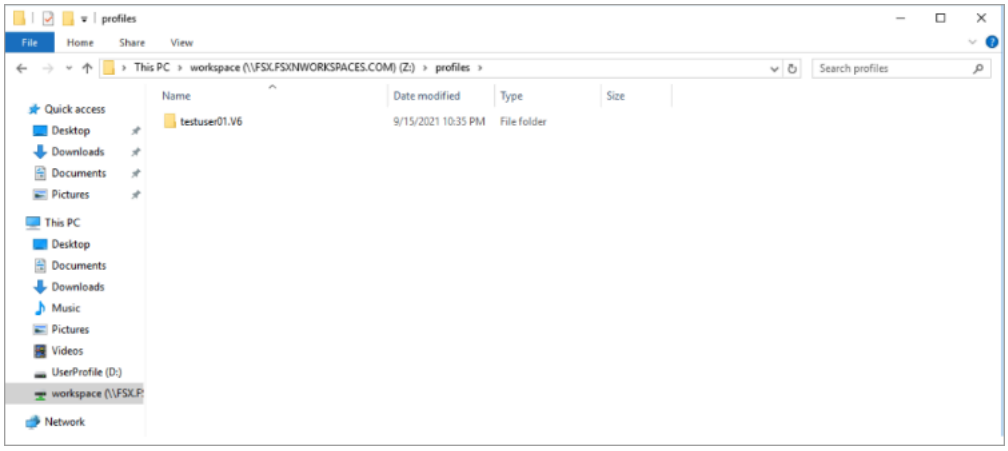
Per esempio:

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

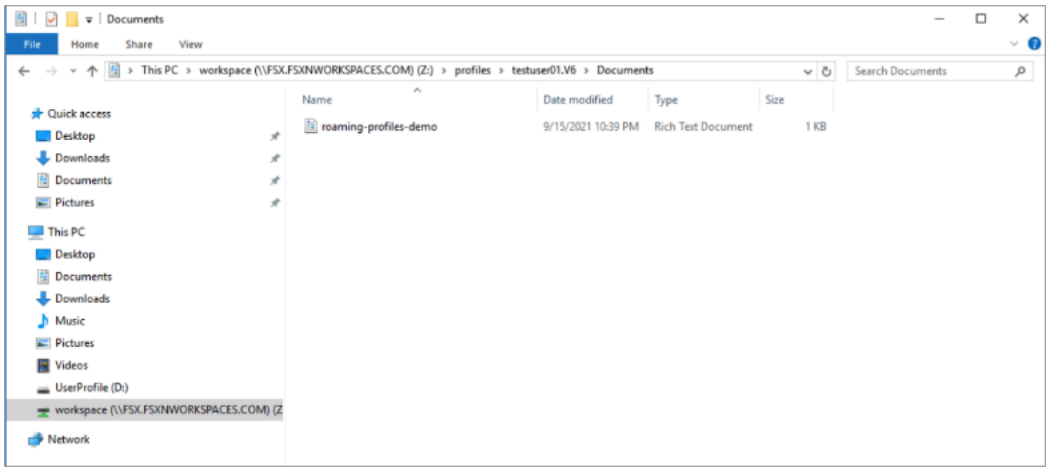
5. Accedere all'utente di prova WorkSpace.
6. In Proprietà del sistema, seleziona la scheda Avanzate e premi il pulsante Impostazioni nella sezione Profili utente. L'utente che ha effettuato l'accesso avrà un tipo di profilo di. `Roaming`



7. Sfoglia la cartella condivisa 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 FSx condivisa Amazon 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*

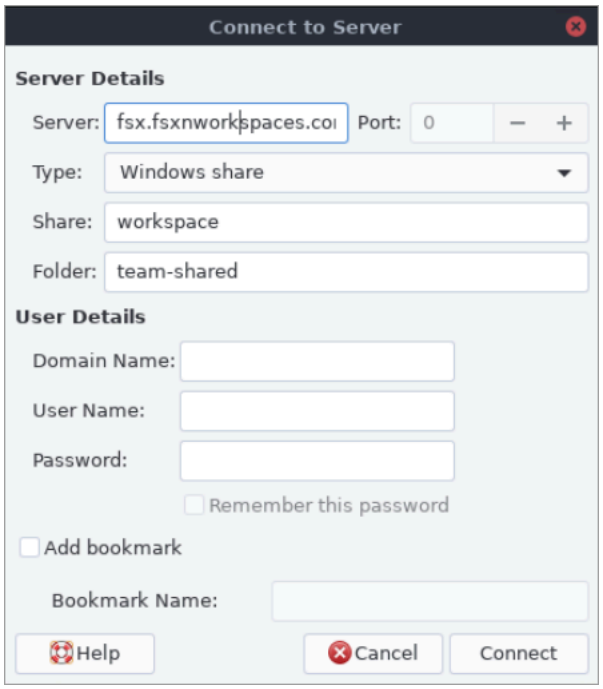
   b. Imposta Tipo su`Windows share`.

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

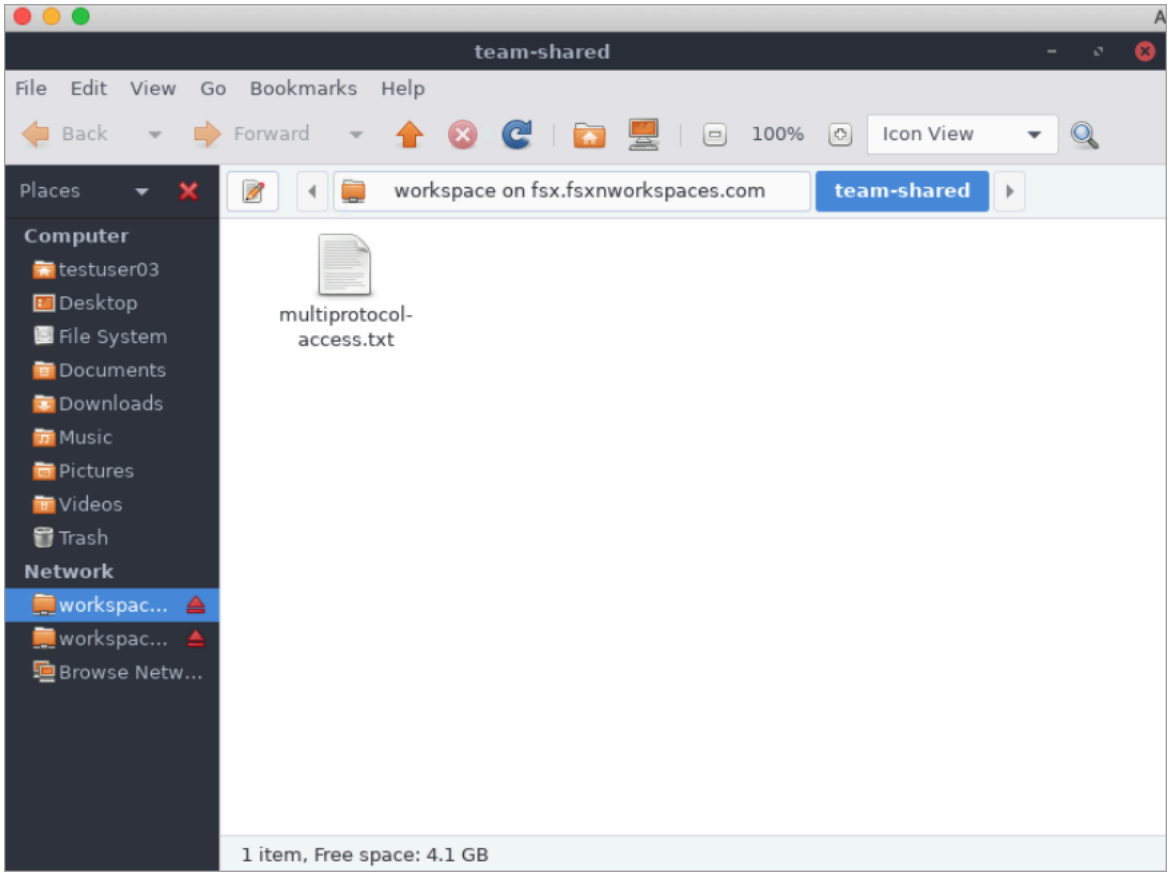
   d. È possibile lasciare la cartella invariata / o impostarla su una cartella, ad esempio una cartella denominata`team-shared`.

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

   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 for 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 dell'SVM anziché il relativo 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. Sostituisci `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. Sostituisci `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 Amazon Elastic VMware Service con FSx for ONTAP

Puoi utilizzarlo FSx per ONTAP come datastore esterno per i Software-Defined Data Center di Amazon Elastic Service VMware (Amazon EVS) (). SDDCs Per ulteriori informazioni, consulta Esegui

carichi di lavoro ad alte prestazioni con Amazon FSx for NetApp ONTAP. Per istruzioni dettagliate, consulta Configurare Amazon FSx for NetApp ONTAP come datastore NFS e Configurare Amazon FSx for NetApp ONTAP come datastore iSCSI.

FSx Utilizzo del cloud con for ONTAP VMware

Puoi utilizzarlo FSx per ONTAP come datastore esterno per VMware Cloud on AWS Software-Defined Data Center (). SDDCs Per ulteriori informazioni, consulta Configurare Amazon FSx for NetApp ONTAP come storage esterno e VMware cloud on AWS with Amazon FSx for NetApp ONTAP Deployment Guide.

Disponibilità, durabilità e opzioni di implementazione

Amazon FSx for NetApp ONTAP utilizza tipi di implementazione Single-AZ e Multi-AZ. Puoi scegliere tra quattro opzioni: Single-AZ 1, Single-AZ 2, Multi-AZ 1 e Multi-AZ 2. Questo argomento descrive le funzionalità 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.

Tipi di implementazione Single-AZ

Puoi scegliere tra Single-AZ 1 e Single-AZ 2 per il tuo file system Single-AZ. Single-AZ 1 è un file system di prima generazione con una coppia ad alta disponibilità (HA), mentre Single-AZ 2 è un file system di seconda generazione con 1—12 coppie HA. Per ulteriori informazioni, consulta Scelta della generazione di file system.

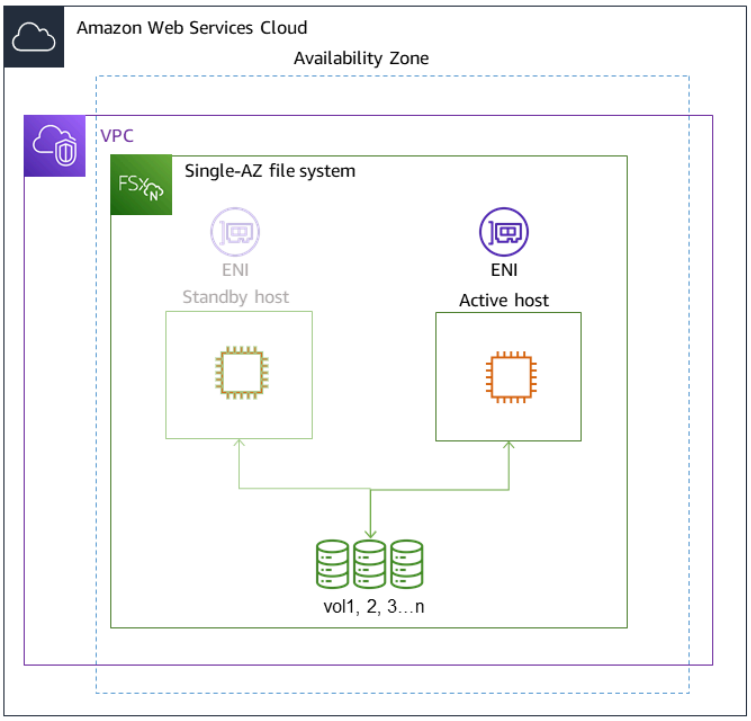
Quando crei un file system Single-AZ, Amazon effettua FSx automaticamente il provisioning da una a dodici coppie di file server in una configurazione di standby attivo, con i file server attivi e in standby di ciascuna coppia situati in domini di errore separati all'interno di una singola zona di disponibilità nel. Regione AWS Durante la manutenzione pianificata del file system o un'interruzione non pianificata del servizio di qualsiasi file server attivo, Amazon esegue FSx 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 monitora FSx continuamente i guasti hardware e sostituisce automaticamente i componenti dell'infrastruttura in caso di guasto. Per ottenere una

durabilità elevata, Amazon replica FSx 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 di prima generazione FSx per ONTAP Single-AZ.



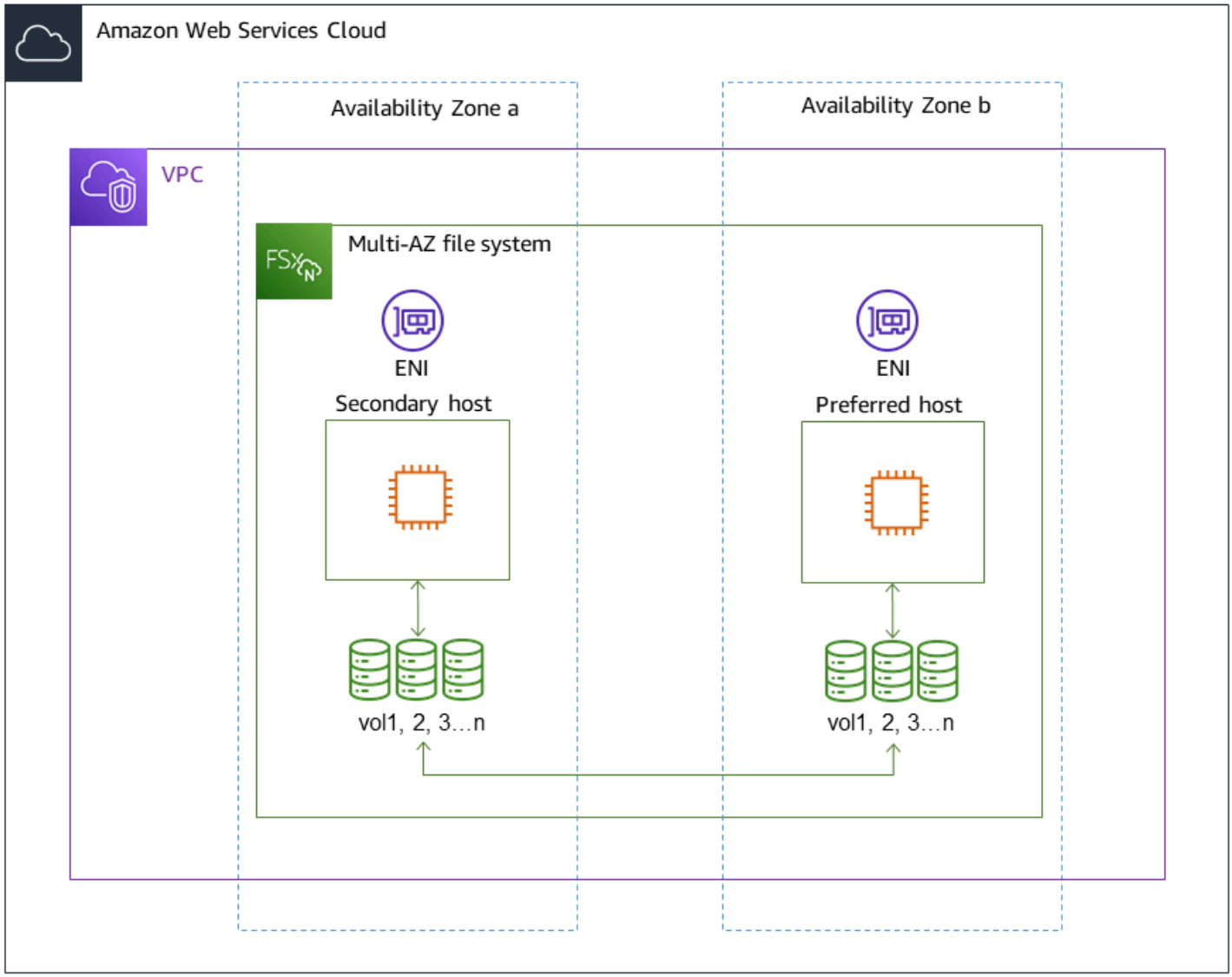
Tipi di implementazione Multi-AZ

È possibile scegliere tra Multi-AZ 1 e Multi-AZ 2 per il file system Multi-AZ. Multi-AZ 1 è un file system di prima generazione e Multi-AZ 2 è un file system di seconda generazione. Entrambe le opzioni hanno una coppia HA. Per ulteriori informazioni, consulta Scelta della generazione di file system.

I file system Multi-AZ supportano tutte le funzionalità 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 di prima generazione per ONTAP Multi-AZ. FSx



Scelta della generazione di file system

La tabella seguente illustra le differenze tra i file system Single-AZ e FSx Multi-AZ for ONTAP di prima e seconda generazione.

FSx per generazioni di file system ONTAP

Dimensione	Prima generazione	Seconda generazione (coppia HA singola)	Seconda generazione (multippia)
Il tipo di distribuzione	SINGLE_AZ_1 MULTI_AZ_1	SINGLE_AZ_2 MULTI_AZ_2	SINGLE_AZ_2
coppie HA	1 paio HA		1—12 paia HA
Archiviazione SSD	Minimo: 1 TiB Massimo: 192 TiB	Minimo: 1 TiB Massimo: 512 TiB	Minimo: 1 TiB (per coppia HA) Massimo: 1 PiB (totale)
SSD IOPS	Minimo: 3 IOPS/ GIB di SSD Massimo: 160.000	Minimo: 3 IOPS/ GIB di SSD Massimo: 200.000	Minimo: 3 IOPS/ GIB di SSD Massimo: 2.400.000 (200.000 per coppia HA)
Capacità di throughput	128 MBps; 256; 512 MBps; 1.024 MBps; 2.048 MBps; 4.096 MBps MBps	384 MBps; 768; 1.536; 3.072; 6.144 MBps MBps MBps MBps	1.536 MBps (per coppia HA); 3.072 (per coppia HA); 6.144 MBps (per coppia HA) MBps

> **Note**
>
> Non è possibile modificare il tipo di distribuzione del file system dopo la creazione. Se desideri modificare il tipo di distribuzione (ad esempio, passare da Single-AZ 1 a Single-AZ

2), puoi eseguire il backup dei dati e ripristinarli su un nuovo file system. Puoi anche migrare i tuoi dati con NetApp SnapMirror AWS DataSync, con o con uno strumento di copia dei dati di terze parti. Per ulteriori informazioni, consulta Migrazione a for ONTAP utilizzando FSx NetApp SnapMirror e Migrazione a FSx for ONTAP utilizzando AWS DataSync.

Processo di failover per ONTAP FSx

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 di seconda generazione con più coppie HA, il comportamento di failover di ciascuna 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 in genere 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 ai file system FSx for ONTAP Single-AZ e Multi-AZ, consulta. Accesso ai dati dall'interno di Cloud AWS

Test del failover su un file system

È possibile testare il failover sul file system 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 FSx console Amazon, nella CLI e nell'API. Per ulteriori informazioni sulla modifica della capacità di throughput del file system e sul monitoraggio dello stato di 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, FSx Amazon fornisce due interfacce di rete elastiche (ENI) nella sottorete associata al file system. Per i file system Multi-AZ, Amazon fornisce FSx anche due ENIs, una in ciascuna delle sottoreti associate al file system. I client comunicano con il tuo FSx file system Amazon 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 dai file server preferiti a quelli 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 relative a sottorete, elastic network interface e indirizzi IP per ciascuno dei tipi di distribuzione del FSx file system ONTAP:

	Single-AZ di prima generazione	Single-AZ di seconda generazione	Multi-AZ
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 SVMs presenti nel file system	Numero di coppie HA + Numero di coppie HA moltiplicato per il numero di SVMs nel file system	1 + il numero di SVMs nel file system

	Single-AZ di prima generazione	Single-AZ di seconda generazione	Multi-AZ
Numero di percorsi della tabella di routing VPC	N/D	N/D	1 + il numero di SVMs 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 scollega FSx automaticamente qualsiasi indirizzo IP elastico, che è un indirizzo IP pubblico raggiungibile da Internet, che viene collegato all'interfaccia di rete elastica di un file system.

Amazon FSx per le prestazioni di NetApp 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 FSx per i file system ONTAP

Le prestazioni del file system vengono misurate in base alla latenza, alla velocità effettiva e I/O alle operazioni al secondo (IOPS).

Latenza

Amazon FSx for NetApp ONTAP offre latenze di funzionamento dei file 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 ciascun 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 FSx file system Amazon fornisce fino a decine GBps di velocità effettiva 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 archiviazione 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. NFSv3 NFSv4e supporto 1.1+. `nconnect` 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 client NFS per confermare se `nconnect` è supportato nella versione del client in uso. Per ulteriori informazioni sul NetApp ONTAP supporto per`nconnect`, consulta il ONTAPsupporto per la versione NFSv4 2.1.

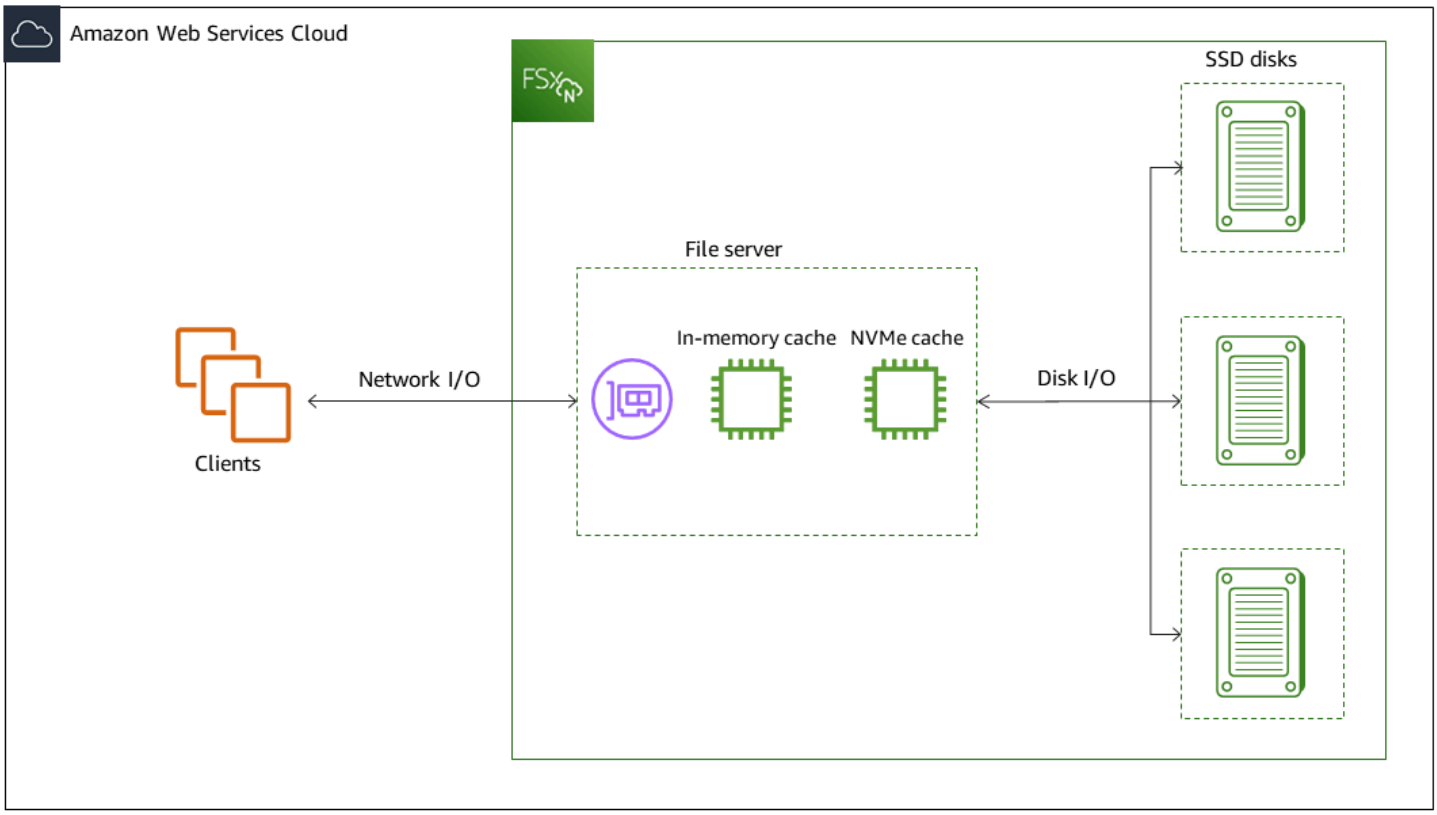
Cornici Jumbo

Per ottenere il massimo throughput di lettura o scrittura, consigliamo di abilitare i jumbo frame su tutte le interfacce di rete nel percorso dati del file system Amazon FSx, incluse le istanze EC2 client. L'impostazione predefinita dell'unità di trasmissione massima (MTU) per le interfacce di rete sul file system for ONTAP è di 9.001 byte FSx .

Dettagli sulle prestazioni

Per comprendere nel dettaglio il modello di prestazioni di Amazon FSx for NetApp ONTAP, puoi esaminare i componenti architettonici di un FSx file system Amazon. Le istanze di calcolo dei tuoi client, indipendentemente dal fatto che esistano internamente AWS o localmente, 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 e NVMe una cache in memoria veloci su ogni file server per migliorare le prestazioni dei 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, NVMe cache e volumi di storage) corrispondono le principali caratteristiche prestazionali di un file system Amazon FSx for NetApp ONTAP che determinano il throughput complessivo e le prestazioni IOPS.

- I/O Prestazioni di rete: delle richieste tra i client e throughput/IOPS il file server (in forma aggregata)
- Dimensioni della memoria e NVMe della cache sul file server: dimensione del set di lavoro attivo che può essere utilizzato per la memorizzazione nella cache
- I/O Prestazioni del disco: throughput/IOPS delle richieste tra il file server e i dischi di archiviazione

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 system. Le prime due caratteristiche prestazionali, le I/O prestazioni di rete e le dimensioni della memoria e NVMe della cache, 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 attività brevi e intensi, con lunghi periodi di inattività tra un'interruzione e l'altra. I/O 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 rete che su disco. I/O I/O Amazon FSx utilizza un meccanismo I/O di credito di rete per allocare throughput e IOPS in base all'utilizzo medio: i file system accumulano crediti quando il loro throughput e l'utilizzo degli IOPS sono inferiori ai limiti di base e possono utilizzare questi crediti per eseguire operazioni. I/O

> **Note**
>
> Per i protocolli iSCSI e NVMe/TCP SAN, le operazioni client di lettura sequenziale possono raggiungere il massimo I/O burst di rete o il throughput di base del file system.

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

Puoi creare file system Single-AZ e Multi-AZ con FSx for ONTAP. I file system di prima generazione (sia Single-AZ che Multi-AZ) e i file system Multi-AZ di seconda generazione sono alimentati da una coppia ad alta disponibilità (HA). I file system Single-AZ di seconda generazione sono alimentati da un massimo di 12 coppie HA. Per ulteriori informazioni, consulta Gestione delle coppie ad alta disponibilità (HA).

FSx per i file system ONTAP Multi-AZ e Single-AZ offrono latenze di funzionamento dei file costanti inferiori al millisecondo con 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 per ridurre le latenze di lettura e aumentare gli IOPS per i dati letti di frequente NVMe :

- File system Multi-AZ 1 e Multi-AZ 2
- File system Single-AZ 1 creati dopo il 28 novembre 2022 con almeno il 2% della capacità di throughput GBps
- File system Single-AZ a 2 file con almeno il 6% GBps di capacità di throughput per coppia

> **Note**
>
> Per i file system di seconda generazione (Single-AZ 2 e Multi-AZ 2), l'utilizzo di una NVMe cache può far sì che il carico di lavoro raggiunga un throughput totale inferiore per carichi di lavoro di I/O ad alto throughput o di grandi dimensioni. Se hai un carico di lavoro vincolato al throughput, ti consigliamo di disabilitare la cache. NVMe Per ulteriori informazioni, consulta Gestione della cache NVMe.

Le tabelle seguenti mostrano la quantità di capacità di throughput che i file system possono scalare in base a fattori quali il numero di coppie ad alta disponibilità (HA) e la disponibilità. Regioni AWS

First-generation file systems

Queste specifiche prestazionali si applicano ai file system Single-AZ e Multi-AZ di prima generazione.

Velocità effettiva massima dello storage SSD per coppia HA per i file system di prima generazione

	Regione Stati Uniti orientali (Ohio), regione Stati Uniti orientali (Virginia settentrionale), regione Stati Uniti occidentali (Oregon) ed Europa (Irlanda)		Per tutti Regioni AWS gli altri paesi è disponibile FSx ONTAP	
	Velocità di lettura () MBps	Velocità effettiva di scrittura () MBps	Velocità effettiva di lettura () MBps	Velocità effettiva di scrittura () MBps
AZ singolo	4.096 1	1.000	2.048	750
Multi-AZ	4.096 1	1.800	2.048	1.300

> **Note**
>
> [1] Per fornire 4 volte la capacità GBps 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.

Second-generation file systems

Queste specifiche prestazionali si applicano ai file system Single-AZ e Multi-AZ di seconda generazione. In genere, i file system di seconda generazione sono in grado di fornire l'intera capacità di lettura fornita per l'intera capacità di lettura e fino a un terzo della capacità di throughput prevista per le scritture. L'eccezione è rappresentata dall' MB/s opzione 6.144, elencata in questa tabella.

Velocità effettiva massima dello storage SSD per coppia HA per file system di seconda generazione

	Produttività di lettura () MBps	Velocità effettiva di scrittura () MBps
AZ singolo	6.144 1	1.024 1
Multi-AZ	6.144	2.048

> **Note**
>
> [1] per coppia HA (fino a 12). Per ulteriori informazioni, consulta Gestione delle 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 fino ai seguenti livelli di velocità effettiva del disco e IOPS:

- Throughput del disco (MBps per TIB di storage): 768
- IOPS su disco (IOPs per TiB di storage): 3.072

> **Note**
>
> Quando si riduce la capacità di archiviazione SSD su un file system di seconda generazione, la maggior parte dei carichi di lavoro ha un impatto minimo sulle prestazioni. Tuttavia, i carichi di lavoro che richiedono molta scrittura potrebbero subire un temporaneo peggioramento delle prestazioni. Potrebbero inoltre verificarsi brevi I/O pause (fino a 60 secondi) quando l'accesso del client viene reindirizzato a nuovi dischi.
> Per ridurre al minimo l'impatto sulle prestazioni, assicurati che i carichi di lavoro continui non consumino costantemente più del 50% della CPU, del 50% della velocità del disco o del 50% di IOPS SSD prima di avviare un'operazione di riduzione dell'SSD. Per ulteriori informazioni sulla riduzione della capacità di archiviazione SSD, consulta. Quando ridurre la capacità di archiviazione SSD

Impatto della capacità di throughput sulle prestazioni

Ogni FSx file system Amazon 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 I/O prestazioni di 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 express (NVMe) in memoria non volatile per la memorizzazione nella cache dei dati su ciascun file server e a livelli più elevati di I/O prestazioni del 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 è in grado di 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

First-generation Single-AZ file system

Queste specifiche prestazionali si applicano ai file system Single-AZ di prima generazione 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 throughput () MBps	Capacità di trasmissione della rete () MBps		IOPS di rete	Caching in memoria (GB)	NVMe memorizzazione nella cache di lettura (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	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	–

FSxcapacità di throughput () MBps	Capacità di trasmissione della rete () MBps	IOPS di rete	Caching in memoria (GB)	NVMe memorizzazione nella cache di lettura (GB)	Velocità effettiva del disco () MBps	IOPS dell'unità SSD *
		di base				

> **Note**
>
> * Gli IOPS SSD vengono utilizzati solo quando si accede a dati che non sono memorizzati nella cache o nella cache in memoria del file server. NVMe

Queste specifiche prestazionali si applicano ai file system Single-AZ di prima generazione in tutti gli altri Regioni AWS paesi in cui è disponibile ONTAP. FSx

Specifiche prestazionali per i file system in tutti gli altri paesi in Regioni AWS cui FSx è disponibile ONTAP

FSx capacità di trasmissione () 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	16	128	600	6.000	18.750
256	300	1.250		32	256	600	12.000	18.750

FSx capacità di trasmissione () MBps	Capacità di trasmissione della rete () MBps		IOPS di rete	Caching in memoria (GB)	Velocità effettiva del disco () MBps		IOPS dell'unità SSD *	
			di valori base					
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 o nella cache in memoria del file server. NVMe

Second-generation Single-AZ file system

Queste specifiche prestazionali si applicano ai file system Single-AZ di seconda generazione.

Specifiche prestazionali per i file system Single-AZ di seconda generazione

FSx capacità di trasmissione () MBps	Capacità di trasmissione della rete () MBps		IOPS di rete	Caching in memoria (GB)	NVMe memorizzazione nella cache (GB)	Velocità effettiva del disco () MBps		IOPS dell'unità SSD *	
	Linea di base	Scoppio				Linea di base	Scoppio	Linea di base	Scoppio

FSx capacità di trasmissione () MBps	Capacità di trasmissione della rete () MBps		IOPS di rete	Caching in memoria (GB)	NVMe memorizzazione nella cache (GB)	Velocità effettiva del disco () MBps		IOPS dell'unità SSD *	
384**	781	6.250	Centinaia di migliaia di valori base	16	–	384	3.125	12.500	65.000
768**	1.563	6.250		32	–	768	3.125	25.000	65.000
1.536	3.125	6.250		64	–	1.536	3.125	50.000	65.000
3.072	6.250	–		128	–	3.072	–	100.000	–
6.144	12.500	–		256	1.900	6.144	–	200.000	–

> **Note**
>
> * Gli IOPS SSD vengono utilizzati solo quando si accede a dati che non sono memorizzati nella cache o nella cache in memoria del file server. NVMe
> ** I file system Single-AZ di seconda generazione supportano capacità di throughput 384 e 768, ma solo con una coppia HA. Per aggiungere coppie HA, il file system deve essere configurato con almeno 1.536 di capacità di throughput. MBps

First-generation Multi-AZ file system

Queste specifiche prestazionali si applicano ai file system Multi-AZ di prima generazione 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)

FSx capacità di throughput () MBps	Capacità di trasmissione della rete () MBps		IOPS di rete	Caching in memoria (GB)	NVMe memorizzazione nella cache (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 o nella cache in memoria del file server. NVMe

Queste specifiche prestazionali si applicano ai file system Multi-AZ di prima generazione in tutti gli altri Regioni AWS paesi in cui è disponibile ONTAP. FSx

Specifiche prestazionali per i file system in tutti gli altri paesi in Regioni AWS cui FSx è disponibile ONTAP

FSx capacità di trasmissione () MBps	Capacità di trasmissione della rete () MBps		IOPS di rete	Caching in memoria (GB)	NVMe memorizzazione nella cache (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 di 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 o nella cache in memoria del file server. NVMe

Second-generation Multi-AZ file systems

Queste specifiche prestazionali si applicano ai file system Multi-AZ di seconda generazione.

Specifiche prestazionali per i file system Multi-AZ di seconda generazione

FSx capacità di trasmissione () MBps	Capacità di trasmissione della rete () MBps		IOPS di rete	Caching in memoria (GB)	NVMe memorizzazione nella cache (GB)	Velocità effettiva del disco () MBps		IOPS dell'unità SSD *	
	Linea di base	Scoppio				Linea di base	Scoppio	Linea di base	Scoppio
384	781	6.250	Centinaia di migliaia di valori base	16	237	384	3.125	12.500	65.000
768	1.563	6.250		32	474	768	3.125	25.000	65.000
1.536	3.125	6.250		64	950	1.536	3.125	50.000	65.000
3.072	6.250	–		128	1.900	3.072	–	100.000	–
6.144	12.500	–		256	3.800	6.144	–	200.000	–

> **Note**
>
> * Gli IOPS SSD vengono utilizzati solo quando si accede a dati che non sono memorizzati nella cache o nella cache in memoria del file server. 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 di prima generazione configurato con 2 TiB di capacità di storage SSD e MBps 512 di capacità di throughput presenta i seguenti livelli di throughput:

- Throughput di rete: 625 linee di MBps base e 1.250 burst (vedere la tabella sulla capacità di throughput) MBps
- Throughput del disco: 512 linee di base e 600 burst. MBps MBps

Il carico di lavoro che accede al file system sarà quindi in grado di supportare fino a 625 velocità di MBps base e 1.250 di MBps burst per le operazioni sui file eseguite sui dati ad accesso attivo memorizzati nella cache e nella cache in memoria del file server. NVMe

Amministrazione delle risorse FSx ONTAP

Utilizzando l' Console di gestione AWS interfaccia a AWS CLI riga di comando e l'API e ONTAP, è possibile eseguire le seguenti azioni amministrative FSx per le risorse ONTAP:

- Creazione, elenco, aggiornamento ed eliminazione di file system, macchine virtuali di archiviazione (SVMs), 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 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

- Capacità di archiviazione del volume

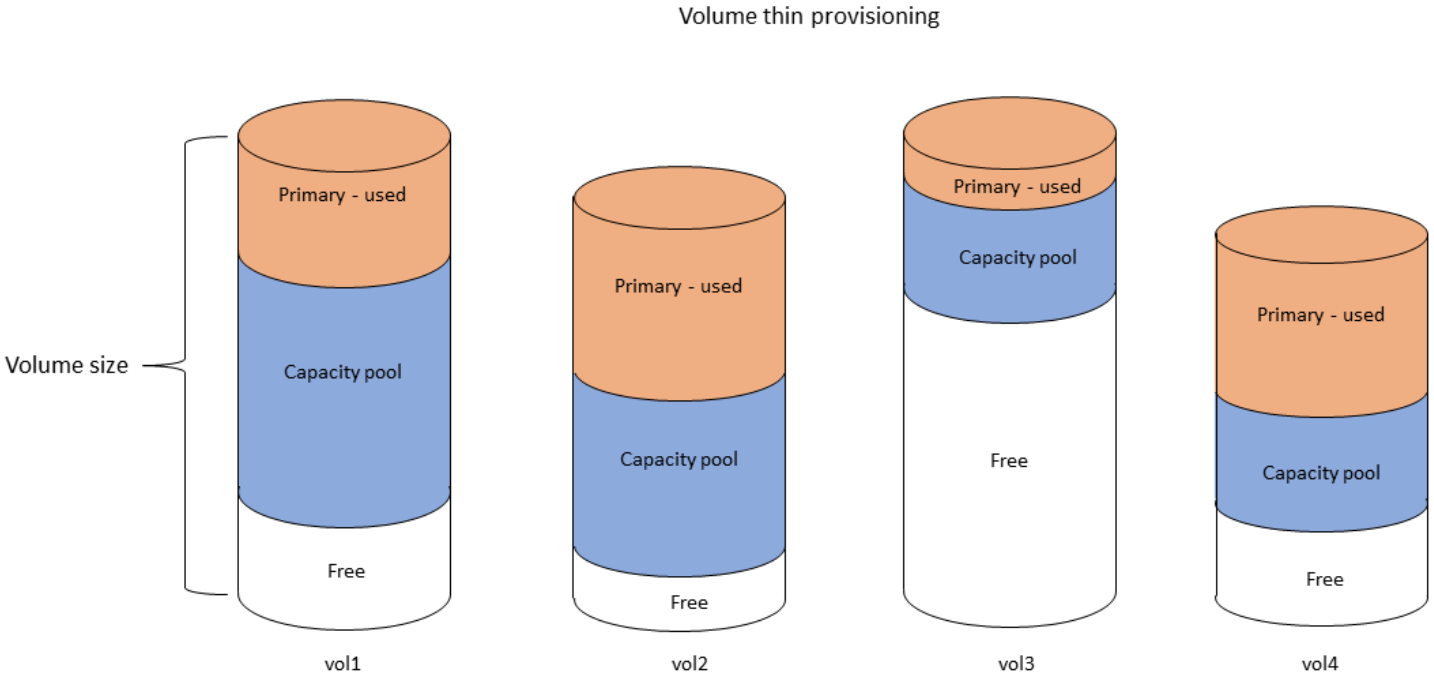
FSx per i livelli di storage ONTAP

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

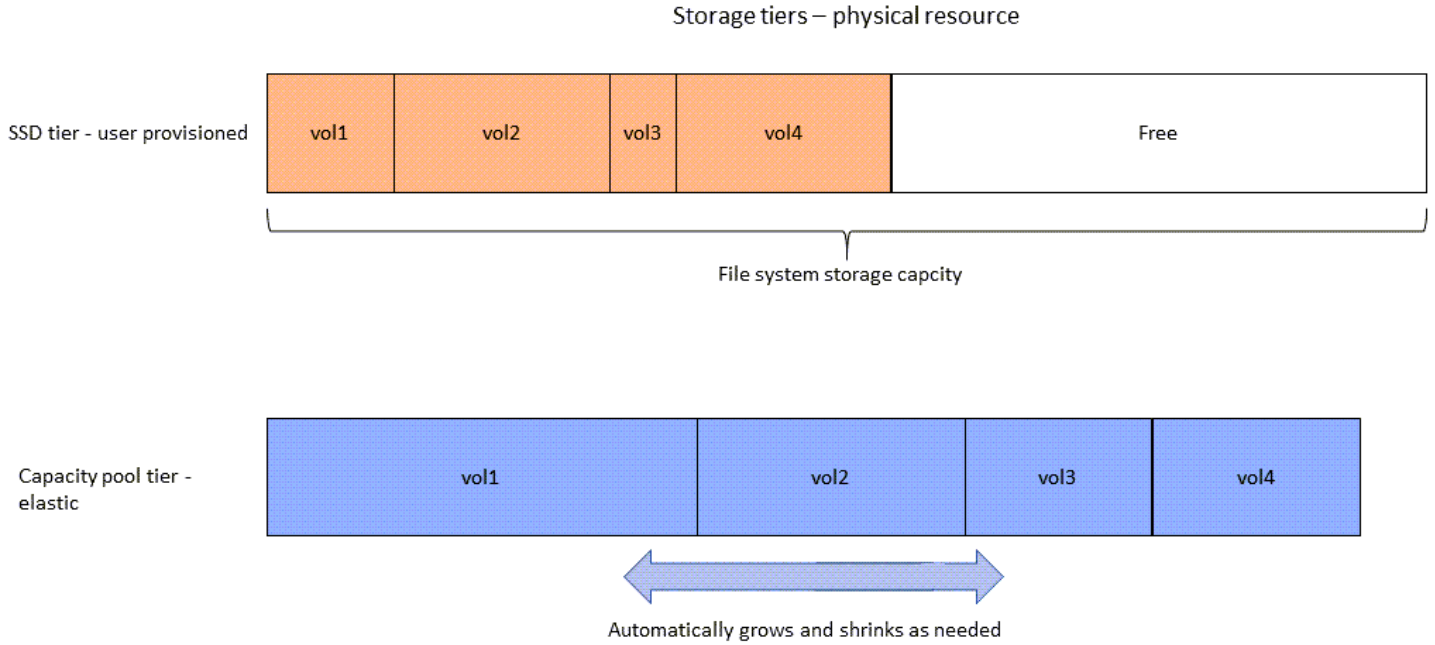
- Livello SSD: lo storage su unità a stato solido (SSD) ad alte prestazioni fornito dall'utente e progettato appositamente per la parte attiva del set di dati.
- Livello di pool di capacità: storage completamente elastico con scalabilità automatica fino a petabyte e ottimizzato in termini di costi per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

Un volume FSx for ONTAP è una risorsa virtuale che, analogamente alle cartelle, non consuma capacità di archiviazione. 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. FSx per ONTAP i volumi sono sottoposti a thin provisioning e lo storage del file system non è riservato in anticipo. Al contrario, 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 volumi di dati su più livelli.

Scelta della giusta quantità di storage SSD per file system

Quando scegli la quantità di capacità di archiviazione SSD per il file system FSx for ONTAP, devi 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 software NetApp 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 è vero indipendentemente dalla politica di suddivisione in più livelli del volume, con l'eccezione che i dati vengono scritti direttamente nello storage del pool di capacità quando vengono utilizzati SnapMirror su un volume configurato con una politica di suddivisione 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 volumi di 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 di seconda generazione, 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.

Efficienza dello storage

NetApp ONTAPoffre funzionalità di efficienza dello storage a livello di blocco a livello di volume che includono compressione, compattazione e deduplicazione. Queste funzionalità consentono di risparmiare fino al 65% in termini di capacità di storage per le condivisioni generiche di file, senza compromettere le prestazioni. È possibile abilitare l'efficienza dello storage in base al volume. Queste funzionalità riducono la quantità di capacità di archiviazione consumata dai dati, consentendoti di consumare meno spazio di archiviazione su SSD, pool di capacità e storage di backup. È possibile abilitare la compressione e la deduplicazione su ogni volume per i dati nell'archiviazione SSD. I risparmi di storage derivanti dalla compressione e dalla deduplicazione nello storage SSD vengono

preservati quando i dati vengono suddivisi in livelli di storage in base al pool di capacità. L'efficienza dello storage è sempre abilitata per i dati di backup, indipendentemente dalla configurazione dell'efficienza di archiviazione del file system.

La tabella seguente mostra alcuni esempi di risparmi tipici in termini di storage.

	Solo compressione	Solo deduplicazione	Compressione e deduplicazione
Condivisioni di file per uso generico	50%	30%	65%
Server e desktop virtuali	55%	70%	70%
Database	65-70%	0%	65-70%
Dati ingegneristici	55%	30%	75%
Dati geosismici	40%	3%	40%

Per la maggior parte dei carichi di lavoro, l'abilitazione della compressione e della deduplicazione non influirà negativamente sulle prestazioni del file system. Per la maggior parte dei carichi di lavoro, la compressione aumenta le prestazioni complessive. Per garantire letture e scritture rapide dalla cache RAM, FSx i file server di ONTAP sono dotati di livelli di larghezza di banda di rete sulle schede di interfaccia di rete front-end (NICs) superiori a quelli disponibili tra i file server e i dischi di archiviazione. Poiché la compressione dei dati riduce la quantità di dati inviati tra i file server e i dischi di archiviazione, per la maggior parte dei carichi di lavoro, si noterà un aumento della capacità di trasmissione complessiva del file system quando si utilizza la compressione dei dati. L'aumento della capacità di trasmissione correlata alla compressione dei dati verrà limitato una volta saturata la scheda NIC front-end del file system.

Amazon FSx for NetApp ONTAP supporta anche altre ONTAP funzionalità 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, vedereMonitoraggio del risparmio in termini di efficienza.

Calcolo dei risparmi in termini di efficienza dello storage

È possibile utilizzare i parametri del CloudWatch file system `LogicalDataStored` and `StorageUsed` 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, 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`

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 TiB) dei dati viene automaticamente trasferito al livello del pool di capacità e il restante 20% (20 TiB) 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 fornire 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 archiviazione del livello SSD. Per i file system Single-AZ di seconda generazione, 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 effettua FSx automaticamente il provisioning di 3 input/output operazioni SSD al secondo (IOPS) per il file system, fino a un massimo di 160.000 IOPS SSD per file system. Per i file system Single-AZ di seconda generazione, 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 for ONTAP, consulta. FSx Impatto della capacità di throughput sulle prestazioni

Argomenti

Aggiornamento dello storage SSD e degli IOPS del file system

Quando hai bisogno di spazio di archiviazione aggiuntivo per la parte attiva del tuo set di dati, puoi aumentare la capacità di archiviazione SSD del tuo file system Amazon FSx for NetApp ONTAP.

Per i file system di seconda generazione, puoi persino ridurre la capacità di archiviazione SSD per soddisfare le mutevoli esigenze di archiviazione del tuo carico di lavoro. Usa la FSx console Amazon, l' FSx API Amazon o AWS Command Line Interface (AWS CLI) per aumentare o diminuire la capacità di archiviazione SSD. Per ulteriori informazioni, consulta Aggiornamento della capacità di archiviazione e provisioning degli IOPS.

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 di seconda generazione, 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, vedere. Scelta della giusta quantità di storage SSD per file system

Aumento della capacità di archiviazione SSD

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

Dopo aver aumentato la capacità di storage, Amazon FSx esegue un processo di ottimizzazione dello storage in background per ribilanciare 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 FSx console Amazon e l'API. AWS CLI Per ulteriori informazioni, consulta Monitoraggio della capacità di storage e degli aggiornamenti IOPS.

Considerazioni sull'aumento della capacità di archiviazione SSD

Ecco alcuni elementi importanti da considerare per aumentare la capacità di archiviazione SSD e gli IOPS del file system:

- (Solo file system di prima generazione) 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 almeno del 10% dell'attuale capacità di archiviazione SSD del file system, fino alla capacità di archiviazione SSD massima per la configurazione del file system.
- Tempo tra un aumento e l'altro: dopo aver aumentato 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 ridimensiona FSx 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 puoi fornire per il tuo file system for ONTAP, consulta. FSx 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 ridurre la capacità di archiviazione SSD

Potresti voler ridurre la capacità di archiviazione SSD del tuo file system FSx for ONTAP di seconda generazione in scenari come i seguenti:

- Dopo aver completato carichi di lavoro basati su progetti in cui non è più necessario lo storage ad alte prestazioni
- Dopo aver completato migrazioni di dati su larga scala in cui è stata utilizzata una capacità aggiuntiva temporanea per accelerare l'ingestione dei dati

Riduzione della capacità di archiviazione SSD

Quando riduci la capacità di archiviazione SSD del tuo file system, Amazon FSx collega un nuovo set di dischi più piccolo (aggregato) a ciascuna delle coppie HA del tuo file system. Amazon esegue FSx quindi un processo di ottimizzazione dello storage in background per spostare i dati in base al volume dai vecchi dischi ai nuovi dischi. Dopo lo spostamento dei dati in ogni volume, Amazon FSx reindirizza l'accesso dei client ai volumi sui nuovi dischi. Amazon rimuove FSx quindi i vecchi dischi dal tuo file system.

Ti verrà addebitata la dimensione esistente e quella appena richiesta del livello SSD durante l'operazione di riduzione dell'unità SSD. Ad esempio, quando riduci la capacità di archiviazione SSD da 10 tebibyte (TiB) a 5 TiB, ti verranno fatturati 15 TiB durante l'operazione di riduzione dell'SSD e 5 TiB al termine dell'operazione di riduzione dell'SSD. Per ulteriori informazioni sulla fatturazione, vedere. AWS report di fatturazione e utilizzo FSx per ONTAP

La riduzione della capacità di archiviazione SSD può richiedere da alcune ore a qualche settimana a seconda di fattori quali la quantità di dati archiviati nel file system, la quantità di nuove scritture in rete trasferite sul file system durante l'operazione di riduzione e la quantità di risorse di rete e disco disponibili sul file system.

Durante l'operazione di riduzione, i dati rimangono disponibili per la lettura e la scrittura. La maggior parte dei carichi di lavoro ha un impatto minimo sulle prestazioni, anche se i carichi di lavoro che richiedono molta scrittura potrebbero subire un temporaneo peggioramento delle prestazioni. Potrebbero verificarsi brevi I/O pause (fino a 60 secondi) quando l'accesso del client viene reindirizzato ai nuovi dischi per ogni volume.

Per ridurre al minimo l'impatto sulle prestazioni, prima di avviare un'operazione di riduzione dell'SSD, è necessario mantenere un margine di manovra adeguato nel file system, assicurandosi che i carichi di lavoro continui non consumino costantemente più del 50% della CPU, del 50% della velocità del disco o del 50% di IOPS SSD. Puoi monitorare questi parametri di utilizzo nella scheda Monitoraggio e prestazioni del tuo file system nella console Amazon FSx .

> **Note**
>
> Se il livello di storage SSD supera l'80% di utilizzo durante l'operazione di riduzione, Amazon FSx sospende l'operazione e la riprende automaticamente dopo che l'utilizzo scende al di sotto dell'80%. Per ridurre l'utilizzo degli SSD sui nuovi dischi, puoi suddividere i dati in base al pool di capacità o eliminare i dati dai volumi per i quali l'accesso del client è stato reindirizzato correttamente al nuovo set di dischi.

Se è necessaria una capacità SSD aggiuntiva durante un'operazione di riduzione, è possibile inviare una richiesta per aumentare la capacità SSD `update-file-system`richiamando l'operazione API AWS CLI o l'operazione UpdateFileSystemAPI equivalente e fornendo un nuovo valore di destinazione. Amazon FSx dà priorità al completamento della richiesta di aumento dell'SSD, in modo che la nuova capacità SSD sia disponibile per l'uso entro pochi minuti prima di riprendere l'operazione di riduzione dell'SSD.

Considerazioni sulla riduzione della capacità di archiviazione SSD

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

- Aumento della capacità di archiviazione durante un'operazione di riduzione: è possibile aumentare la capacità di archiviazione SSD del file system anche mentre è in corso un'operazione di riduzione. Questa flessibilità consente di garantire prestazioni e disponibilità nel caso in cui uno degli aggregati si riempia durante l'operazione di riduzione. Se aumenti la capacità SSD portandola a una dimensione inferiore alla capacità originale, Amazon regola FSx solo le dimensioni dell'aggregato appena richiesto (di destinazione). Tuttavia, se aumenti la capacità SSD portandola a una dimensione superiore a quella originale, Amazon FSx aumenta le dimensioni di entrambi gli aggregati in modo che corrispondano al nuovo valore target. Ad esempio, se si riduce la capacità di storage da 10.000 GiB a 5.000 GiB e quindi si richiede un aumento a 7.000 GiB, solo l'aggregato di destinazione viene aumentato a 7.000 GiB, con una capacità di archiviazione SSD finale di 7.000 GiB per il file system. Ma se si richiede un aumento a 12.000 GiB, entrambi gli aggregati vengono

aumentati a 12.000 GiB. Suggeriamo una pianificazione attenta per evitare uno scenario in cui sia necessario aumentare la capacità SSD a una dimensione uguale o superiore alla capacità SSD originale.

- Sospensione della riduzione dell'SSD: Amazon FSx sospende un'operazione di riduzione dell'SSD se si supera l'80% di utilizzo sul nuovo aggregato e riprende automaticamente l'operazione di riduzione quando l'utilizzo scende al di sotto dell'80%.
- (Solo file system Single-AZ di seconda generazione) Diffusione della capacità di storage: la nuova capacità di storage o IOPS SSD selezionata per il file system viene distribuita in modo uniforme su ciascuno degli aggregati del file system.
- Applicazione di patch durante la riduzione della capacità di archiviazione: Amazon FSx interrompe lo spostamento dei dati per un volume se al file system viene applicata una patch durante un'operazione di riduzione dell'SSD. Di conseguenza, potresti perdere i progressi dell'operazione di riduzione dell'SSD se viene applicata una patch durante l'operazione. Amazon FSx si riavvia automaticamente al `vol move` termine dell'operazione di patch.
- Modalità IOPS fornite: per una modifica IOPS assegnata, è necessario specificare una delle due modalità IOPS:
  - Modalità automatica: Amazon ridimensiona FSx 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. Quando si riduce la capacità dell'SSD, gli IOPS SSD automatici verranno ridimensionati proporzionalmente.

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

  - Modalità fornita dall'utente: è necessario fornire un valore IOPS uguale o superiore agli IOPS attualmente assegnati. Quando si riduce la capacità SSD, è possibile mantenere IOPS SSD aggiuntivi forniti dall'utente, a condizione che non superino il numero massimo di IOPS SSD supportato dall'aggregato più piccolo (50 IOPS per GB di capacità SSD richiesta). Se gli IOPS assegnati sono superiori al massimo supportato dall'aggregato più piccolo, riduci gli IOPS prima di ridurre la capacità dell'SSD.
- Tipi di volume non supportati: Amazon FSx non supporta la riduzione della capacità di storage su file system con SnapLock volumi FlexClones, volumi offline o volumi di protezione dei dati (DP) che non contengono istantanee.

- Operazioni non supportate durante Shrink: non è possibile utilizzare volumi offline, spostare volumi FlexClones, creare o modificare le impostazioni di efficienza di archiviazione SnapLock dei volumi durante l'operazione di riduzione.

Limitazioni per la riduzione della capacità di archiviazione SSD

Le seguenti limitazioni si applicano alla riduzione della capacità di archiviazione SSD del file system:

- (Solo file system di seconda generazione) Riduzione della capacità di archiviazione: è possibile ridurre la capacità di archiviazione solo sui file system di seconda generazione.
- Riduzione minima della capacità di archiviazione: ogni riduzione della capacità di archiviazione SSD deve essere pari almeno al 9% dell'attuale capacità di archiviazione SSD del file system. La riduzione dovrebbe inoltre garantire che la capacità SSD risultante del file system non superi l'80% di utilizzo dopo l'operazione di riduzione. Ad esempio, se il file system ha 10.000 GiB di capacità di storage e 5.000 GiB di storage utilizzati, è possibile ridurre la capacità di archiviazione fino a 6.251 GiB in modo che l'utilizzo dell'SSD rimanga inferiore all'80%. È possibile ridurre la capacità di archiviazione SSD fino alla dimensione minima supportata di 1.024 GiB per coppia HA.
- Per ridurre la capacità di archiviazione SSD sui file system che contengono uno o più volumi con più di 50 TiB di dati nel livello SSD, è necessario fornire almeno MB/s 1.536 di capacità di throughput per coppia HA. Se un volume contiene più di 100 TiB di dati nel livello SSD, è necessario fornire almeno 3.072 di capacità MB/s di throughput per coppia HA. Per i volumi con più di 200 TiB di dati nel livello SSD, è necessario fornire 6.144 di capacità MB/s di throughput per coppia HA.
- Intervallo tra gli aggiornamenti: 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.
- È possibile aumentare ma non diminuire la capacità di throughput del file system
- Non è possibile aggiungere coppie HA al file system
- Non è possibile ripristinare uno stato precedente (utilizzo`volume snapshot restore`) di un volume mentre i dati di quel volume vengono spostati nel nuovo aggregato. Tuttavia, puoi eseguirlo `volume snapshot restore` su altri volumi che attualmente non vengono spostati.

Creazione di un allarme sull'utilizzo della capacità di archiviazione per il 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 di utilizzo della capacità di archiviazione 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. Apri la console all'indirizzo. CloudWatch https://console.aws.amazon.com/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, selezionate 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 Seleziona metrica. 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. Scegli Next (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.

Aggiornamento della capacità di archiviazione e provisioning degli IOPS

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

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

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione a sinistra, scegli File system. Nell'elenco dei file system, seleziona il file system ONTAP FSx per cui desideri aggiornare la capacità di archiviazione SSD e gli IOPS SSD.
3. Scegli Azioni > Aggiorna la capacità di archiviazione. Oppure, nella sezione Riepilogo, scegli Aggiorna accanto al valore della capacità di archiviazione SSD del file system.
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 i tuoi IOPS 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 for ONTAP, FSx consulta. Impatto della capacità di throughput sulle prestazioni

8. Scegliere 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 di seconda generazione, viene visualizzato anche il valore. per-HA-pair

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

Per aumentare la capacità di archiviazione SSD e gli IOPS assegnati per un file system FSx for ONTAP, usa il comando o l'azione API equivalente. AWS CLI update-file-systemUpdateFileSystem 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 IOPs valore deve essere maggiore o uguale a tre volte l'attuale capacità di archiviazione SSD.
  - Se desideri che Amazon aumenti automaticamente FSx gli IOPS degli SSD, usa `Mode=AUTOMATIC` e non usa il `Iops` parametro. 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 puoi fornire per il tuo file system for ONTAP, consulta. FSx 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 AdministrativeActionAmazon FSx for NetApp ONTAP API Reference.

Per ridurre la capacità di archiviazione SSD per un file system (console)

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

2. Nel pannello di navigazione a sinistra, scegli File system. Nell'elenco dei file system, seleziona il file system ONTAP FSx per cui desideri aggiornare la capacità di archiviazione SSD e gli IOPS SSD.
3. Scegli Azioni > Aggiorna il file system > Aggiorna la capacità di archiviazione SSD/IOPS. Oppure, nella sezione Riepilogo, scegli Aggiorna accanto al valore della capacità di archiviazione SSD del file system.
4. Per ridurre la capacità di archiviazione SSD, per Tipo di azione, scegli Diminuisci.
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, effettuate una delle seguenti operazioni.
   - Per Percentuale, inserite il valore di riduzione% desiderato. Questo valore deve essere inferiore di almeno il 9% rispetto al valore corrente.
   - Per Absolute, immettere il valore della capacità di archiviazione desiderata in GiB.
7. Scegliere 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 di seconda generazione, viene visualizzato anche il valore. per-HA-pair

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

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

1. Per ridurre la capacità dell'SSD, usa il seguente comando:

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 4096
```

Se utilizzi la modalità IOPS fornita dall'utente e desideri mantenere il livello IOPS corrente, includi il parametro: `DiskIopsConfiguration`

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 4096 \
--ontap-configuration 'DiskIopsConfiguration={Iops=15000,Mode=USER_PROVISIONED}'
```

2. Per monitorare lo stato di avanzamento dell'operazione di riduzione, usa il comando: describe-file-systems

```
aws fsx describe-file-systems --file-system-id fs-0123456789abcdef0
```

Il comando restituisce informazioni sull'operazione di riduzione nella `AdministrativeActions` sezione. Esempio:

```
{
    "FileSystem": {
        "StorageCapacity": 4096,
        "StorageType": "SSD",
        "AdministrativeActions": [
            {
                "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                "Message": "Moving data for [vol1 vol2]. 2 volume(s) remaining.
 https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/troubleshooting.html",
                "ProgressPercent": 4,
                "RequestTime": 1748981251.591,
                "Status": "IN_PROGRESS",
                "TargetFileSystemValues": {
                    "StorageCapacity": 4096
                }
            }
        ]
    }
}
```

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

Per ulteriori informazioni, consulta `AdministrativeAction`Amazon FSx for NetApp ONTAP API Reference.

Aggiornamento dinamico della capacità di archiviazione

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:

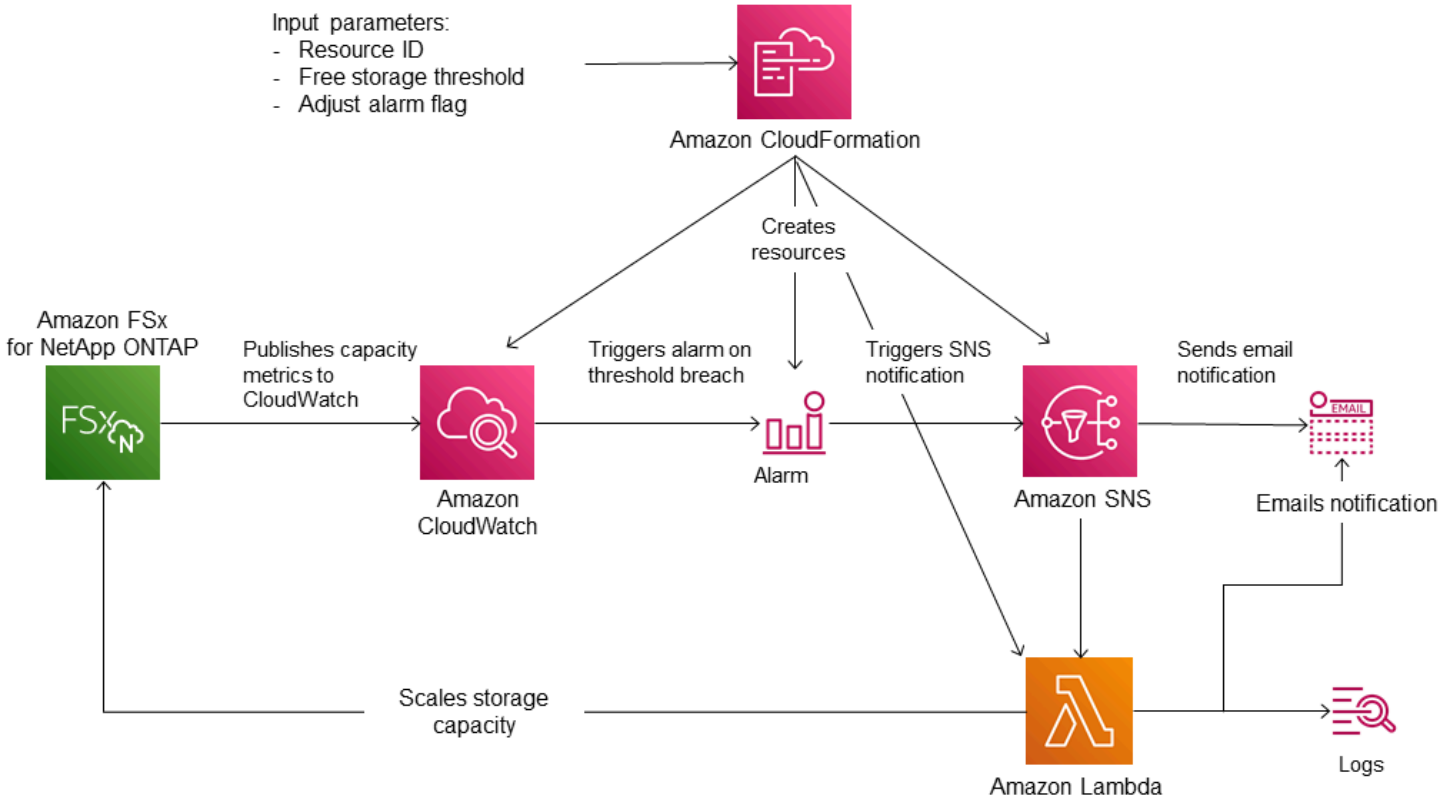
- Il tuo FSx ID del file system for ONTAP.
- La soglia di capacità di archiviazione SSD utilizzata (valore numerico). Questa è la percentuale alla quale verrà CloudWatch attivato l'allarme.
- La percentuale con cui aumentare la capacità di archiviazione (%).
- L'indirizzo e-mail utilizzato per ricevere le notifiche di ridimensionamento.

Argomenti

- Panoramica dell’architettura
- CloudFormation modello
- Implementazione automatizzata con CloudFormation

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 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.

CloudFormation modello

Questa soluzione consente CloudFormation di automatizzare l'implementazione dei componenti utilizzati per aumentare automaticamente la capacità di archiviazione di un file system FSx for ONTAP. Per utilizzare questa soluzione, scarica il modello. FSxOntapDynamicStorageScaling 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.

B massimo FSx SizeinGi

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

Implementazione automatizzata con CloudFormation

La procedura seguente configura e implementa uno CloudFormation stack per aumentare automaticamente la capacità di archiviazione 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 FSx file system Amazon in esecuzione su Amazon Virtual Private Cloud (Amazon VPC) nel tuo. Account AWS Per ulteriori informazioni sulla creazione di FSx risorse Amazon, consultaGuida introduttiva ad Amazon FSx for NetApp ONTAP.

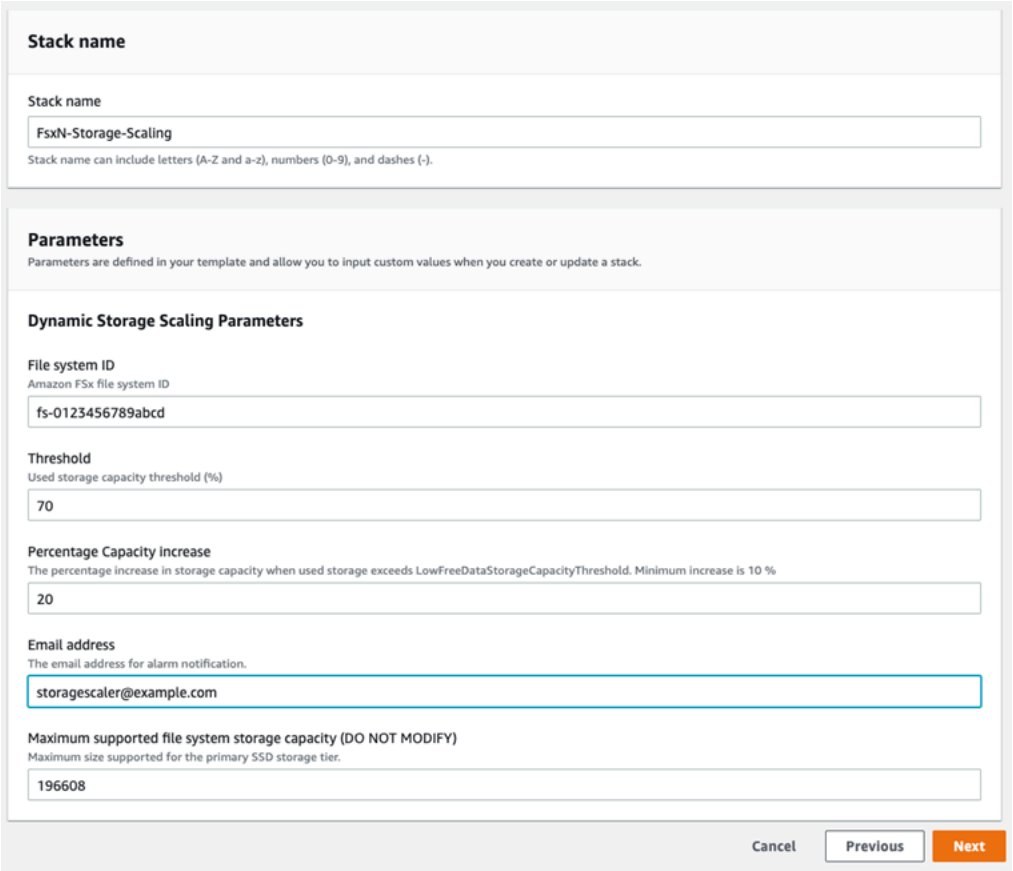
Per lanciare lo stack di soluzioni per l'aumento automatico della capacità di archiviazione

1. Eseguire il download del modello FSxOntapDynamicStorageScaling CloudFormation .

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

2. Dalla 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 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.

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 FSx console Amazon. Il grafico della capacità di archiviazione primaria disponibile mostra la quantità di capacità di archiviazione basata su 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 Console di gestione AWS, utilizzando la procedura seguente.

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

1. Apri la FSx console Amazon 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.

Monitoraggio del risparmio in termini di efficienza

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

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

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

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli il file system ONTAP FSx per cui desideri visualizzare il risparmio in termini di efficienza dello storage dall'elenco dei file system.
3. Scegli 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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

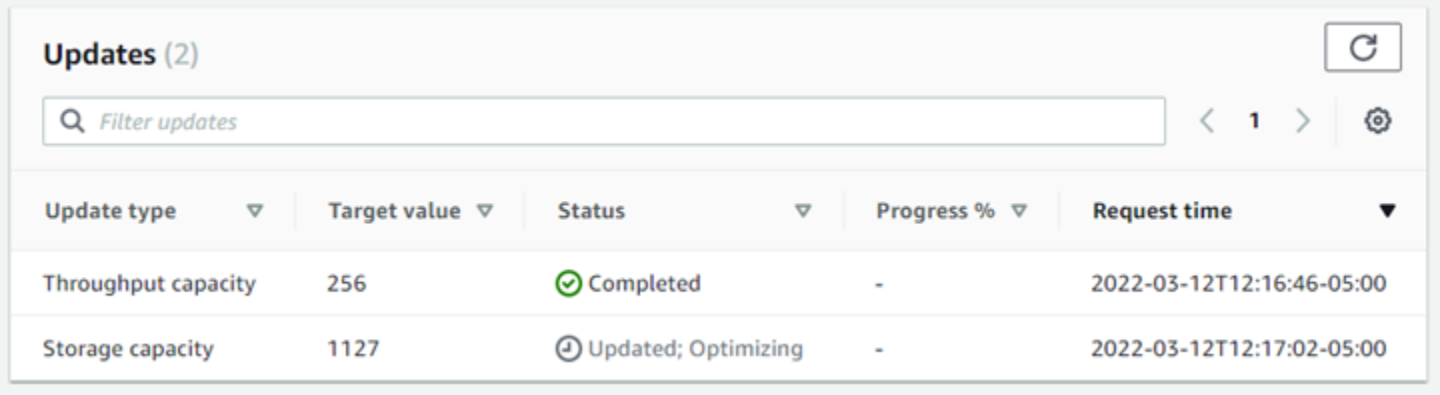
Snapshot Volume Storage Efficiency:            8.81:1
FlexClone Volume Storage Efficiency:           1.00:1
Number of Efficiency Disabled Volumes:         1
```

Monitoraggio della capacità di storage e degli aggiornamenti IOPS

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

Per monitorare lo storage e gli aggiornamenti IOPS (console)

Nella scheda Aggiornamenti della pagina dei dettagli del file system del file system FSx for ONTAP, puoi 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 iniziato a elaborarla.
- In corso: Amazon FSx sta elaborando la richiesta di aggiornamento.
- Aggiornato; ottimizzazione: Amazon FSx ha aumentato la capacità di archiviazione 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.
- Non riuscito: 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 l'aumento e la riduzione 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_OPTIMIZATIO`Nazione. Quando si riduce la capacità di archiviazione SSD di un file system, viene generata una sola `AdministrativeActions` azione: un'`FILE_SYSTEM_UPDATE`azione.

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"
    }
]
```

Quando si riduce la capacità dell'SSD, l'`FILE_SYSTEM_UPDATE`azione include una `Message` proprietà che fornisce informazioni su quali volumi vengono attualmente spostati e quanti volumi rimangono. Esempio:

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "Message": "Moving data for [vol1 vol2]. 2 volume(s) remaining. https://
docs.aws.amazon.com/fsx/latest/ONTAPGuide/troubleshooting.html",
        "ProgressPercent": 8,
        "RequestTime": 1748981251.591,
```

```
        "Status": "IN_PROGRESS",
        "TargetFileSystemValues": {
            "StorageCapacity": 4096,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "AUTOMATIC",
                    "Iops": 12288
                }
            }
        }
    }
]
```

Se l'operazione di riduzione dell'SSD viene messa in pausa perché l'aggregato di destinazione ha superato l'80% di utilizzo, lo stato cambierà e verrà visualizzato un messaggio appropriato: `PAUSED`

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "Message": "Your file system has insufficient free space in its SSD tier.
 Please free up space or increase your file system's storage capacity.",
        "ProgressPercent": 8,
        "RequestTime": 1748981251.591,
        "Status": "PAUSED",
        "TargetFileSystemValues": {
            "StorageCapacity": 4096,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "AUTOMATIC",
                    "Iops": 12288
                }
            }
        }
    }
]
```

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"
        }
    }
]
```

Capacità di archiviazione del volume

FSx i volumi for ONTAP sono risorse virtuali utilizzate per raggruppare i dati, determinare la modalità di archiviazione dei dati e determinare il tipo di accesso ai dati. I volumi, come le cartelle, non consumano di per sé la capacità di archiviazione 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. Puoi monitorare e gestire la capacità di archiviazione dei tuoi volumi FSx for ONTAP utilizzando l'API Console di gestione AWS, AWS CLI and e l'ONTAP CLI.

Argomenti

- Suddivisione dei volumi di dati su più livelli
- Istantanee e capacità di archiviazione di volumi
- Capacità dei file di volume
- Gestione dell'efficienza dello storage
- Abilitazione del dimensionamento automatico
- Attivazione della modalità di scrittura su cloud
- Aggiornamento della capacità di archiviazione
- Aggiornamento di una politica di suddivisione in più livelli

- Aggiornamento dei giorni minimi di raffreddamento
- Aggiornamento della policy di recupero nel cloud di un volume
- Aggiornamento del numero massimo di file su un volume
- Monitoraggio della capacità di archiviazione del volume
- Monitoraggio della capacità dei file di un volume

Suddivisione dei volumi di 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.

> **Note**
>
> FSx for ONTAP supporta il tiering dei dati nel pool di capacità su tutti i SnapLock volumi, indipendentemente dal tipo. SnapLock Per ulteriori informazioni, consulta Funzionamento di SnapLock.

Politiche di suddivisione in livelli di volume

È possibile determinare come utilizzare i livelli di storage del file system FSx for ONTAP scegliendo la politica di suddivisione in più livelli 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 FSx console Amazon AWS CLI, l'API o utilizzando strumenti di NetApp 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 FSx console Amazon.
- 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 FSx API Amazon o la CLI NetApp ONTAP.
- Tutti: questa policy contrassegna tutti i dati degli utenti e i dati delle istantanee come inattivi 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. Se la politica All viene applicata a un volume che contiene già dati, i dati esistenti vengono trasferiti su più livelli dall'SSD al pool di capacità. 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 (incluse le istantanee) nel volume che si trovava nello storage con pool di capacità vengono spostati nello storage SSD tramite un processo in background. Questa migrazione dei dati avviene solo quando l'utilizzo dell'SSD è inferiore al 90% e la policy di recupero dal cloud è impostata su o. `promote` `on-read` Questo

processo in background può essere accelerato leggendo intenzionalmente i dati. Per ulteriori informazioni, consulta Politiche di recupero dal cloud.

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

Come procedura ottimale, durante la migrazione dei dati che si prevede di archiviare a lungo termine in un pool di capacità di storage, si consiglia di utilizzare la politica di suddivisione automatica su più livelli 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. ONTAPesegue periodicamente la deduplicazione post-elaborazione dei dati archiviati nel livello di storage SSD, regolando automaticamente la frequenza in base alla velocità di variazione dei dati nel volume: velocità più elevate attivano i processi di deduplicazione post-elaborazione con maggiore frequenza.

Per impostazione predefinita, la compressione post-elaborazione è disabilitata a ONTAP causa dell'impatto sulle prestazioni che può avere sui carichi di lavoro in corso sul file system. È necessario valutare l'impatto sulle prestazioni del carico di lavoro prima di abilitare la compressione post-elaborazione. Per abilitare la compressione post-elaborazione, assumi il livello di privilegio di diagnostica nella ONTAP CLI ed esegui il comando seguente:

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -is-enabled true
```

ONTAPesegue la compressione post-elaborazione per i dati conservati sullo storage SSD per un minimo di 14 giorni. Per i carichi di lavoro in cui è improbabile l'accesso ai dati dopo un periodo più breve, è possibile modificare le impostazioni di compressione post-elaborazione per eseguire la compressione post-elaborazione prima. Ad esempio, per applicare i risparmi di compressione post-elaborazione ai dati a cui non si accede da 5 giorni, esegui il seguente comando ONTAP CLI:

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-name -threshold-days 5 -threshold-days-min 2 -threshold-days-max 14
```

Per ulteriori informazioni sul comando, vedere Volume Efficiency Modify inactive-data-compression

Conservando i dati su SSD, massimizzi la velocità di trasferimento dei backup di volume che crei, poiché le velocità di trasferimento dei dati sono più elevate per l'archiviazione SSD.

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. Aggiornamento 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. Aggiornamento della policy 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 di seconda generazione, questo consiglio 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 archiviazione 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 dati suddivisi 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 archiviazione 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 Protezione dei dati con istantanee.

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 il nome del file, l'ora dell'ultimo accesso, le autorizzazioni, le 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. Monitoraggio 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, consulta. Aggiornamento del numero massimo di file su un volume

Gestione dell'efficienza dello storage

Abilitando l'efficienza dello storage sui volumi FSx for ONTAP, è possibile ottimizzare l'utilizzo dello storage, ridurre i costi di storage e migliorare le prestazioni complessive del file system.

> **Note**
>
> Ti consigliamo di abilitare l'efficienza dello storage utilizzando la FSx console Amazon, l'API o di AWS CLI assicurarti che le impostazioni di efficienza di storage ottimali vengano applicate ai tuoi volumi.

ONTAPorganizza i file in 4 blocchi di dati kibibyte (KiB). L'efficienza dello storage avviene a livello di blocco di dati anziché a livello di singoli file. Quando l'efficienza dello storage è abilitata, ONTAP

utilizza una combinazione di tecniche di riduzione dei dati per eliminare i dati duplicati, comprimere le dimensioni dei dati e riorganizzare il layout dei dati per un utilizzo ottimale del disco.

Le efficienze di storage vengono applicate in due modi. Vengono applicate ai dati in linea (prima che i dati vengano scritti su disco, in memoria) per offrire risparmi di archiviazione immediati. Vengono inoltre applicati ai dati in background (dopo la scrittura su disco) nel livello di storage SSD attraverso processi periodici di efficienza per ottimizzare l'utilizzo dello storage nel tempo. Le efficienze dello storage in background non si ripercuotono sui dati dopo che sono stati distribuiti su più livelli al pool di capacità. Tuttavia, se i dati hanno ottenuto risparmi di storage mentre erano in SSD, tali risparmi vengono preservati quando i dati vengono suddivisi in livelli per il pool di capacità.

> **Note**
>
> ONTAPnon supporta l'attivazione di efficienze di storage sui volumi di protezione dei dati (DP). Tuttavia, i risparmi di storage ottenuti nel volume di lettura e scrittura (RW) di origine vengono preservati quando i dati vengono replicati nel volume DP di destinazione.

Compressione dei blocchi di dati

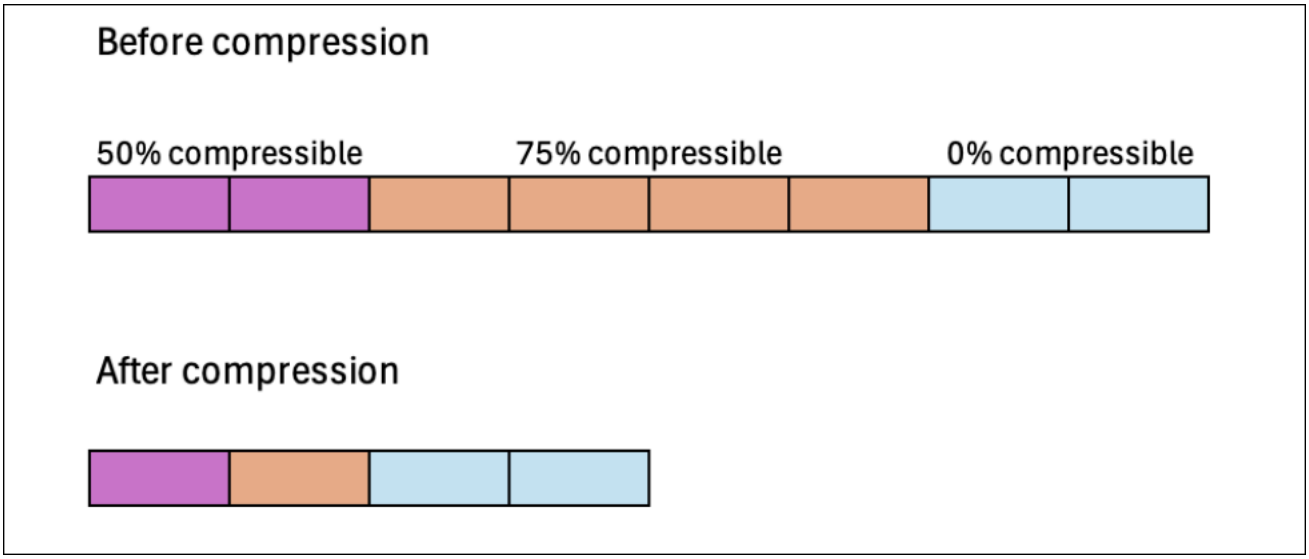
I gruppi di compressione sono raggruppamenti logici di dati che vengono gestiti e compressi insieme come un unico blocco. ONTAPcomprime automaticamente i blocchi di dati in gruppi di compressione, riducendo così lo spazio occupato su disco. Per ottimizzare le prestazioni e l'utilizzo dello storage, ONTAP offre un approccio bilanciato alla gestione dei dati regolando il grado di compressione applicato ai dati in base ai modelli di accesso.

Per impostazione predefinita, i dati vengono compressi in linea utilizzando gruppi di compressione da 8 KB per garantire prestazioni ottimali durante la scrittura dei dati su un volume. Facoltativamente, puoi applicare una compressione più intensa ai dati abilitando la compressione inattiva dei dati su un volume per comprimere ulteriormente i dati in SSD. La compressione inattiva dei dati utilizza gruppi di compressione da 32 KB su dati freddi per ulteriori risparmi di archiviazione. Per ulteriori informazioni, vedere il `volume efficiency inactive-data-compression modify`comando in. NetApp ONTAP Documentation Center

> **Note**
>
> La compressione inattiva dei dati consuma ulteriori IOPS della CPU e del disco e può essere un'attività che richiede molte risorse. Si consiglia di valutare l'impatto sulle prestazioni

dell'esecuzione della compressione inattiva dei dati sul carico di lavoro prima di abilitare questa funzionalità.

L'immagine seguente illustra i risparmi di storage che è possibile ottenere comprimendo i blocchi di dati.



Deduplicazione dei blocchi di dati

ONTAPrileva ed elimina i blocchi di dati duplicati per ridurre le ridondanze nei dati. I blocchi duplicati vengono sostituiti con riferimenti a blocchi unici condivisi.

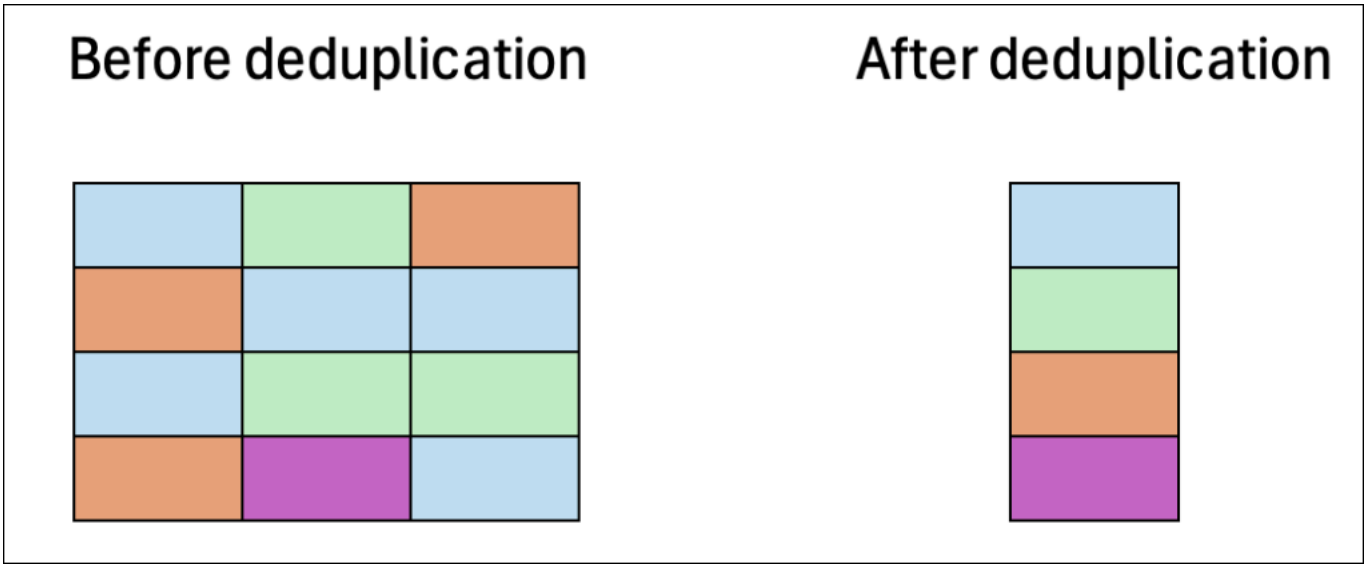
Per impostazione predefinita, i dati vengono deduplicati in linea per ridurre l'ingombro dello storage prima che i dati vengano scritti su disco. ONTAPesegue inoltre uno scanner di deduplicazione in background a intervalli specifici per identificare ed eliminare i dati duplicati dopo la scrittura su disco. Durante queste scansioni pianificate, ONTAP elabora un registro delle modifiche per identificare i blocchi di dati nuovi o modificati dall'ultima scansione che non sono ancora stati deduplicati. Quando vengono trovati dei duplicati, ONTAP aggiorna i metadati in modo che rimandino a una singola copia dei blocchi duplicati e contrassegna i blocchi ridondanti come spazio libero pronto per essere recuperato.

Note

ONTAPapplica la deduplicazione a 4 KB di scritture in entrata alla volta, quindi è possibile ottenere minori risparmi sulla deduplicazione quando si eseguono carichi di lavoro con scritture di dimensioni inferiori a 4 KB.

FSx for ONTAP non supporta la deduplicazione tra volumi.

L'immagine seguente illustra i risparmi di storage che è possibile ottenere con la deduplicazione.



Compattazione dei blocchi di dati

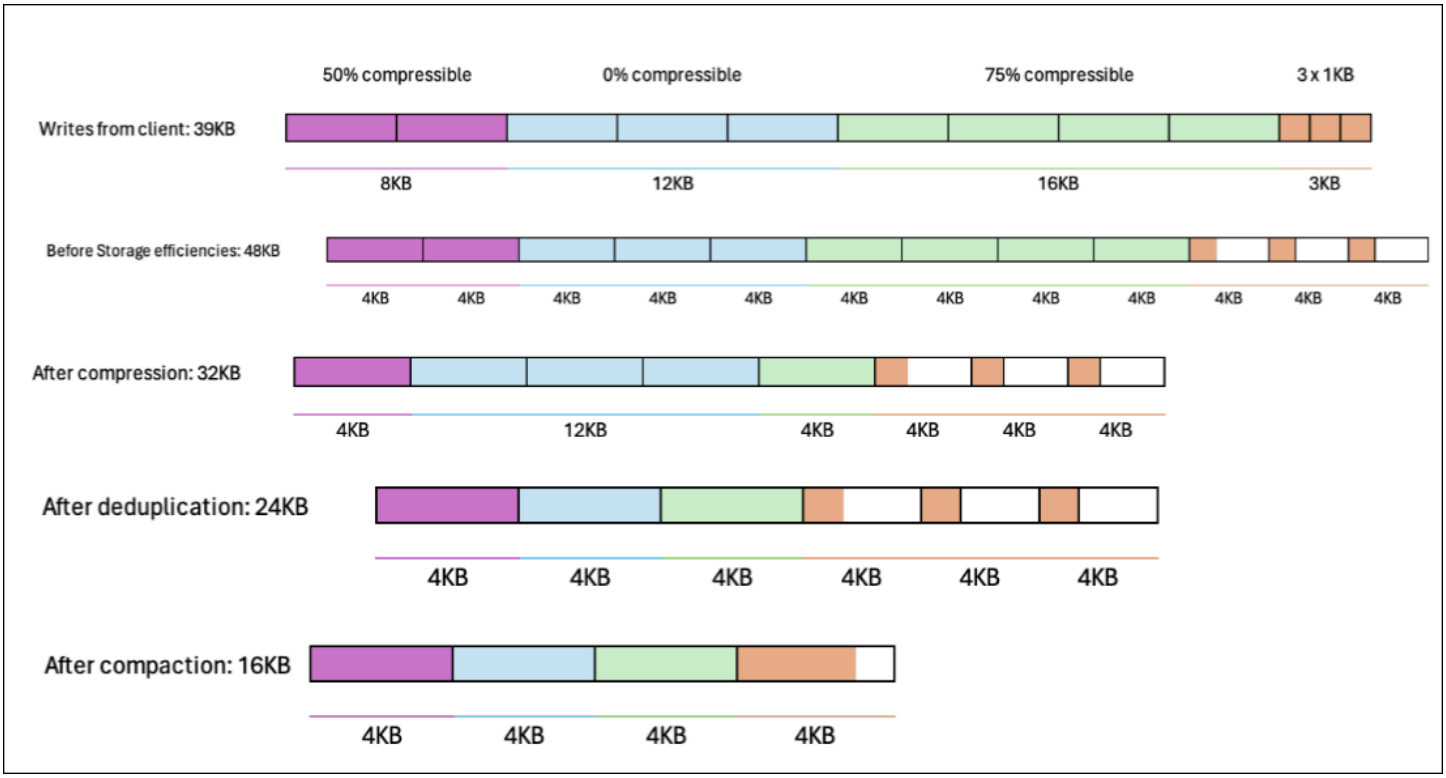
ONTAPconsolida i blocchi di dati parzialmente riempiti che pesano meno di 4 KB ciascuno in un blocco da 4 KB utilizzato in modo più efficiente.

Per impostazione predefinita, i dati vengono compattati in linea per ottimizzare il layout dei dati durante la scrittura su disco per ridurre al minimo il sovraccarico di archiviazione, ridurre la frammentazione e migliorare le prestazioni di lettura.

L'immagine seguente illustra i risparmi di storage che è possibile ottenere con la compattazione.

Esempio: efficienze di storage

L'immagine seguente illustra come le efficienze di storage vengono applicate ai dati.



Abilitazione del dimensionamento automatico

Dimensionamento automatico del volume in modo che il volume raggiunga automaticamente 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 FSx per ONTAP) utilizzando il comando `volume autosize`ONTAP CLI.

Per abilitare il dimensionamento automatico dei volumi (ONTAP CLI)

1. Per accedere alla ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 esempio90) 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 esempio300TB. 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. Usa lo stesso formato di. *max_size*
- Sostituisci *shrink_threshold* con la percentuale di spazio utilizzata alla quale il volume si ridurrà automaticamente di dimensioni.

```
::> 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
```

3. Per mostrare l'impostazione corrente di autosize, esegui il comando seguente. Sostituisci *svm_name* e *vol_name* con le tue informazioni.

```
::> volume autosize -vserver svm_name -volume vol_name
```

Attivazione della modalità di scrittura su cloud

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. Aggiornamento di una politica di suddivisione in più livelli

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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 è stato 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.
   ```

Aggiornamento della capacità di archiviazione

È possibile gestire la capacità di storage dei volumi aumentando o diminuendo manualmente le dimensioni del volume utilizzando l'API Console di gestione AWS, 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 FSx console Amazon e l'API. AWS CLI Per ulteriori informazioni, consulta Aggiornamento dei volumi.

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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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
   ```

Aggiornamento di una politica di suddivisione in più livelli

Puoi modificare la politica di suddivisione in più livelli di un volume utilizzando l'API Console di gestione AWS, 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. Console di gestione AWS

1. Apri la FSx console Amazon 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 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.
   - 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
```

Aggiornamento dei giorni minimi di raffreddamento

I giorni minimi di raffreddamento 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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.
   ```

Aggiornamento della policy 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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.
```

Aggiornamento del numero massimo di file su un volume

FSx i volumi 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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
     ```

Monitoraggio della capacità di archiviazione del volume

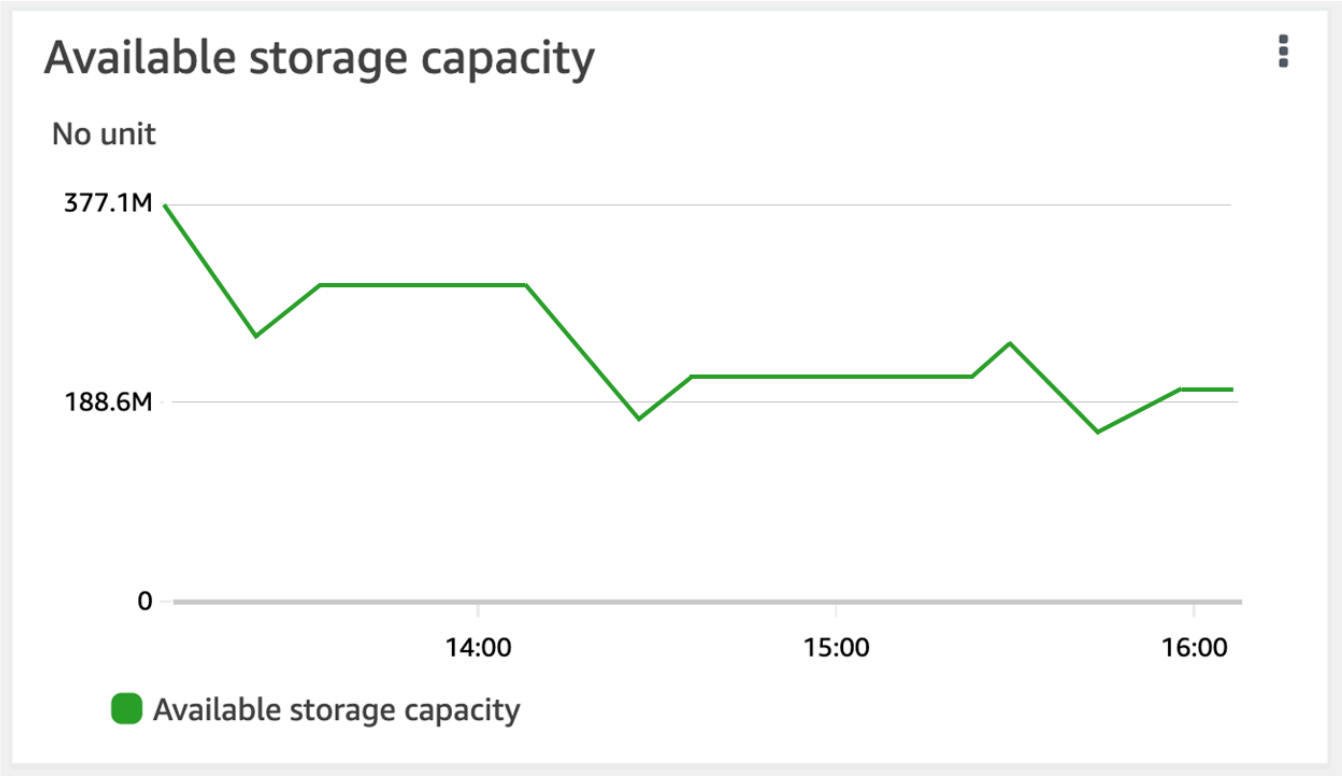
Puoi visualizzare lo spazio di archiviazione disponibile di un volume e la sua distribuzione di storage in Console di gestione AWS e nella AWS CLI CLI di NetApp ONTAP.

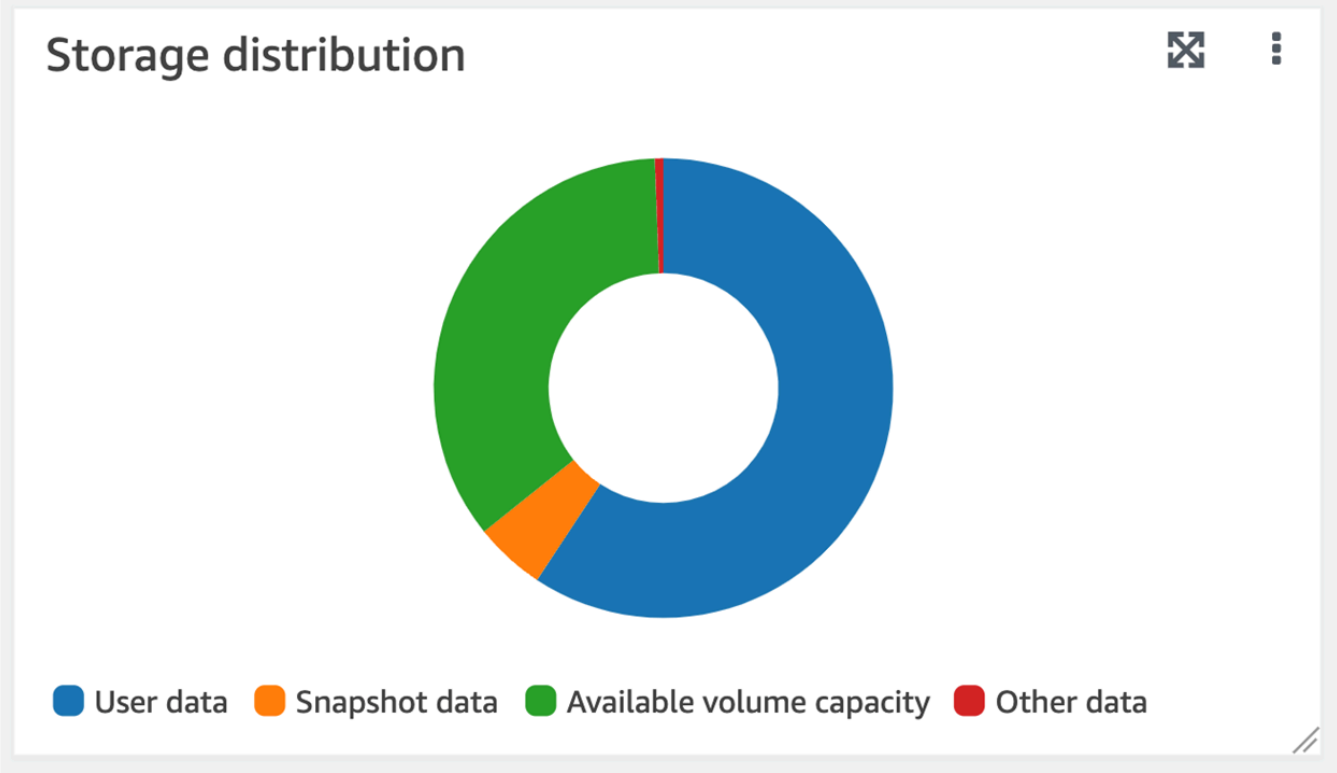
Per monitorare la capacità di archiviazione di un volume (console)

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 FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli Volumi nella colonna di navigazione a sinistra, quindi scegli il volume ONTAP per il quale 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.





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

Puoi 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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`

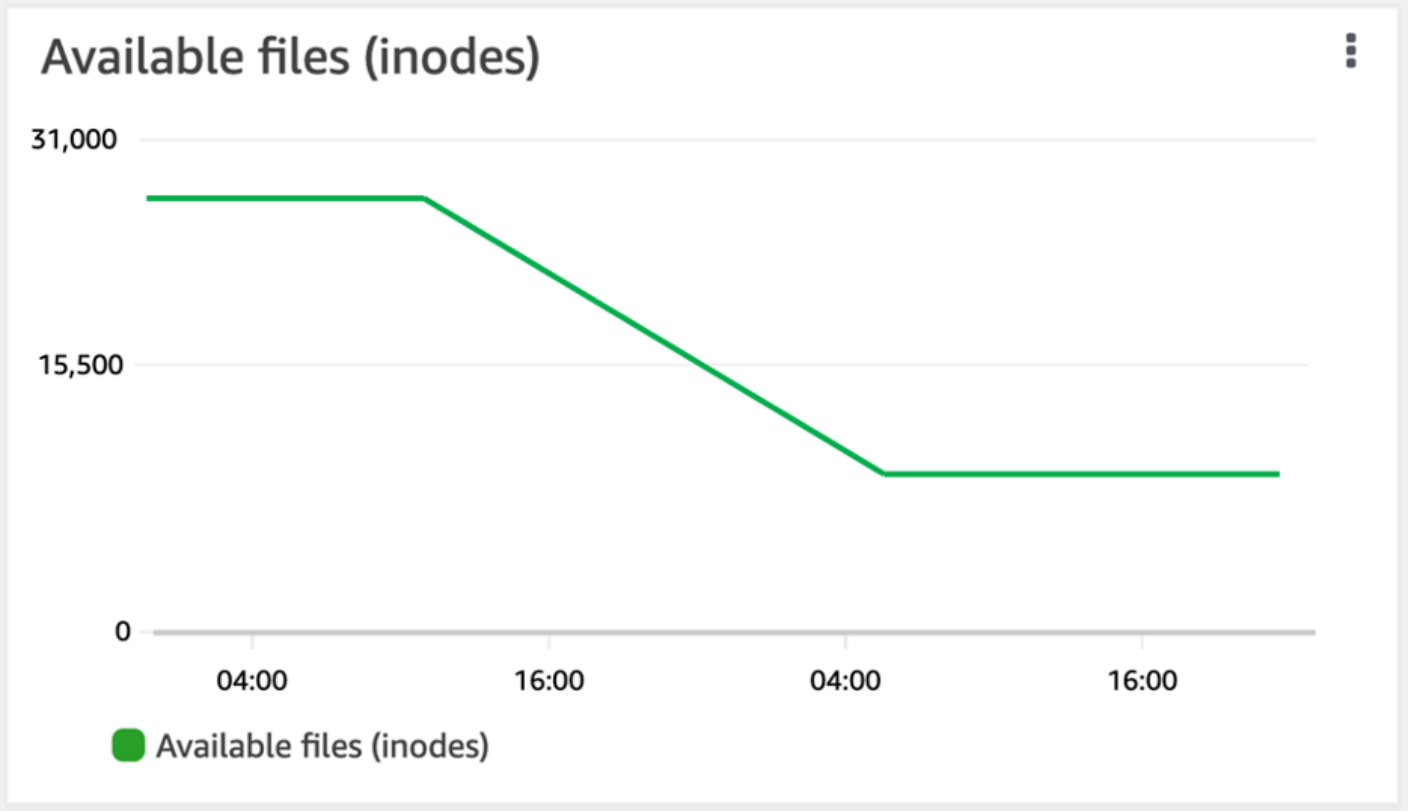
Per aumentare la quantità di spazio disponibile, è possibile aumentare la dimensione del volume oppure eliminare le istantanee che non si utilizzano, come illustrato nelle procedure seguenti.

Per i tipi di FlexVol volume (il tipo di volume predefinito FSx per i volumi ONTAP), puoi anche abilitare il dimensionamento automatico dei volumi. Quando abiliti 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.

Monitoraggio 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` e`FilesUsed`.
- Nella FSx console Amazon, vai alla tabella dei file disponibili (inode) nella scheda Monitoraggio del volume. L'immagine seguente mostra i file disponibili (inode) su un volume che diminuisce nel tempo.



Gestione dei file system ONTAP FSx

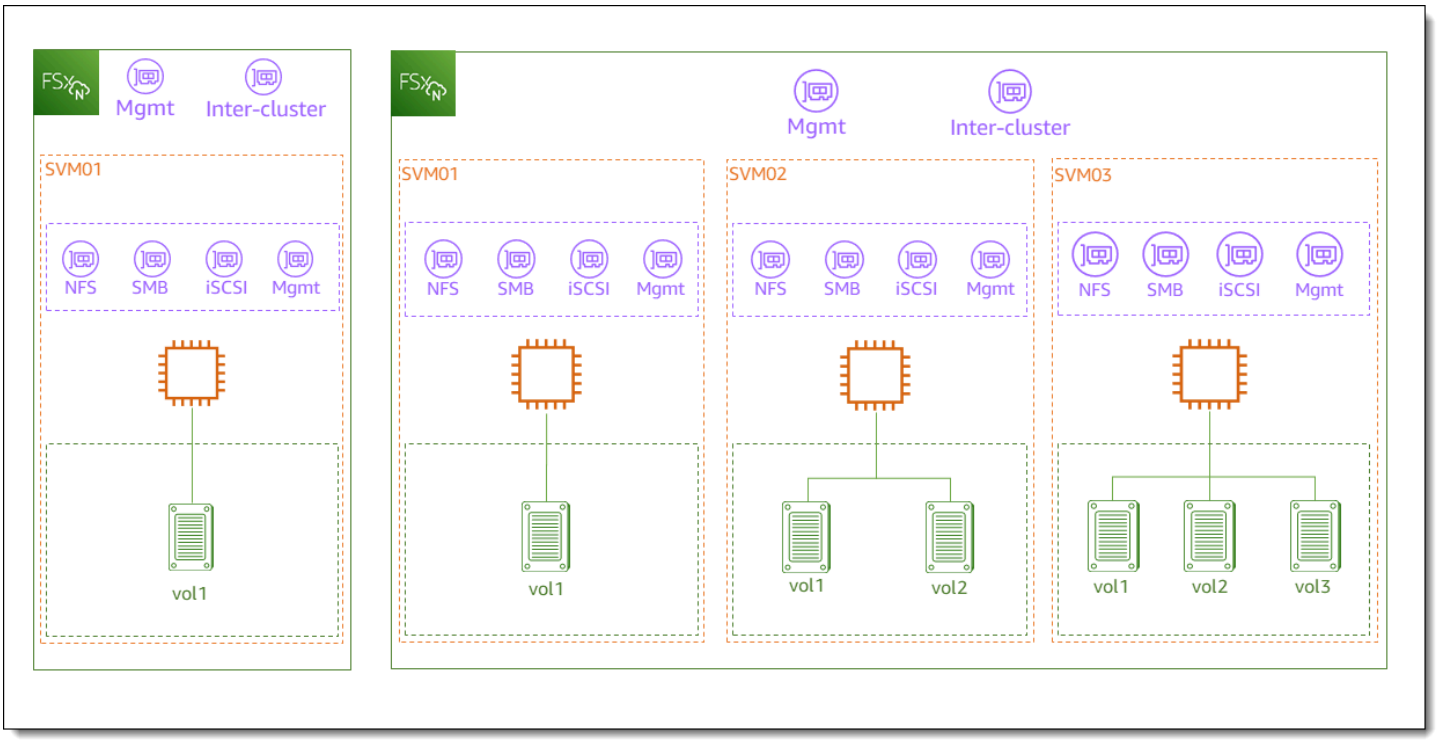
Un file system è la FSx risorsa Amazon principale, analoga a un cluster ONTAP locale. È necessario specificare la capacità di archiviazione e la capacità di throughput dell'unità a stato solido (SSD) per il file system e scegliere un cloud privato virtuale (VPC) in cui creare il file system. Ogni file 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 archiviazione.
- Una o più coppie di file server ad alta disponibilità (HA), che ospitano le macchine virtuali di storage ()SVMs. I file system di prima generazione e i file system Multi-AZ di seconda generazione hanno una coppia HA, mentre i file system Single-AZ di seconda generazione hanno fino a 12 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.
- Uno o più SVMs 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 di prima generazione 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 è composto da più file SVMs, alcuni dei quali SVMs hanno più volumi. SVMs Ciascuno dei file system ha più endpoint di gestione e dispone SVMs 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. I file system Single-AZ di prima generazione supportano una coppia HA. I file system Single-AZ di seconda generazione supportano fino a 12 coppie HA. 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 I file system Multi-AZ di prima e seconda generazione supportano entrambi una coppia HA.

  > **Note**
  >
  > Non è possibile modificare il tipo di distribuzione del file system dopo la creazione. Se desideri modificare il tipo di distribuzione (ad esempio, passare da Single-AZ 1 a Single-AZ 2), puoi eseguire il backup dei dati e ripristinarli su un nuovo file system. È inoltre possibile migrare i dati conNetApp SnapMirror, con o con uno strumento AWS DataSync di copia dei dati di terze parti. Per ulteriori informazioni, consultare Migrazione a for ONTAP utilizzando FSx NetApp SnapMirror e Migrazione a FSx for ONTAP utilizzando AWS DataSync.

- Capacità di archiviazione: si tratta della quantità di storage SSD, fino a 192 tebibyte (TiB) per i file system di prima generazione, 512 TiB per i file system Multi-AZ di seconda generazione e 1 pebibyte (PiB) per i file system Single-AZ di seconda generazione.
- IOPS SSD: per impostazione predefinita, ogni gigabyte di storage SSD include tre IOPS SSD (fino al massimo supportato dalla configurazione del file system). Se necessario, è possibile fornire ulteriori IOPS SSD.
- 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.

Puoi gestire FSx i file system ONTAP utilizzando la NetApp CLI di ONTAP o l'API REST. Puoi anche configurare SnapMirror o stabilire SnapVault relazioni tra un FSx file system Amazon e un'altra distribuzione ONTAP (incluso un altro FSx file system Amazon). FSx Ciascun file system 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, consultare Gestione FSx delle risorse ONTAP tramite applicazioni NetApp e Replica dei dati utilizzando NetApp SnapMirror.

Creazione di file system

Questa sezione descrive come creare un file system FSx for ONTAP utilizzando la FSx console Amazon o l' FSx API Amazon. AWS CLI 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 FSx console Amazon, Amazon crea FSx automaticamente un file system con una singola macchina virtuale di archiviazione (SVM) e un volume, che consente un accesso rapido ai dati delle 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 volumi aggiuntivi SVMs e 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 esigenze. Per informazioni sull'utilizzo dell'opzione di creazione rapida per creare rapidamente un file system con un set predefinito di parametri di configurazione, vedereCrea un file system Amazon FSx for NetApp ONTAP.

1. Apri la FSx console Amazon 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 2, Single-AZ 2, Multi-AZ 1 o Single-AZ 1.
  - I file system Multi-AZ replicano i dati e supportano il failover su più zone di disponibilità nella stessa area. Regione AWS Multi-AZ 1 è un file system ONTAP di prima generazione FSx . Multi-AZ 2 è un file system di seconda generazione. Entrambi supportano una coppia ad alta disponibilità (HA).
  - I file system Single-AZ replicano i dati e offrono il failover automatico all'interno di un'unica zona di disponibilità. Single-AZ 1 è un file system di prima generazione FSx per ONTAP che supporta una coppia HA. Single-AZ 2 è un file system di seconda generazione che supporta fino a 12 coppie HA. Per ulteriori informazioni, consulta Gestione delle coppie ad alta disponibilità (HA).

    Per ulteriori informazioni sui tipi di distribuzione, vedere. Disponibilità, durabilità e opzioni di implementazione

    > **Note**
    >
    > Non è possibile modificare il tipo di distribuzione del file system dopo la creazione. Se desideri modificare il tipo di distribuzione (ad esempio, passare da Single-AZ 1 a Single-AZ 2), puoi eseguire il backup dei dati e ripristinarli su un nuovo file system. È inoltre possibile migrare i dati conNetApp SnapMirror, con o con uno strumento AWS DataSync di copia dei dati di terze parti. Per ulteriori informazioni, consultare Migrazione a for ONTAP utilizzando FSx NetApp SnapMirror e Migrazione a FSx for ONTAP utilizzando AWS DataSync.
- 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 storage necessaria 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 effettui automaticamente FSx 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, consultare 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 che hai scelto.
  - 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 Gestione delle 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 le prestazioni di NetApp 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.
- (Solo Multi-AZ) Per la sottorete preferita, scegli qualsiasi valore dall'elenco delle sottoreti disponibili. Scegliete anche una sottorete Standby per il file server di standby.
- (Solo Single-AZ) Per Subnet, scegliete un valore qualsiasi dall'elenco delle sottoreti disponibili.

- (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 routing 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 i file system Multi-AZ utilizzando l'autenticazione basata su tag. Queste tabelle di routing sono contrassegnate con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Quando si crea FSx per i file system ONTAP Multi-AZ, si CloudFormation consiglia di aggiungere il `Key: AmazonFSx; Value: ManagedByAmazonFSx` tag manualmente.

- Per Tipo di rete, seleziona IPv4(solo per il IPv4 supporto) o Dual-stack (per entrambi e supporto). IPv4 IPv6 È possibile modificare il tipo di rete di un file system esistente in qualsiasi momento. Per ulteriori informazioni, consulta Modifica del tipo di rete.

  > **Note**
  >
  > Se intendi creare un file system FSx per ONTAP che utilizzi la modalità dual-stack, devi prima assegnare un blocco IPv6 CIDR fornito da Amazon al tuo VPC e alle sottoreti. Per ulteriori informazioni, consulta Aggiungere il IPv6 supporto per il tuo VPC nella Guida per l'utente di Amazon Virtual Private Cloud.

- (Solo Multi-AZ) L'intervallo di IPv4 indirizzi degli endpoint specifica l'intervallo di IPv4 indirizzi in cui vengono creati gli endpoint per accedere al file system.

  Sono disponibili tre opzioni per l'intervallo di indirizzi degli endpoint: IPv4

  - Intervallo di IPv4 indirizzi non allocato dal tuo VPC: FSx Amazon sceglie gli ultimi 64 indirizzi IP dall'intervallo CIDR primario del VPC da utilizzare come intervallo di indirizzi endpoint per il IPv4 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 IPv4 indirizzi fluttuante all'esterno del tuo VPC: FSx Amazon 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 IPv4 indirizzi: puoi fornire un intervallo CIDR a tua scelta. L'intervallo di IPv4 indirizzi 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 for ONTAP: FSx
>
> - 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

- (Solo Multi-AZ e dual-stack) L'intervallo di indirizzi dell'endpoint specifica l'intervallo di IPv6 indirizzi in cui vengono creati gli endpoint per accedere al file system IPv6 . Sono disponibili due opzioni per l'intervallo di indirizzi dell'endpoint: IPv6
  - Intervallo di IPv6 indirizzi non allocato dal tuo VPC: FSx Amazon sceglie un blocco di 1024 indirizzi IPv6 disponibili da uno degli intervalli CIDR del VPC da utilizzare come intervallo di indirizzi IPv6 di endpoint per il file system. IPv6
  - Inserisci un intervallo di IPv6 indirizzi: puoi fornire un intervallo CIDR a tua scelta. IPv6 L'intervallo di IPv6 indirizzi che scegli può essere interno o esterno all'intervallo di IPv6 indirizzi del VPC, purché non si sovrapponga a nessuna sottorete.

7. Nella sezione Crittografia, per Chiave di crittografia, scegli la chiave di crittografia AWS Key Management Service (AWS KMS) che protegge i dati del file system a riposo.
8. Per 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 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 SVMs con la ONTAP CLI

     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.
   - Per lo stile di sicurezza Volume, scegli tra Unix (Linux) e NTFS per il volume. Per ulteriori informazioni, consulta Stile di sicurezza del volume.
   - Nella sezione Active Directory, puoi aggiungere un Active Directory alla SVM. Per ulteriori informazioni, consulta Utilizzo di Microsoft Active Directory in FSx 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 del server DNS: gli IPv4 o IPv6 gli indirizzi dei server DNS (Domain Name System) del tuo dominio.
     - Credenziali dell'account di servizio: scegli come fornire le credenziali del tuo account di servizio:

- Opzione 1: ARN Gestione dei segreti AWS segreto: il segreto contenente il nome utente e la password per un account di servizio nel dominio Active Directory. Per ulteriori informazioni, consulta Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.
- Opzione 2: credenziali in chiaro
  - Nome utente dell'account di servizio: il nome utente dell'account di servizio nel Microsoft 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 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 Amministratori delegati, FSx Amministratori AWS delegati o un gruppo personalizzato con AWS 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 (_).
    - (File system con una sola coppia HA) Per lo stile Volume, scegliete uno o. FlexVolFlexGroup FlexVoli volumi sono volumi generici che possono avere dimensioni fino a 300 tebibyte (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 20 e 314.572.800 mebibyte (MiB) per i volumi FlexVol o 800 gibibyte (GiB) e 2.400 TiB per coppia HA per i volumi. FlexGroup Ad esempio, un file system con 12 coppie HA avrebbe una dimensione di volume minima di 9.600 GiB e una dimensione massima di 20.480 TiB.

- 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 Efficienza dello storage.
- 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. Nella sezione SnapLock Configurazione predefinita del volume, per SnapLockConfigurazione, scegli tra Abilitato e Disabilitato. Per ulteriori informazioni sulla configurazione di un volume SnapLock Compliance o di un volume SnapLock Enterprise, consulta Comprendere la conformità SnapLock eComprendere SnapLock Enterprise. Per ulteriori informazioni su SnapLock, consultare Proteggi i tuoi dati con SnapLock.
13. 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.

14. 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.

    Scegli Next (Successivo).

15. 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.
16. Scegliere Create file system (Crea file system).

Per creare un file system (CLI)

- Per creare un file system FSx for ONTAP, utilizzate il comando create-file-systemCLI (o l'operazione API CreateFileSystemequivalente), come illustrato nell'esempio seguente.

> **Note**
>
> Non è possibile modificare il tipo di distribuzione del file system dopo la creazione. Se desideri modificare il tipo di distribuzione (ad esempio, passare da Single-AZ 1 a Single-AZ 2), puoi eseguire il backup dei dati e ripristinarli su un nuovo file system. È inoltre possibile migrare i dati conNetApp SnapMirror, con o con uno strumento AWS DataSync di copia dei dati di terze parti. Per ulteriori informazioni, consultare Migrazione a for

ONTAP utilizzando FSx NetApp SnapMirror e Migrazione a FSx for ONTAP utilizzando AWS DataSync.

```
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 macchine virtuali di archiviazione (SVM); per creare un volume, vedi. Creazione di volumi

Creazione FSx per i file system ONTAP in sottoreti condivise

La condivisione di VPC consente Account AWS a più persone di creare risorse in cloud privati virtuali condivisi e gestiti centralmente (). VPCs 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 FSx per i file system 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 l' FSx 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 FSx file system 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 FSx servizio Amazon 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 condividi le sottoreti con gli account dei partecipanti che verranno creati FSx per i file system ONTAP nelle sottoreti condivise, dovrai fare quanto segue:

- Il proprietario del VPC deve utilizzarlo per condividere in modo sicuro AWS Resource Access Manager le sottoreti con VPCs altri. Account AWS Per ulteriori informazioni, consulta Condivisione AWS delle risorse nella Guida per l'utente. AWS Resource Access Manager
- Il proprietario del VPC deve condividerne uno o più VPCs con un account partecipante. Per ulteriori informazioni, consulta Condividi il tuo VPC con altri account nella Amazon Virtual Private Cloud User Guide.
- Per creare FSx account partecipanti per i file system ONTAP Multi-AZ, il proprietario del VPC deve inoltre concedere al FSx servizio Amazon le autorizzazioni per creare e modificare le tabelle di routing nelle sottoreti condivise per conto degli account dei partecipanti. Questo perché FSx per ONTAP i file system Multi-AZ utilizzano indirizzi IP mobili in modo che i client connessi possano passare senza problemi dal file server preferito a quello 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 o meno file system Multi-AZ FSx for ONTAP nelle sottoreti VPC che il proprietario ha condiviso con i partecipanti utilizzando l'API, e Console di gestione AWS AWS CLI, come descritto nelle sezioni seguenti.

Per gestire la condivisione VPC per file system Multi-AZ (console)

Apri la FSx console Amazon 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 tutto ciò VPCs che possiedi, 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, utilizza il comando describe-shared-vpc-configurationCLI o il comando API DescribeSharedVpcConfigurationequivalente, mostrato di seguito:

```
$ aws fsx describe-shared-vpc-configuration
```

Il servizio risponde a una richiesta riuscita nel modo seguente:

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

2. Per gestire la configurazione VPC condivisa Multi-AZ, usa il comando update-shared-vpc-configurationCLI 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 dei file system

Questo argomento spiega quali proprietà di un file system esistente è possibile aggiornare e fornisce le procedure per farlo utilizzando la FSx console Amazon e la CLI. Puoi aggiornare quanto segue FSx per le proprietà del file system ONTAP utilizzando la FSx console Amazon e AWS CLI l'API:

- 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, consulta 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, consulta Ottimizzazione delle prestazioni con le finestre di FSx manutenzione di Amazon.
- 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 alla CLI, all'API e alla console ONTAP utilizzano indirizzi IP NetApp mobili nelle tabelle di routing Amazon VPC che associ al tuo file system. Puoi associare nuove tabelle di routing che crei ai tuoi file system Multi-AZ esistenti, consentendoti di configurare quali client possono accedere ai tuoi dati anche se la tua 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 i file system Multi-AZ utilizzando l'autenticazione basata su tag. Queste tabelle di routing sono contrassegnate con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Durante la creazione o l'aggiornamento FSx per l'utilizzo di file system ONTAP Multi-AZ, si CloudFormation consiglia di aggiungere il `Key: AmazonFSx; Value: ManagedByAmazonFSx` tag manualmente.

Per aggiornare un file system (console)

Le seguenti procedure forniscono istruzioni su come effettuare aggiornamenti a un file system di FSx for ONTAP esistente utilizzando. Console di gestione AWS

Per aggiornare i backup giornalieri automatici

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Per visualizzare la pagina dei dettagli del file system, nel riquadro di navigazione a sinistra, scegli File system, quindi scegli FSx il file system ONTAP che desideri aggiornare.
3. Scegli la scheda Backup nel secondo pannello della pagina.
4. Scegliere Aggiorna.
5. Modifica le impostazioni di backup giornaliero automatico per questo file system.
6. Scegli Salva per salvare le modifiche.

Per aggiornare la finestra di manutenzione settimanale

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Per visualizzare la pagina dei dettagli del file system, nel riquadro di navigazione a sinistra, scegli File system, quindi scegli FSx il file system ONTAP che desideri aggiornare.
3. Scegli 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. Scegli Salva per salvare le modifiche.

Per modificare la password amministrativa del file system

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Per visualizzare la pagina dei dettagli del file system, nel riquadro di navigazione a sinistra, scegli File system, quindi scegli FSx il file system ONTAP che desideri aggiornare.
3. Scegli la scheda Amministrazione.
4. Nel pannello di amministrazione ONTAP, scegli Aggiorna sotto la password dell'amministratore ONTAP.
5. Nella finestra di dialogo Aggiorna le credenziali di 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 FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Per visualizzare la pagina dei dettagli del file system, nel riquadro di navigazione a sinistra, scegli File system, quindi scegli FSx il file system ONTAP che desideri aggiornare.
3. Per Azioni, scegli Aggiorna file system > Aggiorna tabelle di routing. Oppure, nel pannello Rete e sicurezza, scegli Gestisci accanto alle tabelle di routing del file system.
4. Nella finestra di dialogo Gestisci le tabelle degli itinerari, esegui 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 update-file-systemCLI (o l'operazione API UpdateFileSystemequivalente), 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, imposta la `AutomaticBackupRetentionDays` proprietà su 0.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

Gestione delle coppie ad alta disponibilità (HA)

Ciascun file system FSx for ONTAP è alimentato da una o più coppie di file server ad alta disponibilità (HA) in una configurazione in 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. FSx per ONTAP, i file system di prima generazione sono alimentati da una coppia HA, che offre fino al 4% GBps della capacità di throughput e 160.000 SSD. IOPs FSx per ONTAP, i file system Multi-AZ di seconda generazione sono alimentati anche da una coppia HA e offrono fino al 6% di capacità di throughput e 200.000 IOPS SSD. GBps FSx per ONTAP i file system Single-AZ di seconda generazione sono alimentati da un massimo di 12 coppie HA, in grado di fornire fino al 72% di capacità di throughput e 2.400.000 IOPS SSD (6 GBps di capacità di throughput e 200.000 IOPS SSD per coppia HA). GBps

Quando crei il tuo file system dalla FSx console Amazon, 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 un massimo del 6% di capacità GBps di throughput e 200.000 SSD IOPs, e 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**
>
> È possibile aggiungere coppie HA ai file system Single-AZ di seconda generazione. Per ulteriori informazioni, consulta Aggiungere coppie ad alta disponibilità (HA). Altrimenti, è 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

Aggiungere coppie ad alta disponibilità (HA)

FSx per ONTAP i file system sono composti da una o più coppie di file server HA. I file system di prima generazione e i file system Multi-AZ di seconda generazione supportano una coppia HA, mentre i file system Single-AZ di seconda generazione supportano fino a 12 coppie HA. È inoltre possibile aggiungere altre coppie HA dopo aver creato un file system Single-AZ di seconda generazione (fino a un massimo di 12). L'aggiunta di coppie HA non comporta interruzioni e in genere richiede solo pochi minuti per essere completata.

Quando aggiungi coppie HA al tuo file system, considera i seguenti punti:

- L'aggiunta di coppie HA al file system introduce nuovi file server con un proprio storage (o aggregato). Le nuove coppie HA hanno la stessa capacità di throughput e capacità di storage delle coppie HA esistenti del file system. Ad esempio, supponiamo che il file system disponga di due coppie HA con un totale di 12 di capacità GBps di throughput e 2 tebibyte (TiB) di storage SSD. Se aggiungi una nuova coppia HA, il file system avrà una capacità GBps di throughput del 18% e 3 TiB di storage SSD.
- Per sfruttare le prestazioni aggiuntive delle nuove coppie HA, è necessario spostare alcuni dei volumi esistenti nelle nuove coppie HA e rimontare i client per connettersi a tali coppie. Per ulteriori informazioni, consulta Bilanciamento dei carichi di lavoro tra coppie HA.

- Non è possibile modificare la capacità di throughput del file system, la capacità di archiviazione SSD o gli IOPS SSD assegnati quando si aggiungono coppie HA o mentre è in corso un aggiornamento per aggiungere coppie HA.
- Non è possibile rimuovere le coppie HA dopo averle aggiunte. Ti consigliamo di scalare la capacità di throughput del file system se hai bisogno temporaneamente di maggiori prestazioni (supponendo che il file system non abbia la massima capacità di throughput). Ciò aumenta la capacità di throughput delle coppie HA esistenti del file system.
- Il protocollo iSCSI è disponibile su file system con sei o meno coppie ad alta disponibilità (coppie HA). Il NVMe/TCP protocollo è disponibile sui file system di seconda generazione con sei o meno coppie HA. Per ulteriori informazioni, consulta Accesso ai dati di FSx for ONTAP.
- Quando si aggiungono nuove coppie HA al file system, la NVMe cache è abilitata per impostazione predefinita per i nuovi nodi del file system. Si consiglia di disabilitarla per carichi di lavoro che richiedono un throughput elevato. Per ulteriori informazioni, consulta Gestione della cache NVMe.

Per aggiungere coppie HA

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Per visualizzare la pagina dei dettagli del file system, nel riquadro di navigazione a sinistra, scegli File system, quindi scegli FSx il file system ONTAP che desideri aggiornare.
3. Nel pannello Riepilogo, per Numero di coppie HA, scegliete Aggiorna.
4. Dal menu a discesa HA Pairs, selezionate il numero di coppie HA da aggiungere al file system.
5. Scegli il pulsante Aggiorna.

Dopo aver aggiunto le coppie HA, è importante ribilanciare i dati esistenti per garantire che I/O rimangano distribuiti uniformemente tra le coppie HA del file system. Per ulteriori informazioni, consulta Bilanciamento dei carichi di lavoro tra coppie HA.

Bilanciamento dei carichi di lavoro tra coppie HA

Se disponi di un file system con più coppie ad alta disponibilità (HA), la velocità effettiva e lo storage sono distribuiti su ciascuna delle coppie HA. FSx for ONTAP bilancia automaticamente i file man mano che vengono scritti nel file system, ma i dati del carico di lavoro non I/O sono più bilanciati una volta aggiunte le coppie HA. Inoltre, in rari casi, i dati del carico di lavoro I/O potrebbero risultare sbilanciati tra le coppie HA esistenti del file system, il che può influire sulle prestazioni complessive del carico di lavoro. Se il carico di lavoro presenta uno squilibrio, puoi ribilanciarlo 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 notate che gli aggregati sono squilibrati, potete aumentare la capacità di storage principale del file system (aumentando proporzionalmente la capacità di storage di ciascun aggregato) oppure spostare i volumi tra gli aggregati. Per ulteriori informazioni, consulta Spostamento di volumi tra aggregati.

Sbilanciamento tra l'utilizzo di file server e dischi

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 I/O hotspotting su un sottoinsieme di coppie HA (un sottoinsieme dei 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 utilizzati per vedere quali hanno la maggiore attività all'interno di un aggregato. Per ulteriori informazioni su questa procedura, consulta Ribilanciamento dei volumi.
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.

Mappatura delle CloudWatch dimensioni alle risorse dell'API REST e della CLI ONTAP

Il tuo file system di seconda generazione 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 l'utente Utilizzo della CLI NetApp ONTAP di Amazon FSx for ONTAP. NetApp

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Usa 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

Dopo aver aggiunto le coppie HA o se riscontri I/O uno squilibrio tra i file server (in particolare per quanto riguarda l'utilizzo del throughput di rete), puoi ribilanciare i client. Se stai ribilanciando i client dopo aver aggiunto coppie HA, puoi passare a. Rimontaggio dei client Altrimenti, dovresti prima identificare i client ad alto traffico che desideri spostare per ribilanciare l'I/O del carico di lavoro.

Se riscontri uno I/O squilibrio tra i file server (in particolare per quanto riguarda l'utilizzo del throughput di rete), la causa potrebbe essere un numero elevato di client. I/O Per identificare i client ad alto traffico, utilizza la CLI di ONTAP.

Identifica i client ad alto traffico

1. Per accedere tramite SSH alla NetApp CLI ONTAP del tuo file system, segui i passaggi documentati nella sezione della Guida per l'utente Utilizzo della CLI NetApp ONTAP 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
   ```

Rimontaggio dei client

- È possibile ribilanciare i client con altre coppie HA. A tale scopo, smonta il volume dal client e rimontalo utilizzando il nome DNS dell'endpoint dell'SVM NFS/SMB : 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 file server che sta registrando 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 versoFsxId01234567890abcdef-01. L'output del `network interface show` comando indica che questo è l'indirizzo172.31.15.89. Per eseguire il montaggio su un dispositivo diverso, selezionate qualsiasi altro indirizzo (in questo esempio, l'unico altro indirizzo è172.31.8.112, corrispondente aFsxId01234567890abcdef-03).

Ribilanciamento dei volumi

Se riscontri uno I/O squilibrio tra i volumi o gli aggregati, puoi ribilanciare i volumi per ridistribuire il traffico tra i volumi. I/O

> **Note**
>
> Se riscontri 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. 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'impatto di ciascun volume che si intende spostare I/O .

1. Per accedere tramite SSH alla NetApp CLI ONTAP del tuo file system, segui i passaggi documentati nella sezione della Guida per l'utente Utilizzo della CLI NetApp ONTAP 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, è possibile 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 mostrate 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 peraggr1. 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. Se hai aggiunto nuove coppie HA, dovresti spostare i volumi esistenti in nuovi aggregati. Per ulteriori informazioni, consulta Spostamento di volumi tra aggregati.

Gestione della cache NVMe

La NVMe cache è abilitata per impostazione predefinita nel file system di seconda generazione. Se il file system di seconda generazione ha un carico di lavoro che richiede un throughput elevato, puoi disabilitare la cache per migliorare le prestazioni. NVMe La procedura seguente spiega come abilitare, disabilitare e convalidare la cache del file system. NVMe

Per gestire la cache NVMe

1. SSH nel tuo ONTAP file system. Per ulteriori informazioni, consulta the section called “Utilizzo della CLI NetApp ONTAP”.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. Usa il comando system node external-cache modifyONTAPCLI. Scegli **`true`** se abilitare o **`false`** disabilitare la NVMe cache.

   ```
   ::> system node external-cache modify -node * -is-enabled [true|false]
   ```

3. Usa il comando system node external-cache showONTAPCLI per verificare se la NVMe cache è abilitata o disabilitata.

   ```
   ::> system node external-cache show -node * -fields is-enabled
   ```

La NVMe cache è abilitata o disabilitata in base al nodo. Quando si aggiungono nuove coppie ad alta disponibilità (HA) al file system, ogni nuovo nodo ha lo stesso comportamento predefinito dei nodi del nuovo file system. Pertanto, la NVMe cache verrebbe abilitata per tutti i nuovi nodi su un file system anche se i nodi esistenti l'hanno disabilitata. Per ulteriori informazioni, consulta Aggiungere coppie ad alta disponibilità (HA).

Gestione del tipo di rete

Quando si crea un file system FSx for ONTAP, è necessario specificare un tipo di rete, che deve essere una delle seguenti opzioni:

- `IPv4`consente al file system di comunicare utilizzando solo il protocollo Internet versione 4 (IPv4).
- `Dual-stack`consente al file system di comunicare utilizzando sia il protocollo Internet versione 6 (IPv6) che IPv4.

Puoi modificare il tipo di rete di un file system FSx for ONTAP esistente in qualsiasi momento utilizzando la Console di FSx gestione Amazon AWS CLI, l' AWS API o uno dei AWS SDKs. Ad esempio, se le tue sottoreti supportano entrambe le modalità IPv4 e l' IPv6 indirizzamento, puoi aggiornare il file system esistente dalla modalità IPv4 -only alla modalità dual-stack. Puoi anche aggiornare il tuo file system dual-stack a -only. IPv4

Utilizzo della modalità dual-stack

È consigliabile utilizzare la modalità dual-stack se è necessario accedere e gestire i FSx file system Amazon in modo nativo dai client. IPv6 Configurando il tuo FSx file system Amazon per utilizzare l'indirizzamento dual-stack, puoi accedere ai dati dei file sia dai IPv6 client che dai IPv4 client nello stesso Amazon VPC, nel VPC di un altro o nella tua rete Account AWS locale. Ad esempio, con un FSx file system Amazon configurato per utilizzare il dual-stack, puoi avere IPv4 client esistenti e nuovi IPv6 client che accedono ai dati dei tuoi file archiviati nel tuo file system.

Per impostazione predefinita, Amazon FSx e Amazon VPC utilizzano il protocollo di IPv4 indirizzamento. Pertanto, come prerequisito per l'utilizzo IPv6, devi prima assegnare un blocco CIDR (IPv6 Classless Inter-Domain Range) fornito da Amazon al tuo VPC e alle tue sottoreti prima di poterlo utilizzare con i tuoi file system Amazon. IPv6 FSx Per informazioni sull'attivazione IPv6 del tuo VPC, consulta Aggiungi IPv6 supporto per il tuo VPC nella Guida per l'utente di Amazon Virtual Private Cloud.

Quando FSx crei per i file system ONTAP impostati in modalità dual-stack, puoi specificare l'intervallo di IPv6 indirizzi, oltre all'intervallo di IPv4 indirizzi esistente, in cui verranno creati gli endpoint per accedere al tuo file system. Per impostazione predefinita, Amazon FSx sceglie un blocco di 1024 indirizzi IP da uno degli intervalli IPv6 CIDR del VPC da utilizzare come intervallo di indirizzi endpoint per il file IPv6 system.

Modifica del tipo di rete

Puoi modificare il tipo di rete di un file system utilizzando la FSx console Amazon, AWS Command Line Interface (AWS CLI) o l' FSx API Amazon.

Per modificare il tipo di rete di un file system (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Vai a File system e scegli FSx il file system ONTAP di cui desideri modificare il tipo di rete.
3. Per Azioni, scegli Aggiorna tipo di rete. Oppure, nel pannello Rete e sicurezza, scegli Gestisci accanto al tipo di rete del file system.

Viene visualizzata la finestra Aggiorna tipo di rete.

4. Per Tipo di rete desiderato, scegli uno dei due IPv4o Dual-stack.

   - Se scegli`IPv4`, non sono necessarie ulteriori configurazioni.
   - Se lo desideri`Dual-stack`, specifica l'intervallo di IPv6 indirizzi che verranno utilizzati dagli endpoint del file system:
     - Intervallo di IPv6 indirizzi non allocato dal tuo VPC: FSx Amazon sceglie un intervallo di indirizzi IP /118 disponibile da uno degli intervalli CIDR del VPC da utilizzare come intervallo IPv6 di indirizzi endpoint per il file system. IPv6
     - Inserisci un intervallo di IPv6 indirizzi: puoi fornire un intervallo CIDR a tua scelta. IPv6 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.

5. Scegli Aggiorna.

Per modificare il tipo di rete (CLI) di un file system

- Per modificare il tipo di rete di un file system, utilizzate il comando update-file-systemCLI (o l'operazione UpdateFileSystemAPI equivalente), come illustrato nell'esempio seguente.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --network-type DUAL
```

Monitoraggio dei dettagli del file system

Puoi visualizzare informazioni di configurazione dettagliate per il tuo file system FSx for ONTAP utilizzando la FSx console Amazon AWS CLI, l'API e AWS SDKs Supported.

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: visualizza le seguenti informazioni di amministrazione del file system:
  - Amazon VPC predefinito
  - Tabelle di routing Amazon VPC associate a un file system Multi-AZ
  - Tipo di rete del file system (IPv4-only o dual-stack)
  - Endpoint o intervallo di indirizzi IPv4 IPv6
  - L'ID della chiave AWS Key Management Service (AWS KMS)
- 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 dei file system SVMs
- 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 describe-file-systemsCLI o l'operazione API. DescribeFileSystems

FSx per lo stato del file system ONTAP

Puoi visualizzare lo stato di un FSx file system Amazon utilizzando la FSx console Amazon, il AWS CLI comando describe-file-systemso l'operazione API DescribeFileSystems.

Stato del file system	Description
DISPONIBILE	Il file system è stato creato con successo ed è disponibile per l'uso.
CREAZIONE IN CORSO	Amazon FSx sta creando un nuovo file system.
ELIMINAZIONE IN CORSO	Amazon FSx sta eliminando un file system esistente.
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 non è in FSx grado di ripristinarlo. 2. Durante la creazione di un nuovo file system, Amazon non FSx è stato in grado di creare un nuovo file system.

Eliminazione dei file system

Puoi eliminare un file system FSx for ONTAP utilizzando la FSx console Amazon AWS CLI, l' FSx API Amazon e SDKs.

Per eliminare un file system:

- Utilizzo della console: seguire la procedura descritta inPulizia delle risorse.
- Utilizzo della CLI o dell'API: prima elimina tutti i volumi e SVMs il file system. Quindi usa il comando delete-file-systemCLI o l'operazione DeleteFileSystemAPI.

Gestione delle FSx macchine virtuali di archiviazione ONTAP

In FSx ONTAP, i volumi sono ospitati su file server virtuali denominati macchine virtuali di archiviazione (). SVMs Un SVM è un file server isolato con credenziali amministrative ed endpoint propri per l'amministrazione e l'accesso ai dati. Quando accedi ai dati in FSx 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 crea FSx automaticamente una SVM predefinita sul tuo file system quando crei un file system utilizzando. Console di gestione AWS Puoi crearne altri SVMs sul tuo file system in qualsiasi momento utilizzando la console o AWS CLI l' FSx API Amazon e SDKs. Non è possibile creare SVMs utilizzando la CLI ONTAP o l'API REST.

Puoi unirti SVMs 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 ONTAP.

Numero SVMs massimo di file system

La tabella seguente elenca il numero massimo di file SVMs che è possibile creare per un file system. Il numero massimo di SVMs dipende dalla quantità di capacità di throughput fornita in megabyte al secondo (MBps) e anche dal tipo di rete del file system.

Coppie ad alta disponibilità (HA)	Quantità di capacità di trasmissione () MBps	Numero SVMs massimo di file system (modalità IPv4 solo)	Numero SVMs massimo di file system (modalità dual-stack)
1 coppia HA	128	6	6
	256	6	6
	384	6	6
	512	14	11
	768	6	6
	1,024	14	11
	1.536	14	11
	2.048	24	11
	3.072	14	11
	4,096	24	11
	6.144	24	11

Coppie ad alta disponibilità (HA)	Quantità di capacità di trasmissione () MBps	Numero SVMs massimo di file system (modalità IPv4 solo)	Numero SVMs massimo di file system (modalità dual-stack)
2—12 paia HA	Qualsiasi	11	11

Argomenti

- Creazione di macchine virtuali di archiviazione (SVM)
- Aggiornamento delle macchine virtuali di archiviazione (SVM)
- Gestione delle configurazioni SVM di Microsoft Active Directory
- Controllo dell'accesso ai file
- Configurazione di un server SMB in un gruppo di lavoro
- Monitoraggio dei dettagli di configurazione della macchina virtuale di archiviazione (SVM)
- Eliminazione di macchine virtuali di archiviazione (SVM)

Creazione di macchine virtuali di archiviazione (SVM)

È possibile creare un SVM FSx per ONTAP utilizzando l' Console di gestione AWS API, e. AWS CLI

Il numero massimo di file SVMs che è possibile creare per un file system dipende dal tipo di implementazione del file system, dal tipo di rete e dalla quantità di capacità di throughput fornita. Per ulteriori informazioni, consulta Numero SVMs massimo di 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 ONTAP.
- Lo stile di sicurezza del volume root: imposta lo stile di sicurezza del volume root (Unix o NTFS) in modo che corrisponda al tipo di client che utilizzi per accedere ai 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 SVMs con la ONTAP CLI.

Per creare una macchina virtuale di archiviazione (console)

1. Apri la FSx console Amazon 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.
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 SVMs con la ONTAP CLI

   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. L'FQDN non può superare i 255 caratteri.
     - Indirizzi IP del server DNS: gli IPv4 o IPv6 gli indirizzi dei server DNS del dominio.
     - Credenziali dell'account di servizio: scegli come fornire le credenziali del tuo account di servizio:

    - Opzione 1: ARN Gestione dei segreti AWS segreto: il segreto contenente il nome utente e la password per un account di servizio nel dominio Active Directory. Per ulteriori informazioni, consulta Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.
    - Opzione 2: credenziali in chiaro
      - Nome utente dell'account di servizio: il nome utente dell'account di servizio nel Microsoft 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 si desidera aggiungere il file system.
  - Gruppo di amministratori di file system delegati: nome del gruppo dell'AD che può amministrare il file system.

    Se si utilizza AWS Managed Microsoft AD, è necessario specificare un gruppo come Amministratori delegati, FSx Amministratori AWS delegati o un gruppo personalizzato AWS 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)

- FSx Per creare una macchina virtuale di archiviazione (SVM) 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 archiviazione, Amazon FSx restituisce la descrizione in formato JSON, come mostrato 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 delle macchine virtuali di archiviazione (SVM)

Puoi aggiornare le seguenti proprietà di configurazione della macchina virtuale di archiviazione (SVM) utilizzando la FSx console Amazon e AWS CLI l' FSx API Amazon:

- 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 di Microsoft Active Directory.

Per aggiornare le credenziali dell'account amministratore SVM (console)

1. Apri la FSx console Amazon 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 macchine virtuali SVMs disponibili Account AWS nel tuo attuale sistema Regione 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 SVM FSx for ONTAP, 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 archiviazione, Amazon FSx restituisce la descrizione in formato JSON, come mostrato 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"
      }
    }
  }
}
```

Gestione delle configurazioni SVM di Microsoft Active Directory

È possibile aggiungere una SVM a Microsoft Active Directory o modificare la configurazione di Microsoft Active Directory di una SVM già aggiunta a Microsoft Active Directory. FSx for ONTAP si integra con per gestire in modo sicuro Gestione dei segreti AWS le credenziali dell'account del servizio di accesso al dominio.

Per aggiornare la configurazione di SVM Microsoft Active Directory (console)

1. Apri la FSx console Amazon 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 ONTAP file system per il quale desiderate aggiornare un SVM.
   - Scegli la scheda Storage virtual machines.

   —Oppure—

   - Per visualizzare un elenco di tutte le macchine virtuali SVMs disponibili Account AWS nel tuo sistema attuale Regione AWS, espandi ONTAPe scegli Storage virtual machines.
3. Scegli la macchina virtuale di archiviazione che desideri aggiornare.
4. Scegli Azioni > Aggiorna la configurazione di Microsoft Active Directory. Viene visualizzata la finestra di configurazione Update Microsoft Active Directory.
5. Per le credenziali dell'account del servizio di accesso al dominio, scegli Gestito in Secrets Manager (consigliato) per utilizzare Secrets Manager per la gestione sicura delle credenziali.

   > **Note**
   >
   > L'utilizzo di Secrets Manager elimina la necessità di archiviare credenziali in testo semplice e fornisce una gestione centralizzata delle credenziali. Per ulteriori informazioni, consulta Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.
6. Per Secret, scegli un segreto esistente da Secrets Manager che contenga le credenziali aggiornate dell'account del servizio di accesso al dominio oppure scegli Crea nuovo segreto per crearne uno.
7. Aggiorna gli altri campi di configurazione di Microsoft Active Directory in base alle esigenze del tuo ambiente.
8. Scegli Aggiorna configurazione per salvare le modifiche.

Per aggiornare la configurazione di SVM Microsoft Active Directory (CLI)

- Per aggiornare la configurazione di Microsoft Active Directory di un SVM FSx for ONTAP, utilizzate il comando update-storage-virtual-machineCLI con il `--active-directory-configuration` parametro, come illustrato nell'esempio seguente.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--active-directory-configuration DomainJoinServiceAccountSecret=secret-arn
```

Controllo dell'accesso ai file

Amazon FSx for 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 degli accessi ai file
- Panoramica delle attività per l'impostazione del controllo dell'accesso ai file

Panoramica del controllo degli accessi 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 aiutarvi 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.

Oltre agli 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 vengono archiviati nel formato di `EVTX` 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 a file e 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 eliminare	ACCESSO ALL'OGGETTO: è stato richiesto un handle per un oggetto (file o directory) con l'intenzione di eliminare	Accesso ai file
564/4660	Eliminazione dell'oggetto	ACCESSO AGLI OGGETTI: 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 gli attributi degli oggetti Object/Write Object/Get Object Attributes/Set	ACCESSO ALL'OGGETTO: tentativo di accesso all'oggetto (lettura, scrittura, attributo get, attributo set). **Note** Per questo evento,	Accesso ai file

ID evento (EVT/EVTX)	Evento	Descrizione	Categoria
		ONTAP verifica solo la prima operazione di lettura e scrittura SMB (riuscita o non riuscita) 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.	
N/A/4664	Collegamento rigido	ACCESSO AGLI OGGETTI: è stato effettuato un tentativo di creare un collegamento fisico	Accesso ai file

ID evento (EVT/EVTX)	Evento	Descrizione	Categoria
ID evento ONTAP N/A/N/A 9999	Rinomina oggetto	ACCESSO AGLI OGGETTI: oggetto rinominato. Questo è un evento ONTAP. Attualmente non è supportato da Windows come singolo evento.	Accesso ai file
ID evento ONTAP N/A/N/A 9998	Scollega oggetto	ACCESSO AGLI OGGETTI: oggetto non collegato. Questo è un evento ONTAP. Attualmente non è supportato da Windows come singolo evento.	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
- READDIR
- WRITE
- IMPOSTA ATTR
- CREATE
- COLLEGAMENTO
- APRI ATTR
- REMOVE

- GETATTR
- VERIFICARE
- VERIFICARE
- RENAME

Panoramica delle attività per l'impostazione del controllo dell'accesso ai file

La configurazione di ONTAP FSx per il controllo dell'accesso ai file prevede 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 una SVM specifica.
3. Abilita il controllo su quella SVM.
4. Configura le politiche di controllo su file e directory.
5. Visualizza i registri degli eventi di controllo dopo che ONTAP FSx li ha emessi.

I dettagli delle attività sono forniti nelle seguenti procedure.

Ripetete le operazioni per qualsiasi altra SVM del file system per cui desiderate abilitare il controllo dell'accesso ai file.

Requisiti di controllo

Prima di configurare e abilitare il controllo su una SVM, è necessario conoscere i seguenti requisiti e considerazioni.

- Il controllo NFS supporta l'audit Access Control Entries (ACEs) designato come typeu, che genera 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 l'audit. ACEs Durante la conversione in bit di modalità, ACLs gli audit vengono ignorati. ACEs Quando si convertono i bit della modalità in ACLs, gli audit non vengono generati. ACEs
- 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 i record di controllo vengono archiviati prima della conversione in un formato di file EVTX o XML.) È necessario assicurarsi che vi sia spazio sufficiente per i volumi di staging negli 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 log di controllo da conservare nella directory di controllo utilizzando il `-rotate-limit` parametro durante la creazione di una configurazione di controllo, che può contribuire a garantire che vi sia spazio disponibile sufficiente per i log di controllo nel volume.

Creazione di configurazioni di controllo su SVMs

Prima di 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 controllo, è necessario abilitarla sulla 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 log e che la directory non contenga collegamenti simbolici. Specificate la directory di destinazione con il parametro. `-destination`

È possibile creare una configurazione di controllo che ruoti i registri di controllo in base alla dimensione del registro o a una pianificazione, come segue:

- Per ruotare i log di controllo in base alla dimensione del registro, utilizzate 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 la SVM denominata `svm1` che controlla le operazioni sui file e gli eventi di accesso e disconnessione CIFS (SMB) (impostazione predefinita) utilizzando la rotazione basata sulla dimensione. Il formato di registro è `EVTX` (predefinito), i log vengono memorizzati nella `/audit_log` directory e avrete un solo 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 log di controllo in base a una pianificazione, utilizzate 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 dei log 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 di 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 log di controllo vengono creati nel `EVTX` formato convertito (impostazione predefinita) o nel formato di file. `XML` 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 delle politiche 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 dei file.

Per ulteriori informazioni sul `vserver audit create` comando, consulta Creare una configurazione di controllo.

Abilitazione del controllo su una SVM

Dopo aver completato la configurazione di controllo, è necessario abilitare il controllo sulla SVM. A tale scopo, utilizzate il seguente comando:

```
vserver audit enable -vserver svm_name
```

Ad esempio, utilizzate il comando seguente per abilitare il controllo sulla SVM denominata. `svm1`

```
vserver audit enable -vserver svm1
```

È possibile disabilitare il controllo degli accessi in qualsiasi momento. Ad esempio, utilizzate il comando seguente per disattivare il controllo sulla SVM denominata. `svm4`

```
vserver audit disable -vserver svm4
```

Quando si disabilita il controllo, la configurazione di controllo non viene eliminata sulla SVM, il che significa che è possibile riattivare il controllo su quella 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 controllare per i tentativi di accesso degli utenti. È possibile configurare le politiche di controllo per monitorare sia i tentativi di accesso riusciti che quelli non riusciti.

È possibile configurare le politiche di controllo SMB e NFS. Le policy di audit SMB e NFS hanno requisiti di configurazione e funzionalità di controllo diversi in base allo stile di sicurezza del volume.

Politiche di controllo su file e directory in stile di sicurezza NTFS

È possibile configurare i criteri di controllo NTFS utilizzando la scheda Sicurezza di Windows o l'ONTAP CLI.

Per configurare le politiche di controllo NTFS (scheda Sicurezza di Windows)

È possibile configurare le politiche di controllo NTFS aggiungendo voci a NTFS associate a un SACLs 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 elenchi di controllo di accesso discrezionali (DACLs) per l'applicazione delle autorizzazioni di accesso a file e cartelle, SACLs per il controllo di file e cartelle o entrambi e. SACLs DACLs

1. Dal menu Strumenti di Windows Explorer, seleziona Map network drive.
2. Completa la casella Map Network Drive:

    a. Scegli una lettera di Drive.

b. Nella casella Cartella, digita il nome del server SMB (CIFS) che contiene la condivisione, contenente i dati che desideri controllare e il nome della condivisione.

c. Scegli Fine.

L'unità selezionata è montata e pronta per essere visualizzata nella finestra di Windows Explorer in cui sono visualizzati i file e le cartelle contenuti nella condivisione.

3. Seleziona il file o la directory per cui desideri abilitare il controllo dell'accesso.
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. Scegli la scheda Controllo.
8. Esegui le azioni desiderate:

Se vuoi...	Effettuare le seguenti operazioni
Imposta il controllo per un nuovo utente o gruppo	1. Scegli Aggiungi. 2. Nella casella Immetti il nome dell'oggetto da selezionare, digita il nome dell'utente o del gruppo che desideri aggiungere. 3. Scegli OK.
Rimuovi il controllo da un utente o un gruppo	1. Nella casella Immetti il nome dell'oggetto da selezionare, seleziona l'utente o il gruppo che desideri rimuovere. 2. Scegli Rimuovi. 3. Scegli OK. 4. Ignorate il resto di questa procedura.
Modifica il controllo per un utente o un gruppo	1. Nella casella Immetti il nome dell'oggetto da selezionare, scegli l'utente o il gruppo che desideri modificare. 2. Scegli Modifica. 3. Scegli OK.

Se state 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 ***object***.

9. Nella casella Applica a, selezionate come desiderate applicare questa voce di controllo.

   Se state configurando il controllo su un singolo file, la casella Applica a non è attiva, poiché per impostazione predefinita è Solo questo oggetto.

10. Nella casella Accesso, selezionate gli elementi da controllare e se desiderate controllare gli eventi riusciti, gli eventi di errore o entrambi.

    - Per controllare gli eventi riusciti, selezionate la casella Operazione riuscita.
    - Per controllare gli eventi di errore, selezionate la casella Fallimento.

    Scegliete le azioni da monitorare per soddisfare i requisiti di sicurezza. Per ulteriori informazioni su questi eventi verificabili, consulta la documentazione di Windows. È possibile controllare i seguenti eventi:

    - Controllo completo
    - Traverse folder /esegui file
    - Elenca cartella/leggi dati
    - Leggi gli attributi
    - Leggi gli attributi estesi
    - Crea file/scrivi dati
    - Crea cartelle/aggiungi dati
    - Attributi di scrittura
    - Scrivi attributi estesi
    - Eliminare sottocartelle e file
    - Eliminazione
    - Autorizzazioni di lettura
    - Modifica le autorizzazioni
    - Assumi la proprietà

11. Se non desideri che l'impostazione di controllo si propaghi ai file e alle cartelle successivi del contenitore originale, seleziona la casella Applica queste voci di controllo solo a oggetti e/o contenitori all'interno di questo contenitore.
12. Scegli Applica.
13. Dopo aver aggiunto, rimosso o modificato le voci di controllo, scegliete OK.

La *object* casella Voce di controllo per si chiude.

14. Nella casella Controllo, scegliete le impostazioni di ereditarietà per questa cartella. Scegliete solo il livello minimo che fornisce gli eventi di controllo che soddisfano i vostri 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 le voci di controllo ereditabili di questo oggetto.
    - Scegliete entrambe le caselle.
    - Non scegliete nessuna delle due scatole.

    Se state impostando SACLs 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 la CLI ONTAP, è possibile configurare le policy di controllo NTFS senza bisogno 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 ntfs sacl add.

Ad esempio, il comando seguente crea una politica di sicurezza denominata in base alla SVM denominata. `p1` `vs0`

```
vserver security file-directory policy create -policy-name p1 -vserver vs0
```

Quindi, il comando seguente applica la politica `p1` di sicurezza alla `vs0` SVM.

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

Politiche di controllo su file e directory in stile di sicurezza UNIX

È possibile configurare il controllo per file e directory in stile di sicurezza UNIX aggiungendo audit ACEs (espressioni di controllo degli accessi) a NFS v4.x (elenchi di controllo degli accessi). ACLs Ciò consente di monitorare determinati eventi di accesso a file e directory NFS per motivi di sicurezza.

> **Note**
>
> Per NFS v4.x, sia quelli discrezionali che quelli di sistema ACEs sono archiviati nello stesso ACL. Pertanto, è necessario fare attenzione quando si aggiunge l'audit ACEs a un ACL esistente per evitare di sovrascrivere e perdere un ACL esistente. L'ordine in cui si aggiunge l'audit ACEs a un ACL esistente non ha importanza.

Per configurare le politiche di controllo UNIX

1. Recuperate l'ACL esistente per il file o la directory utilizzando il comando `nfs4_getfacl` o equivalente.
2. Aggiungi l'audit desiderato. ACEs
3. Applica l'ACL aggiornato al file o alla directory utilizzando il comando `nfs4_setfacl` o equivalente.

   Questo esempio utilizza l'`-a`opzione per concedere 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 registri degli eventi di controllo

È possibile visualizzare i registri degli eventi di controllo salvati nei formati di `XML` file `EVTX` o.

- `EVTX`formato di 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:

  - Visualizzazione 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 visualizzazione dettagliata per visualizzare dati specifici dell'evento.
  - Visualizzazione 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 di 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 registri di controllo, a condizione che si disponga dello schema XML e delle informazioni sulle definizioni dei campi XML.

Configurazione di un server SMB in un gruppo di lavoro

È possibile configurare un server Server Message Block (SMB) in un gruppo di lavoro come alternativa all'aggiunta di una SVM a Microsoft Active Directory quando l'infrastruttura di dominio Microsoft Active Directory non è disponibile. Un gruppo di lavoro è una peer-to-peer rete che utilizza il protocollo SMB e ha solo account e gruppi locali.

Il processo di configurazione di un server SMB come membro di un gruppo di lavoro è costituito dai seguenti:

- Creazione del server SMB su una macchina virtuale di archiviazione (SVM).
- Creazione di utenti e gruppi locali.
- Aggiungere utenti o gruppi locali come membri del gruppo di lavoro.

Tieni presente che i server SMB in modalità gruppo di lavoro non supportano le seguenti funzionalità SMB:

- SMB3 Protocollo di testimonianza
- SMB3 Azioni CA
- SQL su SMB
- Reindirizzamento delle cartelle
- Profili di roaming
- Oggetto della politica di gruppo (GPO)
- Volume Snapshot Service (VSS)

Inoltre, un server SMB in modalità gruppo di lavoro supporta solo l'autenticazione NTLM e non supporta l'autenticazione Kerberos.

Le seguenti procedure illustrano il processo di configurazione di un server SMB su una SVM in un gruppo di lavoro, la creazione di account locali e l'aggiunta di tali account all'appartenenza al gruppo di lavoro. Utilizzerai la NetApp ONTAP CLI dal file system o dall'interfaccia di gestione SVM per implementare queste procedure. Per ulteriori informazioni, consulta Utilizzo della CLI NetApp ONTAP.

Argomenti

- Creazione di un server SMB in un gruppo di lavoro
- Creazione di un account utente locale sul server SMB
- Creazione di gruppi locali sul server SMB
- Aggiungere utenti locali al gruppo locale

Creazione di un server SMB in un gruppo di lavoro

È possibile utilizzare il vserver cifs createONTAP CLIcomando per creare un server SMB sulla SVM e specificare il gruppo di lavoro a cui appartiene.

Prima di iniziare

L'SVM e i volumi (e le interfacce) utilizzati per fornire i dati devono essere stati configurati per consentire il protocollo SMB.

LIFs Devono essere in grado di connettersi ai server DNS configurati sull'SVM. Potrebbe essere richiesta una licenza CIFS sul file system, tuttavia non è richiesta una licenza CIFS se il server SMB verrà utilizzato solo per l'autenticazione.

Per creare un server SMB in un gruppo di lavoro

1. Per accedere alla ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 il server SMB in un gruppo di lavoro:

```
FSxIdabcde123456::> vserver cifs create -vserver vserver_name -cifs-
server cifs_server_name -workgroup workgroup_name [-comment workgroup_description]
```

Il comando seguente crea il server SMB `smb_server01` nel gruppo di lavoro: `workgroup01`

```
FSxIdabcde123456::> vserver cifs create -vserver svm1 -cifs-server SMB_SERVER01 -
workgroup workgroup01
```

Se si è connessi alla porta di gestione dell'SVM, non è necessario specificare a. `-vserver`

3. Verificare la configurazione del server SMB utilizzando il `vserver cifs show` comando.

Nell'esempio seguente, l'output del comando mostra che un server SMB denominato `smb_server01` è stato creato su SVM `svm1` nel gruppo di lavoro: `workgroup01`

```
FSxIdabcde123456::> vserver cifs show -vserver svm1

                                               Vserver: svm1
                            CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                     Fully Qualified Domain Name: -
                             Organizational Unit: -
    Default Site Used by LIFs Without Site Membership: -
                                     Workgroup Name: workgroup01
                                Authentication Style: workgroup
                  CIFS Server Administrative Status: up
                             CIFS Server Description:
                             List of NetBIOS Aliases: -
```

Creazione di un account utente locale sul server SMB

È possibile creare un account utente locale che può essere utilizzato per autorizzare l'accesso ai dati contenuti nella SVM tramite una connessione SMB. È inoltre possibile utilizzare account utente locali per l'autenticazione durante la creazione di una sessione SMB. La funzionalità utente locale è abilitata per impostazione predefinita al momento della creazione dell'SVM. Quando si crea un account utente locale, è necessario specificare un nome utente e specificare l'SVM a cui associare l'account.

Per creare account utente locali sul server SMB

1. Crea l'utente locale utilizzando il comando vserver cifs users-and-groups local-user createONTAPCLI:

   ```
   vserver cifs users-and-groups local-user create -vserver svm_name -user-
   name user_name optional_parameters
   ```

   I seguenti parametri opzionali potrebbero essere utili:

   - `-full-name`— Il nome completo dell'utente.
   - `-description`— Una descrizione per l'utente locale.
   - `-is-account-disabled {true|false}`— Speciifica se l'account utente è abilitato o disabilitato. Se questo parametro non è specificato, l'impostazione predefinita è abilitare l'account utente.

   Il comando richiede la password dell'utente locale.
2. Immettere una password per l'utente locale, quindi confermare la password.
3. Verifica che l'utente sia stato creato correttamente:

   ```
   vserver cifs users-and-groups local-user show -vserver svm_name
   ```

L'esempio seguente crea un utente localeSMB_SERVER01\sue, con un nome completoSue Chang, associato a SVM: svm1

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user create -vserver svm1
 -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user show
Vserver  User Name                  Full Name  Description
-------- -------------------------- ---------- -------------
svm1     SMB_SERVER01\Administrator            Built-in administrator account
svm1     SMB_SERVER01\sue           Sue Chang
```

Creazione di gruppi locali sul server SMB

È possibile creare gruppi locali che possono essere utilizzati per autorizzare l'accesso ai dati associati alla SVM tramite una connessione SMB. È inoltre possibile assegnare privilegi che definiscono i diritti o le capacità utente di un membro del gruppo.

La funzionalità dei gruppi locali è abilitata per impostazione predefinita al momento della creazione dell'SVM. Quando si crea un gruppo locale, è necessario specificare un nome per il gruppo e specificare l'SVM a cui associare il gruppo. È possibile specificare un nome di gruppo con o senza il nome di dominio locale e, facoltativamente, specificare una descrizione per il gruppo locale. Non è possibile aggiungere un gruppo locale a un altro gruppo locale.

Per creare un gruppo locale sul server SMB

1. creare il gruppo locale utilizzando il comando vserver cifs users-and-groups local-group createONTAPCLI.

   ```
   vserver cifs users-and-groups local-group create -vserver svm_name -group-
   name group_name [-description local_group_description
   ```

   È utile includere una descrizione per il gruppo locale.
2. Verifica che il gruppo sia stato creato correttamente:

   ```
   vserver cifs users-and-groups local-group show -vserver svm_name
   ```

L'esempio seguente crea un gruppo locale `SMB_SERVER01\engineering` associato a SVM: `svm1`

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group create -vserver svm1 -
group-name SMB_SERVER01\engineering
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group show -vserver svm1

Vserver          Group Name                  Description
---------------- --------------------------- ----------------------------
svm1             BUILTIN\Administrators      Built-in Administrators group
svm1             BUILTIN\Backup Operators    Backup Operators group
svm1             BUILTIN\Guests              Built-in Guests group
svm1             BUILTIN\Power Users         Restricted administrative privileges
svm1             BUILTIN\Users               All users
```

```
svm1            SMB_SERVER01\engineering
```

Aggiungere utenti locali al gruppo locale

È possibile gestire l'appartenenza ai gruppi locali aggiungendo e rimuovendo utenti locali o di dominio oppure aggiungendo e rimuovendo gruppi di dominio. Ciò è utile se desideri controllare l'accesso ai dati in base ai controlli di accesso posizionati sul gruppo o se desideri che gli utenti dispongano dei privilegi associati a quel gruppo. Se non desideri più che un utente locale, un utente di dominio o un gruppo di dominio disponga di diritti di accesso o privilegi basati sull'appartenenza a un gruppo, puoi rimuovere il membro dal gruppo.

Quando aggiungi membri a un gruppo locale, tieni presente quanto segue:

- Non puoi aggiungere utenti al gruppo speciale Everyone.
- Non è possibile aggiungere un gruppo locale a un altro gruppo locale.
- Per aggiungere un utente o un gruppo di dominio a un gruppo locale, ONTAP deve essere in grado di risolvere il nome in un SID.

Quando rimuovi membri da un gruppo locale, tieni presente quanto segue:

- Non puoi rimuovere membri dal gruppo speciale Everyone.
- Per rimuovere un membro da un gruppo locale, ONTAP deve essere in grado di risolvere il suo nome in un SID.

È necessario disporre del `fsxadmin` ruolo necessario per eseguire i comandi utilizzati in questa procedura. Per ulteriori informazioni, consulta ONTAPruoli e utenti.

Per gestire l'appartenenza al gruppo locale

- Aggiungi o rimuovi un membro da un gruppo utilizzando i comandi CLI vserver cifs users-and-groups local-group add-memberse vserver cifs users-and-groups local-group ONTAP remove-members.
  - Per aggiungere membri a un gruppo di lavoro:

```
vserver cifs users-and-groups local-group add-members -vserver svm_name -group-
name group_name -member-names name[,...]
```

È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da aggiungere al gruppo locale specificato.

- Per visualizzare i membri di un gruppo di lavoro:

```
vserver cifs users-and-groups local-group show-members -vserver svm_name -group-
name group_name
```

- Per rimuovere membri da un gruppo di lavoro:

```
vserver cifs users-and-groups local-group remove-members -vserver svm_name -
group-name group_name -member-names name[,...]
```

È possibile specificare un elenco delimitato da virgole di utenti locali, utenti di dominio o gruppi di dominio da rimuovere dal gruppo locale specificato.

L'esempio seguente aggiunge un utente locale `SMB_SERVER01\sue` al gruppo locale su SVM: `SMB_SERVER01\engineering` `svm1`

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group add-members -vserver svm1
 -group-name SMB_SERVER01\engineering -member-names SMB_SERVER01\sue
```

L'esempio seguente rimuove l'utente locale `SMB_SERVER01\sue` e `SMB_SERVER01\james` dal gruppo locale `SMB_SERVER01\engineering` su `svm1` SVM:

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group remove-
members -vserver svm1 -group-name SMB_SERVER01\engineering -member-names
 SMB_SERVER01\sue,SMB_SERVER01\james
```

L'esempio seguente elenca i membri del gruppo `SMB_SERVER01\engineering` locale:

```
FsxIdabcdef01234::> vserver cifs users-and-groups local-group show-members -
vserver svm_name -group-name group_name

           Vserver: svm1
      Domain Name: SMB_SERVER01
       Group Name: SMB_SERVER01\engineering
      Member Name: SMB_SERVER01\anita
                   SMB_SERVER01\james
```

```
                    SMB_SERVER01\liang
```

Monitoraggio dei dettagli di configurazione della macchina virtuale di archiviazione (SVM)

Puoi visualizzare FSx le macchine virtuali di archiviazione ONTAP attualmente presenti sul tuo file system utilizzando la FSx console Amazon AWS CLI, e l' FSx API Amazon.

Per visualizzare una macchina virtuale di archiviazione 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 tutto ciò che è presente SVMs nel tuo account. Regione AWS

Eliminazione di macchine virtuali di archiviazione (SVM)

Puoi eliminare un SVM FSx for ONTAP solo utilizzando la FSx console Amazon AWS CLI, il e l'API. Prima di poter eliminare una SVM, devi prima eliminare 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 FSx console Amazon 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 macchine SVMs 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 volumi.
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, utilizza il comando delete-storage-virtual-machineCLI (o l'operazione API DeleteStorageVirtualMachineequivalente), come illustrato nell'esempio seguente.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

Gestione dei FSx volumi ONTAP

Ogni macchina virtuale di archiviazione (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 archiviazione

LUNs iSCSI (). I volumi sono dotati di thin provisioning, il che significa che consumano la capacità di archiviazione 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 simultaneo NFS e SMB) allo stesso volume.

Puoi creare volumi utilizzando Console di gestione AWS, AWS CLI, l' FSx API Amazon oNetApp Console. 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 o NTFS): 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 conveniente.
- 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 tuoi volumi ai backup utilizzando questa opzione. Puoi impostare questa opzione utilizzando l' FSx API AWS CLI o Amazon.

Argomenti

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 FSx console Amazon AWS CLI, e l' FSx API Amazon.

- FlexVoli volumi offrono l'esperienza più semplice per i file system con una coppia ad alta disponibilità (HA), quindi sono lo stile di volume predefinito per i file system di prima generazione e i file system di seconda generazione con una coppia HA. 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 di seconda

generazione con più di una coppia HA. 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 per ONTAP assegna otto componenti a un volume per coppia HA. FlexGroup

Quando crei il FlexGroup volume, le sue dimensioni vengono suddivise 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 dei dati e tra i componenti. I/O 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 a quando i componenti non sono bilanciati. 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-timeimmagine 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 puoi creare utilizzando la FSx console Amazon AWS CLI, e l' FSx API Amazon.

- 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

Quando si crea un volume FSx per ONTAP, è possibile scegliere tra due stili di sicurezza: Unix e NTFS. 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 ONTAP FSx 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 FSx console Amazon, 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 dei volumi.

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 NFS v4.x. ACLs
- NTFS: scegli questo stile di sicurezza se il file system è gestito da un amministratore 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 il tipo di autorizzazione utilizzato su file e directory è NTFS. ACLs

Creazione di volumi

Puoi creare un volume FSx per ONTAP FlexVol o un FlexGroup volume utilizzando la FSx console Amazon, l' FSx API Amazon AWS CLI, oltre all'interfaccia a riga di comando (CLI) NetApp ONTAP e all'API REST.

Per creare un FlexVol volume (console)

> **Note**
>
> Lo stile di sicurezza del volume viene impostato automaticamente sullo stile di sicurezza del volume principale.

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli Volumi.
3. Selezionare Create volume (Crea volume).
4. Per 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) su questo volume. Per ulteriori informazioni, consulta Efficienza dello storage.
- Per lo stile di sicurezza Volume, scegli tra Unix (Linux) e NTFS 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 Comprendere la conformità SnapLock eComprendere SnapLock Enterprise. Per ulteriori informazioni su SnapLock, consultare 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 più coppie HA solo utilizzando la FSx console Amazon. Per creare FlexVol volumi per file system con più coppie HA, usa l' AWS CLI FSx API Amazon o gli strumenti di NetApp gestione.

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli Volumi.
3. Selezionare Create volume (Crea volume).
4. Per 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 2.400 tebibyte (TiB) per coppia HA. Ad esempio, un file system con 12 coppie ad alta disponibilità (HA) avrebbe una dimensione di volume minima di 9.600 GiB e una dimensione massima di 20.480 TiB.
   - 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 Efficienza dello storage.

- Per lo stile di sicurezza Volume, scegli tra Unix (Linux) e NTFS 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 Comprendere la conformità SnapLock eComprendere SnapLock Enterprise. Per ulteriori informazioni su SnapLock, consultare 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 CLI create-volume (o l'operazione API CreateVolumeequivalente), 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 dei volumi

Puoi aggiornare la configurazione di un volume FSx for ONTAP utilizzando la FSx console Amazon, l'API Amazon e l' FSx API Amazon AWS CLI, oltre all'interfaccia a riga di comando (CLI) NetApp ONTAP e all'API REST. Puoi modificare le seguenti proprietà di un volume FSx for ONTAP esistente:

- Nome 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' FSx API AWS CLI e Amazon)

Per ulteriori informazioni, consulta Gestione dei FSx volumi ONTAP.

Per aggiornare la configurazione di un volume (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Vai 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 `/vol5`.
7. Per le dimensioni del volume, puoi aumentare o diminuire le dimensioni del volume entro l'intervallo specificato nella FSx console Amazon. 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) sul volume oppure scegli Disabilitato per disabilitarle.
9. Per la politica di suddivisione in più livelli del pool di capacità, scegli una nuova politica di tiering del pool di storage per il volume, che può essere Auto (impostazione predefinita), Solo Snapshot, Tutto 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 a NTFS o UNIX ACLs 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 API UpdateVolumeequivalente), 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
```

Volumi in espansione FlexGroup

Puoi aggiungere ulteriori volumi costituenti al tuo FlexGroup volume con il `volume expand` comando nella ONTAP CLI. Si tratta di una procedura consigliata dopo l'aggiunta di coppie ad alta disponibilità (HA) al file system, in quanto garantisce il FlexGroup bilanciamento del volume.

Prima di espandere il FlexGroup volume, considera i seguenti punti:

- Tutti i volumi FlexGroup's costituenti hanno la stessa capacità di archiviazione. Quando si espande il FlexGroup volume con componenti aggiuntivi, ogni componente ha le stesse dimensioni dei componenti esistenti. Pertanto, assicuratevi che ogni aggregato disponga di spazio sufficiente prima di aggiungere i componenti.
- AWS raccomanda di mantenere otto volumi costituenti per aggregato per ogni volume. FlexGroup Otto volumi costituenti per aggregato massimizzano il parallelismo dei FlexGroup volumi e offrono le prestazioni ottimali per il carico di lavoro. In genere, consigliamo di espandere il FlexGroup volume con componenti aggiuntivi solo se si aggiungono coppie HA. Questo è l'unico scenario in cui sarebbe necessario aggiungere componenti per mantenere otto componenti per aggregato.
- Se il FlexGroup volume è in una SnapMirror relazione, entrambi i FlexGroup volumi di origine e di destinazione devono avere lo stesso numero di componenti. In caso contrario, SnapMirror i trasferimenti falliranno. SnapMirroropera a livello di componente e trasferisce i dati tra ogni singolo componente. Pertanto, se si espande un FlexGroup volume con volumi costituenti aggiuntivi, è necessario espandere anche manualmente qualsiasi volume che sia in relazione con esso. SnapMirror
- Quando si espande un FlexGroup volume con componenti aggiuntivi, tutte le copie istantanee esistenti diventano copie «parziali». Le copie parziali non possono essere ripristinate, ma possono

essere sfogliate e i singoli file possono essere ripristinati. Inoltre, ciò comporta la perdita di qualsiasi incrementalità per i FSx backup, AWS i backup o le relazioni di Amazon. SnapMirror

- Non puoi rimuovere i volumi costituenti dopo averli aggiunti.

Aggiungere componenti di volume FlexGroup

Puoi usare la ONTAP CLI per aggiungere volumi costituenti al tuo volume. FlexGroup

Per aggiungere componenti di volume FlexGroup

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system FSx Amazon 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 volume expand ONTAP CLI per espandere il FlexGroup volume con componenti aggiuntivi. Sostituisci i valori seguenti:

   - `svm_name`con il nome della macchina virtuale di archiviazione (SVM) che ospita il FlexGroup volume (ad esempio,). `svm1`
   - `vol_name`con il nome del FlexGroup volume che si desidera espandere (ad esempio,`vol1`).
   - `aggregates`con un elenco di aggregati separati da virgole a cui si desidera aggiungere FlexGroup i volumi costituenti. Ad esempio, per un singolo aggregato o `aggr1` per più aggregati. `aggr1,aggr2`
   - `constituent_per_aggregate`con il numero di componenti aggiuntivi che si desidera aggiungere a ciascuno dei componenti specificati. `aggregates` È necessario aggiungere solo un numero sufficiente di componenti per garantire che il FlexGroup volume abbia un numero equilibrato di componenti tra gli aggregati su cui risiede.

   ```
   ::> volume expand -vserver svm_name -volume vol_name -aggr-list aggregates -aggr-
   list-multiplier constituents_per_aggregate
   ```

> **Important**
>
> Non puoi rimuovere i FlexGroup componenti dopo averli aggiunti, quindi controlla i tuoi input prima di eseguire il comando precedente.

Spostamento di volumi tra aggregati

Quando si aggiungono coppie ad alta disponibilità (HA) al file system, è necessario ribilanciare i dati esistenti spostando i volumi nei nuovi aggregati. Per spostare un volume tra gli aggregati, puoi usare il `volume move` comando nella CLI di ONTAP.

Prima di utilizzare il `volume move` comando, considera i seguenti punti:

- L'utilizzo del `volume move` comando può influire sulle prestazioni in quanto consuma le risorse di rete e disco del file system. Pertanto, si consiglia di spostare i volumi tra gli aggregati durante i periodi di scarsa attività. In alternativa, è possibile ridurre l'utilizzo del throughput di rete e del disco sul file system a non più del 50% durante lo spostamento dei volumi.
- Per ridurre l'impatto sulle prestazioni sul file system, consigliamo di spostare un singolo volume tra due coppie e aggregati HA alla volta. Ad esempio, se il file system ha quattro coppie HA, consigliamo di spostare due volumi alla volta (supponendo che i volumi non vengano spostati da o verso le stesse coppie HA). ONTAP supporta lo spostamento di fino a otto volumi contemporaneamente su ciascuna coppia HA, ma spostamenti di volume più simultanei ridurranno le prestazioni sia del client I/O che di eventuali spostamenti di volume in corso.
- Tutti i dati archiviati sul livello SSD sul volume interessato vengono spostati fisicamente su un diverso set di dischi su un file server diverso. Questa operazione viene eseguita in background e richiede tempo. La velocità di trasferimento dipende dalla capacità di trasmissione del file system e dalla quantità di attività sul file system. Tuttavia, lo spostamento del volume può essere limitato. Per ulteriori informazioni, consulta Limitazione dei movimenti di volume.
- I dati archiviati nel pool di capacità non vengono spostati fisicamente perché le coppie HA condividono lo stesso storage del pool di capacità. ONTAPSposta invece i metadati che descrivono in modo completo ogni blocco del pool di capacità (una mossa logica). Tieni presente che i metadati dei file vengono sempre archiviati sul livello SSD. Per ulteriori informazioni, consulta Suddivisione dei volumi di dati su più livelli.

Fasi dello spostamento di un volume

Un'operazione di spostamento di un volume prevede due fasi: la fase di replica e la fase di cutover. Durante la fase di replica, i dati esistenti vengono replicati nel nuovo aggregato del volume. Durante la fase di cutover, ONTAP tenta un trasferimento rapido finale al nuovo aggregato del volume. Ciò include il trasferimento di tutti i dati che sono stati scritti durante la fase di trasferimento e il reindirizzamento del nuovo traffico verso il nuovo aggregato del volume. Per impostazione predefinita, la finestra intermedia dura 30 secondi e si interrompe tutto al volume desiderato. I/O Se ONTAP non è in grado di eseguire tutti questi passaggi durante la finestra di cutover, fallirà. Per impostazione predefinita, ONTAP cercherà di eseguire il taglio tre volte consecutive. Se tutti e tre i tentativi consecutivi falliscono, ONTAP riproverà una volta all'ora fino a quando non avrà successo. È possibile ridurre il carico sul file system per garantire il successo della fase di cutover riducendo o sospendendo il I/O traffico verso il volume prima dell'inizio della fase di cutover.

Il volume iniziale si sposta

Per avviare un movimento di volume

1. Per accedere alla CLI NetApp ONTAP, stabilisci una sessione SSH sulla porta di gestione del file system FSx Amazon 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 volume move start ONTAP CLI. Sostituisci i valori seguenti:

   - `vserver_name`con il nome della SVM che ospita il volume che stai spostando.
   - `volume_name`con il nome del componente del volume (ad esempio,). `vol1__0001`
   - `aggregate_name`con il nome dell'aggregato di destinazione per il volume.
   - `-enforce-network-throttling`per limitare la velocità effettiva totale del volume move. Questo è facoltativo.

   ```
   ::> volume move start -vserver svm_name -volume volume_name --destination-
   aggregate 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.
```

Important

Lo spostamento dei volumi consuma risorse di rete e disco per i file server di origine e di destinazione. Pertanto, le prestazioni del carico di lavoro possono essere influenzate da eventuali spostamenti di volume in corso. Inoltre, il I/O traffico verso il volume verrà temporaneamente sospeso durante la fase di cutover del trasferimento del volume.

Monitoraggio dei movimenti di volume

Per monitorare un movimento di volume

- 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: aggr1
Source Node: FsxId01234567890abcdef-01
Move State: healthy
```

L'output del comando mostra il tempo stimato per completare lo spostamento. Al termine, `Move phase` mostrerà lo `completed` stato.

Mantenimento di FlexGroup volumi equilibrati

Affinché il carico di lavoro funzioni in modo ottimale, è necessario che i FlexGroup volumi si estendano su tutti gli aggregati e abbiano un numero pari di volumi costituenti per aggregato. Consigliamo di avere otto componenti per aggregato. Per il ribilanciamento dei volumi, prendete in considerazione i seguenti scenari: FlexGroup

- Spostamento FlexGroup dei componenti tra aggregati esistenti: se spostate un volume FlexGroup's costituente su un altro aggregato di un aggregato altrimenti bilanciatoFlexGroup, dovreste spostare un altro componente meno utilizzato nell'aggregato originale. In questo modo si garantisce un numero pari di componenti per aggregato. FlexGroup

  Spostamento FlexGroup dei costituenti in nuovi aggregati dopo l'aggiunta di coppie HA: se spostate i volumi di un FlexGroup's costituente in nuovi aggregati dopo aver aggiunto coppie HA, dovreste espanderli FlexGroup con altri costituenti sugli aggregati che hanno perso i costituenti. In questo modo si garantisce un numero pari di componenti per aggregato. FlexGroup Per ulteriori informazioni, consulta the section called “FlexGroupVolumi in espansione”.

Limitazione dei movimenti di volume

Se desideri limitare la larghezza di banda di uno spostamento di volume sul tuo file system, puoi aggiungere l'`-enforce-network-throttling`opzione all'inizio dell'operazione.

> **Note**
>
> L'utilizzo di questa opzione influisce sui trasferimenti di dati di SnapMirror replica in entrata per il file system. Tieni traccia di come configuri le opzioni di replica del tuo file system perché non puoi visualizzarle dopo averle impostate.

Per limitare un movimento di volume

1. L'acceleratore utilizza l'acceleratore di replica globale. Per impostare l'acceleratore di replica globale, utilizzate il seguente comando nella CLI. ONTAP

```
::> options -option-name replication.throttle.enable on
```

2. Specificate la larghezza di banda totale massima che può essere utilizzata dalla replica, sostituendo la seguente opzione:

   - `kbs_throttle`con il throughput massimo desiderato da utilizzare per qualsiasi replica (compresi SnapMirror gli spostamenti di volume), in kilobyte al secondo.

```
::> options -option-name replication.throttle.incoming.max_kbs kbs_throttle
::> options -option-name replication.throttle.outgoing.max_kbs kbs_throttle
```

Monitoraggio dei volumi

Puoi vedere i volumi attualmente presenti sul tuo file system utilizzando la FSx console Amazon AWS CLI, l' FSx API Amazon e SDKs.

Per monitorare 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

```
$ aws fsx describe-volumes
{
    "Volumes": [
        {
            "CreationTime": "2024-03-04T20:17:44+00:00",
            "FileSystemId": "fs-abcdef0123a0bb087",
            "Lifecycle": "CREATED",
            "Name": "SVM8_ext_root",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
                "JunctionPath": "/",
                "SecurityStyle": "NTFS",
                "SizeInMegabytes": 1024,
                "StorageEfficiencyEnabled": false,
```

```
                "StorageVirtualMachineId": "svm-01234567890abcdef",
                "StorageVirtualMachineRoot": true,
                "TieringPolicy": {
                    "Name": "NONE"
                },
                "UUID": "42ce3de0-da64-11ee-a22d-7f7cdfb8d381",
                "OntapVolumeType": "RW",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
                "VolumeStyle": "FLEXVOL",
                "AggregateConfiguration": {
                    "Aggregates": [
                        "aggr1"
                    ]
                },
                "SizeInBytes": 1073741824
            },
            "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcdef0123a0bb087/fsvol-abcdef0123456789a",
            "VolumeId": "fsvol-abcdef0123456789a",
            "VolumeType": "ONTAP"
        }
    ]
}
```


Visualizzazione di volumi offline

Non è possibile creare o eliminare backup di volumi quando il volume di origine è offline. È possibile utilizzare il comando `volume show`ONTAPCLI per determinare lo stato corrente di un volume.

```
volume show -vserver svm-name
```

Per informazioni sull'accesso alla ONTAP CLI sul file system, consulta. Utilizzo della CLI NetApp ONTAP

```
FsxIdabc12345::> volume show -vserver vs1
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
vs1       vol1         aggr1        online     RW          2GB      1.9GB    5%
vs1       vol1_dr      aggr0_dp     online     DP        200GB    160.0GB   20%
vs1       vol2         aggr0        online     RW        150GB    110.3GB   26%
```

```
vs1       vol2_dr      aggr0_dp     online     DP         150GB    110.3GB   26%
vs1       vol3         aggr1        online     RW         150GB    120.0GB   20%
vs1       vol3_dr      aggr1_dp     online     DP         150GB    120.0GB   20%
vs1       vol4         aggr1        online     RW         200GB    159.8GB   20%
7 entries were displayed.
```

Per riportare online un volume offline, utilizzate il comando `volume online`ONTAPCLI, come illustrato nell'esempio seguente. Se esiste solo un SVM (Vserver), non è necessario specificare il parametro. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

Eliminazione di volumi

Puoi eliminare un volume FSx for ONTAP utilizzando la FSx console Amazon, l' FSx API Amazon AWS CLI, oltre all'interfaccia a riga di comando (CLI) NetApp ONTAP e all'API REST.

Prima di eliminare un volume, assicurati che nessuna applicazione acceda ai dati del volume che desideri eliminare.

> **Important**
>
> Puoi eliminare i volumi utilizzando la FSx console Amazon, l'API o la CLI solo se il volume ha i FSx backup Amazon abilitati.

Esecuzione di un backup finale del volume

Quando elimini un volume utilizzando la FSx console Amazon, hai la possibilità di eseguire un backup finale del volume. Come best practice, ti consigliamo di scegliere di eseguire un backup finale. 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.

Per ulteriori informazioni sui backup di volume, consulta. Protezione dei dati con backup di volume

Per eliminare un volume (console)

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

2. Nel riquadro di navigazione a sinistra, scegli File system, quindi scegli il 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. (solo SnapLock Enterprise volumi) Per Bypass SnapLock Enterprise Retention, scegli Sì.
7. 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.
8. Conferma l'eliminazione del volume inserendo delete nel campo Conferma eliminazione.
9. 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 API DeleteVolumeequivalente), come illustrato nell'esempio seguente.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

Eliminazione di volumi SnapLock

Questa sezione spiega come eliminare un SnapLock volume.

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 file Account AWS che contiene SnapLock Enterprise i nostri Compliance volumi AWS e FSx per ONTAP, sospendi il tuo account per 90 giorni lasciando intatti i dati. Se non riapri l'account durante 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 necessarie. Per eliminare un volume SnapLock Enterprise utilizzando la ONTAP CLI, è necessario disporre del `fsxadmin` ruolo. Per ulteriori informazioni, consulta Ruoli e utenti degli amministratori del file system.

Per eliminare un volume SnapLock Enterprise che contiene dati WORM con una politica di conservazione attiva utilizzando la FSx console Amazon, la CLI o l'API FSx Amazon, devi disporre `fsx:BypassSnapLockEnterpriseRetention` dell'autorizzazione IAM.

> **Warning**
>
> Il periodo minimo di conservazione per un volume di log SnapLock di 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.

Creazione di un LUN iSCSI

Questo processo descrive come creare un LUN iSCSI su un file system Amazon FSx for NetApp ONTAP utilizzando il comando CLI. NetApp ONTAP lun create Per ulteriori informazioni, consulta il Documentation lun createCenter. NetApp ONTAP

> **Note**
>
> Il protocollo iSCSI non è supportato per i file system con più di sei coppie HA.

Questo processo presuppone che sul file system sia già stato creato un volume. Per ulteriori informazioni, consulta Creazione di volumi.

1. Per accedere alla ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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. Create un LUN utilizzando il lun create NetApp CLI comando, 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 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, `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
```

Fasi successive

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 Provisioning di iSCSI per Linux o Provisioning di iSCSI per Windows.

Ottimizzazione delle prestazioni con le finestre di FSx manutenzione di Amazon

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 ti FSx 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. Quando vengono applicate le patch, ogni file server del file system viene patchato uno alla volta e ogni file server impiega in genere fino a un'ora per ricevere la patch. Prima che venga applicata la patch a qualsiasi file server all'interno di una coppia HA, il file system esegue automaticamente il failover sul partner HA dei file server, il che può comportare una breve pausa di I/O (meno di 60 secondi) per qualsiasi I/O diretto verso quella coppia HA. Il file system eseguirà quindi il failback, il che potrebbe causare un'altra breve pausa di I/O (meno di 60 secondi). Si sceglie l'ora di inizio della finestra di manutenzione durante la creazione del file system. Se non scegli una finestra, ne viene assegnata automaticamente una.

> **Important**
>
> Per garantire la corretta applicazione delle patch al file system, FSx for ONTAP metterà online tutti i volumi offline per tutta la durata del processo di applicazione delle patch. Tutti i volumi che Amazon FSx riporterà online non saranno accessibili ai clienti.

FSx for ONTAP consente di regolare la finestra di manutenzione in base alle esigenze, per adattarla al carico di lavoro e ai requisiti operativi. È possibile spostare la finestra di manutenzione con la frequenza necessaria, a condizione che tale periodo 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 FSx gestione Amazon AWS CLI, AWS l'API o una delle altre AWS SDKs per modificare la finestra di manutenzione dei tuoi file system.

Per modificare la finestra di manutenzione settimanale (console)

1. Apri la FSx console Amazon 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)

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 throughput del file system in qualsiasi momento. Tieni presente che il file system richiede una configurazione specifica per raggiungere la massima capacità di throughput. Ad esempio, per fornire il 4% della capacità GBps di throughput per un file system di prima generazione, 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 con cui 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 Performance.

Quando modifichi la capacità di throughput del tuo file system, Amazon FSx spegne 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 “Aggiornamento delle 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 tuo 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. Puoi utilizzare le CloudWatch metriche per determinare quali di queste dimensioni modificare per migliorare le prestazioni. Per ulteriori informazioni, consulta the section called “Monitoraggio nella FSx console Amazon”.

Come vengono gestite le richieste concorrenti

Per i file system di prima generazione, è possibile richiedere un aggiornamento della capacità di throughput appena prima dell'inizio della capacità di archiviazione SSD e del flusso di lavoro di aggiornamento IOPS assegnato o mentre è in corso. La sequenza di FSx gestione delle due richieste da parte di Amazon è la seguente:

- Se invii contemporaneamente un SSD/IOPS aggiornamento e un aggiornamento della capacità di throughput, entrambe le richieste vengono accettate. All' SSD/IOPS aggiornamento viene assegnata la priorità prima dell'aggiornamento della capacità di throughput.
- Se si invia un aggiornamento della capacità di throughput mentre è in corso un SSD/IOPS aggiornamento, la richiesta di aggiornamento della capacità di throughput viene accettata e messa in coda dopo l'SSD/IOPS update. The throughput capacity update starts after SSD/IOPSaggiornamento (sono disponibili nuovi valori) e durante la fase di ottimizzazione. Questa operazione richiede in genere meno di 10 minuti.
- Se si invia un SSD/IOPS aggiornamento mentre è in corso un aggiornamento della capacità di throughput, la richiesta di aggiornamento dello SSD/IOPS storage viene accettata e messa in coda

per iniziare dopo il completamento dell'aggiornamento della capacità di throughput (è disponibile una nuova capacità di throughput). Questa operazione richiede in genere 20 minuti.

Quando richiedi un aggiornamento della capacità di throughput per i file system di seconda generazione, considera i seguenti punti:

- È necessario attendere almeno sei ore tra l'aggiornamento della capacità di throughput per i file system di seconda generazione.
- Il periodo di recupero della capacità di throughput è condiviso con la scalabilità. SSD/IOPS
- La scalabilità e SSD/IOPS la scalabilità della capacità di throughput non possono essere eseguite contemporaneamente o messe in coda mentre entrambe sono in corso.
- Non è possibile aggiungere coppie ad alta disponibilità (HA) insieme o mentre è in corso il ridimensionamento o la scalabilità della capacità di throughput. SSD/IOPS Tuttavia, l'aggiunta di coppie HA non ha lo stesso tempo di recupero rispetto alla scalabilità e alla scalabilità della capacità di throughput SSD/IOPS . Per ulteriori informazioni, consulta Aggiungere coppie ad alta disponibilità (HA).

Per ulteriori informazioni sullo storage SSD e sugli aggiornamenti IOPS forniti, consulta. Gestione della capacità di archiviazione

Aggiornamento della capacità di throughput

Puoi modificare la capacità di throughput di un file system utilizzando la FSx console Amazon, AWS Command Line Interface (AWS CLI) o l' FSx API Amazon.

> **Note**
>
> È necessario attendere almeno sei ore tra l'aggiornamento della capacità di throughput per i file system di seconda generazione.

Per modificare la capacità di throughput di un file system (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il 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.
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 FSx console Amazon AWS 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`all'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 FSx console Amazon AWS CLI, e l'API. Per ulteriori informazioni, consulta Monitoraggio delle variazioni della capacità di throughput.

Monitoraggio delle variazioni della capacità di throughput

Puoi monitorare l'avanzamento di una modifica della capacità di throughput utilizzando la FSx console Amazon, l'API e il AWS CLI.

Monitoraggio delle variazioni della capacità di throughput 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 throughput di 128 MBps e una capacità di throughput di destinazione di 256. MBps

```
.
.
```

```
.
    "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`

Gestione delle condivisioni SMB

Per gestire le condivisioni di file SMB sul tuo FSx file system Amazon, puoi utilizzare la GUI 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 archiviazione (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 System Manager con NetApp NetApp Console.

Per connettere cartelle condivise al tuo FSx file system Amazon

1. Avvia l'istanza Amazon EC2 e collegala a Microsoft Active Directory a cui è collegato FSx il file system Amazon. 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 FSx console Amazon, 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 tuo FSx file system Amazon nell'elenco dello strumento Cartelle condivise.

Ora che Shared Folders è connesso al tuo FSx file system Amazon, 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 vedere le condivisioni attive per il tuo FSx file system Amazon. 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.
  - Utilizzo della 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 a destra 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.

Gestione FSx delle risorse ONTAP tramite applicazioni NetApp

Oltre a, e AWS API and Console di gestione AWS AWS CLI SDKs, puoi anche utilizzare questi strumenti e applicazioni di NetApp gestione per gestire le tue risorse FSx for ONTAP:

Argomenti

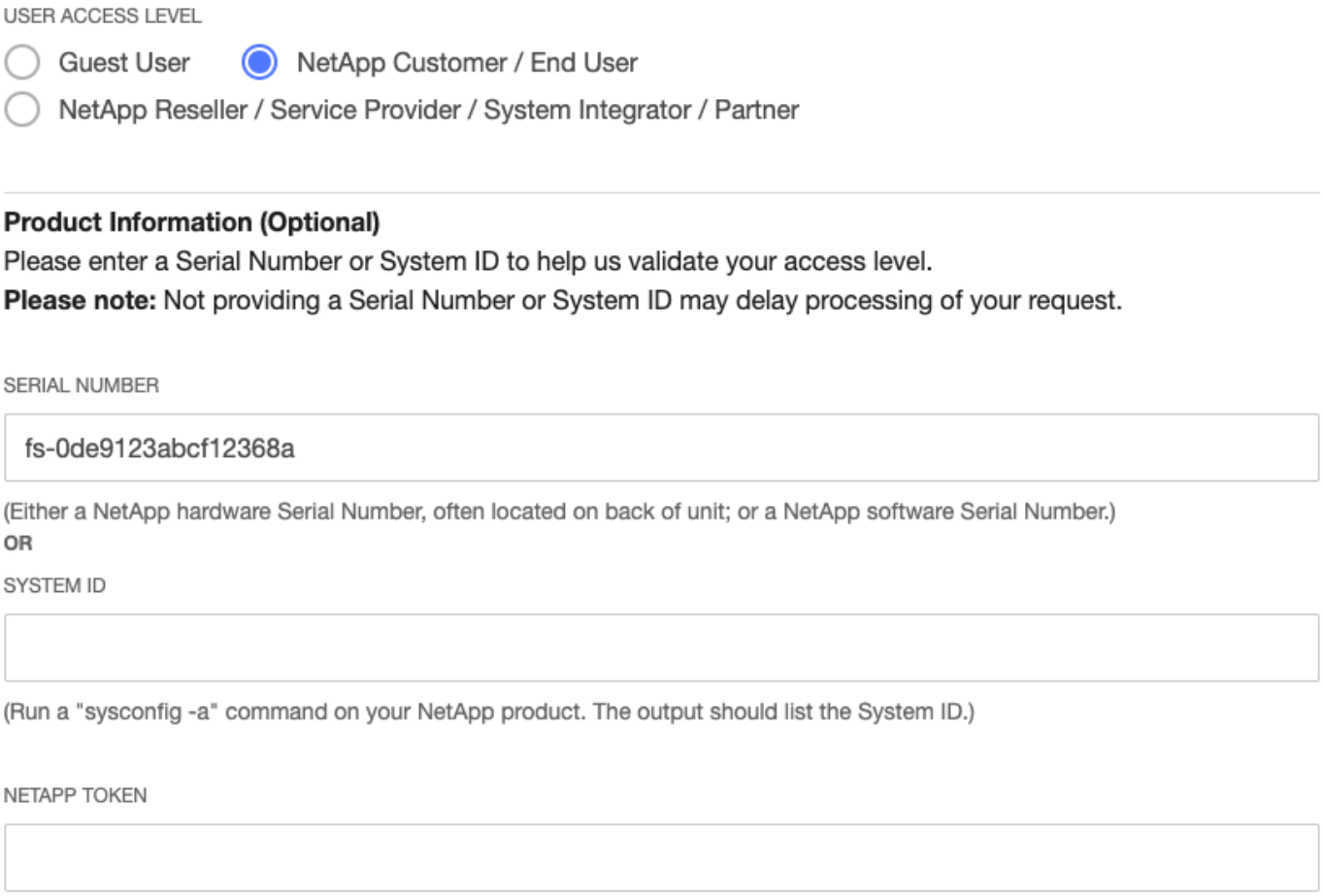
- Registrazione di un NetApp account
- Uso di NetApp Console
- Utilizzo della CLI NetApp ONTAP
- Utilizzo dell'API REST di ONTAP

> **Important**
>
> Amazon si sincronizza FSx 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 Console di gestione AWS, AWS CLI, e SDKs.

Registrazione di un NetApp account

Per scaricare alcuni NetApp software, ad esempio NetApp ConsoleSnapCenter, 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 NetApp Customer/End utente. 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 Console

NetApp La console (in precedenzaNetApp BlueXP) è un piano di controllo unificato che semplifica le esperienze di gestione dei servizi di archiviazione e dati in ambienti locali e cloud. NetApp La console fornisce un'interfaccia utente centralizzata per gestire, monitorare e automatizzare le implementazioni

ONTAP in sede e in locale. AWS Per ulteriori informazioni, consulta la documentazione della NetApp console e la documentazione sulla gestione di Amazon FSx for NetApp ONTAP.

> **Note**
>
> NetApp Consolenon è supportato per i file system di seconda generazione con più di una coppia ad alta disponibilità (HA).

Utilizzo di System Manager con NetApp NetApp Console

Puoi gestire i tuoi file system Amazon FSx for NetApp ONTAP utilizzando System Manager direttamente daNetApp Console. NetApp Consoleti 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 NetApp Console. Per ulteriori informazioni, consulta l'argomento Integrazione di ONTAP System Manager con NetApp Console nella documentazione di NetApp ONTAP.

> **Note**
>
> NetApp System Manager non è supportato per i file system di seconda generazione con più di una coppia HA.

Utilizzo della CLI NetApp ONTAP

Puoi gestire le tue risorse Amazon FSx for NetApp ONTAP utilizzando la NetApp ONTAP CLI. 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 i comandi ONTAP CLI sul file system FSx for ONTAP, in modo analogo all'esecuzione su un cluster. NetApp ONTAP È possibile accedere alla ONTAP CLI sul file system stabilendo una connessione Secure Shell (SSH) all'endpoint di gestione del file system e accedendo con nome utente e password. `fsxadmin` È possibile impostare la `fsxadmin` password quando si crea un 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 ONTAP CLI. Per ulteriori informazioni

sull'impostazione della password del file system`fsxadmin`, consultaAggiornamento dei file system. Puoi trovare il nome DNS e l'indirizzo IP dell'endpoint di gestione del tuo file system nella FSx console Amazon, nella scheda Amministrazione della pagina dei dettagli del file system FSx for ONTAP.

Per connetterti all'endpoint di gestione del file system con SSH, accedi innanzitutto a un' EC2 istanza nello stesso VPC del file system FSx for ONTAP. Una volta effettuato l'accesso all' EC2 istanza, utilizza l'`fsxadmin`utente e la password SSH nell'indirizzo IP o nel nome DNS dell'endpoint di gestione del file system, come negli esempi seguenti.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

Il comando SSH con valori di esempio:

```
ec2user $ ssh fsxadmin@198.51.100.0
```

Il comando SSH che utilizza il nome DNS dell'endpoint di gestione:

```
ec2user $ ssh fsxadmin@file-system-management-endpoint-dns-name
```

Il comando SSH che utilizza un nome DNS di esempio:

```
ec2user $ 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 tutti SVMs 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 ONTAP disponibili.

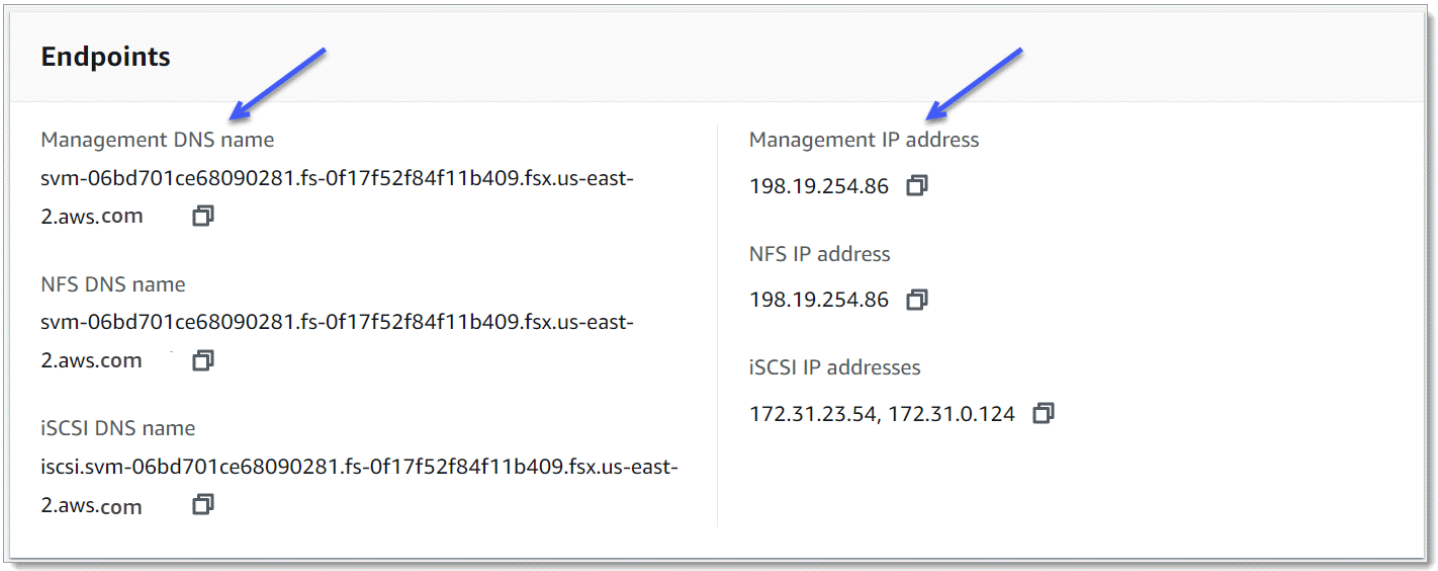
Per visualizzare un elenco dei comandi che `fsxadmin` possono essere eseguiti, utilizza il seguente comando `security login role show`ONTAPCLI:

```
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
.
.
.
378 entries were displayed.
```

Gestione SVMs con la ONTAP CLI

È possibile accedere alla ONTAP CLI sulla SVM stabilendo una connessione Secure Shell (SSH) all'endpoint di gestione dell'SVM utilizzando il nome utente e la password. `vsadmin` Puoi trovare il nome DNS e l'indirizzo IP dell'endpoint di gestione SVM nella FSx console Amazon, 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` 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 delle macchine virtuali di archiviazione (SVM). 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 accedi al file system FSx for ONTAP utilizzando l'API ONTAP REST utilizzando `fsxadmin` le credenziali, esegui una delle seguenti operazioni:

- Disabilita la convalida TLS.

  Or

- Affidati alle autorità di AWS certificazione (CAs): il pacchetto di certificati per ciascuna CAs regione è disponibile al seguente indirizzo: URLs
  - https://fsx-aws-certificates.s3.amazonaws.com*aws-region*/bundle- .pem per Public Regioni AWS
  - https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle- *aws-region* .pem per AWS GovCloud regioni
  - https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle- .pem per le regioni della Cina *aws-region* AWS

Per un riferimento completo ai comandi dell'API NetApp ONTAP REST, consulta il riferimento online all'API REST. NetApp ONTAP

Etichettare le risorse Amazon FSx

Per aiutarti a gestire i tuoi file system e altre FSx risorse Amazon, puoi assegnare i tuoi metadati a ciascuna risorsa sotto forma di tag. Con i tag, puoi classificare AWS le tue risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Questa classificazione 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

Nozioni di base sui tag

Un tag è un'etichetta che si assegna 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.

È possibile utilizzare i tag per classificare AWS le risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ad esempio, puoi definire un set di tag per i FSx file system Amazon del tuo account che ti aiutino a tenere traccia del proprietario e del livello di stack di ogni istanza.

Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Con un set di chiavi di tag coerente, la gestione delle risorse risulta semplificata. Puoi cercare e filtrare le risorse in base ai tag che aggiungi. Per ulteriori informazioni su come implementare una strategia efficace di etichettatura delle risorse, consulta Tagging AWS resources in. Riferimenti generali di AWS

Alcuni comportamenti di tagging da tenere a mente:

- I tag non hanno alcun significato semantico per Amazon FSx e vengono interpretati rigorosamente come una stringa di caratteri.
- I tag non vengono assegnati in automatico 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 puoi impostare il valore di un tag 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' FSx API Amazon, il AWS Command Line Interface (AWS CLI) o un AWS SDK, puoi fare quanto segue:
  - Puoi utilizzare l'azione `TagResource` API per applicare tag alle risorse esistenti.
  - Per alcune azioni di creazione di risorse, puoi specificare i tag per una risorsa al momento della creazione della risorsa. 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 delle risorse, Amazon FSx ripristina il processo di creazione delle risorse. Questo comportamento aiuta a garantire che le risorse vengano create con tag o non vengano create affatto e che nessuna risorsa rimanga senza tag in qualsiasi momento.

    > **Note**
    >
    > Sono necessarie determinate autorizzazioni AWS Identity and Access Management (IAM) affinché gli utenti possano taggare le risorse al momento della creazione. Per ulteriori informazioni, consulta Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

Tagging delle risorse

Puoi taggare FSx le risorse Amazon presenti nel tuo account. Se utilizzi la FSx console Amazon, puoi applicare tag alle risorse utilizzando la scheda Tag nella schermata delle risorse pertinente. Quando crei risorse, puoi applicare la chiave Name con un valore e puoi applicare tag a tua scelta quando crei un nuovo file system. Tuttavia, anche se la console organizza le risorse in base alla chiave Name, questa chiave non ha alcun significato semantico per il servizio Amazon FSx .

Per implementare un controllo granulare sugli utenti e i gruppi che possono taggare le risorse al momento della creazione, puoi applicare autorizzazioni a livello di risorsa basate su tag nelle tue policy IAM alle azioni dell' FSxAPI Amazon che supportano l'etichettatura alla creazione. Utilizzando tali autorizzazioni nelle tue politiche, ottieni i seguenti vantaggi:

- Le tue risorse sono adeguatamente protette sin dalla creazione.

- Poiché i tag vengono applicati immediatamente alle risorse, qualsiasi autorizzazione a livello di risorsa basata su tag che controlla l'uso delle risorse ha effetto immediato.
- 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 dei tag sono impostati sulle risorse esistenti, puoi applicare autorizzazioni a livello di risorsa alle azioni e alle azioni dell' FSx API `TagResource` `UntagResource` Amazon nelle tue policy IAM.

Per ulteriori informazioni sulle autorizzazioni necessarie per etichettare le FSx risorse Amazon al momento della creazione, consultaConcessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

Per ulteriori informazioni sull'utilizzo dei tag per limitare l'accesso alle FSx risorse Amazon nelle policy IAM, consultaUtilizzo dei tag per controllare l'accesso alle FSx risorse Amazon.

Per informazioni su come etichettare le risorse per la fatturazione, consulta Utilizzo dei tag di allocazione dei costi nella Guida per l'AWS Billing utente.

Copiare i tag nei backup

Quando crei o aggiorni un volume nell' FSx API Amazon oppure AWS 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 name quando crei un backup utilizzando la FSx console Amazon), i tag non vengono copiati dal volume anche se li hai abilitati. `CopyTagsToBackups`

Per ulteriori informazioni sui backup, consultare Protezione dei dati con backup di volume. Per ulteriori informazioni sull'abilitazione`CopyTagsToBackups`, consulta Per creare un volume (CLI) la Per aggiornare la configurazione di un volume (CLI) Guida per l'utente di Amazon FSx for NetApp ONTAP o CreateVolumeil riferimento UpdateVolumeall'API Amazon FSx for NetApp ONTAP.

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 UTF-8 e i seguenti caratteri: `+ - = . _ : / @` (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 `aws:` prefisso è riservato all'uso. AWS Se un tag ha una chiave di tag con questo prefisso, non puoi modificare o eliminare la chiave o il valore del tag. I tag con il prefisso `aws:` non vengono conteggiati per il limite del numero di tag per risorsa.

Non è possibile eliminare una risorsa in base esclusivamente ai relativi tag; è necessario specificare l'identificatore della risorsa. Ad esempio, per eliminare un file system etichettato con una chiave di tag chiamata`DeleteMe`, è necessario utilizzare l'`DeleteFileSystem`azione con l'identificatore di risorsa del file system, ad esempio. `fs-1234567890abcdef0`

Quando taggate risorse pubbliche o condivise, i tag assegnati sono disponibili solo per le vostre risorse Account AWS; nessun altro Account AWS ha accesso a tali tag. Per il controllo dell'accesso basato su tag alle risorse condivise, ciascuna Account AWS deve assegnare il proprio set di tag per controllare l'accesso alla risorsa.

Autorizzazioni e tagging

Per ulteriori informazioni sulle autorizzazioni necessarie per etichettare le FSx risorse Amazon al momento della creazione, consultaConcessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

Per ulteriori informazioni sull'utilizzo dei tag per limitare l'accesso alle FSx risorse Amazon nelle policy IAM, consultaUtilizzo dei tag per controllare l'accesso alle FSx risorse Amazon.

Protezione dei dati

Oltre a replicare automaticamente i dati del tuo file system per garantire un'elevata durabilità, con Amazon FSx hai anche le seguenti opzioni che puoi utilizzare per proteggere ulteriormente i tuoi dati:

- Backup di FSx volume nativi di Amazon che supportano le tue esigenze di conservazione e conformità dei backup all'interno di Amazon FSx.
- AWS Backup Utilizzati per implementare una strategia di backup e conservazione automatizzata e gestita centralmente su più Servizi AWS piattaforme.
- Istantanee che consentono agli utenti di annullare facilmente modifiche indesiderate ai file, ripristinando i file alle versioni precedenti.
- Consente SnapLock di creare volumi di archiviazione WORM (write once, read many) per impedire la modifica o l'eliminazione dei file una volta eseguito il commit, per un periodo di conservazione specificato.
- FlexCachei volumi offrono una replica dei dati efficiente, economica e ad alte prestazioni per carichi di lavoro che richiedono una lettura intensiva, con dati che rimangono per lo più invariati.
- SnapMirrorUtilizzatelo per creare una replica programmata e automatica del file system su un secondo file system per la protezione dei dati e il disaster recovery.

Argomenti

Protezione dei dati con backup di volume

Con FSx for ONTAP, puoi proteggere i tuoi dati eseguendo backup giornalieri automatici e backup avviati dall'utente dei volumi del tuo 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. È possibile ripristinare i backup di volume su qualsiasi file system FSx for ONTAP esistente a cui si ha accesso e

che si trova nello stesso Regione AWS luogo in cui è archiviato il backup. Lavorare con FSx i backup di Amazon semplifica la creazione, la visualizzazione, il ripristino e l'eliminazione dei backup dei volumi.

Amazon FSx supporta il backup di ONTAP volumi con un sistema `OntapVolumeType` di lettura-scrittura (RW).

> **Note**
>
> Amazon FSx non supporta il backup di volumi di protezione dei dati (DP), volumi Load Sharing Mirror (LSM) o volumi di destinazione per e. FlexCache SnapMirror

Argomenti

Come funzionano i backup

Tutti i FSx backup di Amazon (backup giornalieri automatici e backup avviati dall'utente) sono incrementali, il che significa che memorizzano solo le modifiche ai dati dal completamento del backup

precedente. Ciò riduce al minimo sia il tempo necessario per creare un backup sia la quantità di storage utilizzata da ciascun backup. I backup incrementali ottimizzano i costi di storage evitando l'archiviazione di dati duplicati. FSx per ONTAP i backup sono per volume, e ogni backup contiene solo i dati di un volume specifico. I FSx backup di Amazon vengono archiviati in modo ridondante su più zone di disponibilità per ottenere un'elevata durabilità.

FSx I backup di Amazon utilizzano istantanee point-in-time, immagini di sola lettura dei volumi, per mantenere l'incrementalità tra i backup. Ogni volta che viene eseguito un backup, Amazon scatta FSx prima un'istantanea del volume. L'istantanea di backup viene archiviata nel volume e occupa lo spazio di archiviazione sul volume. Amazon confronta FSx quindi questa istantanea con la precedente istantanea di backup (se ne esiste una) 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 che lo snapshot di backup più recente è stato eseguito correttamente, Amazon FSx elimina lo snapshot di backup precedente. L'istantanea utilizzata 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.

Quando si elimina un backup, vengono eliminati solo i dati esclusivi di quel backup. Ogni FSx backup Amazon contiene tutte le informazioni necessarie per creare un nuovo volume dal backup, ripristinando efficacemente un' point-in-timeistantanea del volume.

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

> **Note**
>
> Se si utilizza NDMP per i backup, ONTAP non consente che le attività di manutenzione, come le operazioni di patch, continuino mentre è in corso un NDMP trasferimento. Per evitare di ritardare le patch, Amazon FSx interromperà qualsiasi sessione di NDMP trasferimento attiva quando viene applicata un'operazione di patch durante la finestra di manutenzione del file system. Una volta completata l'applicazione delle patch, dovrai riavviare manualmente le sessioni di NDMP trasferimento dal lato client, poiché Amazon FSx non può riprenderle automaticamente. Per evitare interruzioni dei backup, consigliamo di utilizzare Amazon FSx Backups o AWS Backup, che supportano operazioni di backup e patch simultanee.

Requisiti di storage

Il volume e il file system devono disporre ciascuno di una capacità di archiviazione SSD sufficiente per archiviare un'istantanea di backup. Quando si esegue un'istantanea di backup, la capacità di archiviazione 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.

Backup giornalieri automatici

Quando si crea un file system, i backup giornalieri automatici sono abilitati per impostazione predefinita per i volumi del file system. È possibile abilitare o disabilitare i backup giornalieri automatici per i file system esistenti in qualsiasi momento. I backup giornalieri automatici per tutti i volumi vengono eseguiti durante la finestra di backup giornaliera del file system, che viene impostata automaticamente quando si crea un file system. È possibile modificare la finestra di backup giornaliera in qualsiasi momento. Per prestazioni di backup ottimali, si consiglia di scegliere una finestra di backup giornaliera al di fuori del normale orario di funzionamento, quando client e applicazioni accedono ai dati sui volumi. Si consiglia inoltre di scegliere una finestra di backup che non si sovrapponga alla finestra di manutenzione del file system. Se le finestre si sovrappongono, le attività di manutenzione hanno la precedenza e i backup automatici vengono eseguiti al termine della manutenzione. I backup già in corso continueranno durante la manutenzione, tuttavia, la creazione di nuovi backup potrebbe non avvenire fino al completamento della manutenzione. Se la manutenzione viene eseguita per l'intera durata della finestra, i backup automatici potrebbero non essere eseguiti durante tale finestra.

Utilizzando la console, è possibile impostare il periodo di conservazione per i backup giornalieri automatici su un valore compreso tra 1 e 90 giorni durante la creazione di un file system o in qualsiasi momento. Il periodo di conservazione dei backup giornalieri automatici predefinito è di 30 giorni. Amazon FSx elimina un backup giornaliero automatico una volta scaduto il periodo di conservazione. Utilizzando l'API AWS CLI and, puoi impostare il periodo di conservazione su un valore compreso tra 0 e 90 giorni; impostandolo su 0, i backup giornalieri automatici vengono disattivati.

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

Non puoi creare un backup di volume (backup giornalieri automatici o backup avviati dall'utente) se il volume è offline. Per ulteriori informazioni, consulta Visualizzazione di 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 non li elimini. AWS Backup

Puoi eliminare manualmente un backup giornaliero automatico utilizzando la FSx console Amazon, 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.

Backup avviati dall'utente

Con Amazon FSx, puoi eseguire manualmente il backup dei volumi del tuo file system in qualsiasi momento utilizzando l'API Console di gestione AWS 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 FSx console Amazon, l'API o la CLI. Non vengono mai eliminati automaticamente da Amazon FSx.

Per istruzioni su come creare un backup avviato dall'utente, consulta. Creazione di backup avviati dall'utente

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 aggiungi tag durante la creazione di un backup avviato dall'utente, inclusa l'assegnazione di un nome a un backup quando usi la console, Amazon FSx non copia i tag dal volume, anche se `CopyTagsToBackups` è abilitato.

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 NetApp ONTAP. 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 controlli migliorati. L'utilizzo AWS Backup semplifica lo sviluppo di una strategia di backup centralizzata per la conformità legale, normativa e professionale. Inoltre, semplifica 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 FSx avviato dall'utente Amazon del tuo volume e offrono le stesse opzioni di ripristino dei backup eseguiti utilizzando la console Amazon. FSx L'utilizzo AWS Backup per gestire questi backup offre funzionalità aggiuntive, inclusa la possibilità di creare backup pianificati con una frequenza ogni ora. È possibile aggiungere un ulteriore livello di difesa per proteggere i backup da eliminazioni involontarie o dolose archiviandoli in un archivio di 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 AWS Backup utilizzando la FSx console Amazon, la CLI e l'API. Tuttavia, non puoi eliminare i backup creati da AWS Backup nella FSx console Amazon, nella CLI o nell'API. Per ulteriori informazioni, consulta la sezione Guida introduttiva alla AWS Backup AWS Backup Developer Guide.

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

Puoi utilizzare i tag per selezionare quali delle tue risorse FSx for ONTAP sono protette in un piano di backup. Questi tag devono essere applicati a livello di volume anziché a livello di file system nel suo complesso. Per ulteriori informazioni, consulta Assegnazione di risorse a un piano di backup nella Guida per gli AWS Backup sviluppatori.

Ripristino dei backup su un nuovo volume

È possibile ripristinare un backup di un volume su un nuovo volume su un file system che si trova nello stesso in Regione AWS cui è archiviato il backup. Non è possibile ripristinare un backup su un file system che si trova in un luogo Regione AWS diverso dal backup.

Quando si ripristina un backup su FSx un file system ONTAP di seconda generazione, i client possono montare e leggere i dati da un volume durante il ripristino. I clienti possono montare il volume che stai ripristinando e leggere i dati del file dopo che Amazon FSx ha caricato tutti i metadati sul nuovo volume e il volume riporta lo stato del ciclo di vita di. `CREATED` Puoi trovare lo stato del ciclo di vita di un volume nella pagina dei dettagli di Volumes nella FSx console Amazon e nella risposta del comando CLI describe-volumes.

Quando si leggono i dati da un volume durante il ripristino da un backup, se i dati non sono ancora stati scaricati sul volume, si verificheranno latenze di lettura fino a decine di millisecondi per il primo accesso. Queste letture sono memorizzate nella cache del livello SSD e puoi aspettarti latenze di lettura inferiori al millisecondo per le letture successive.

Il tempo impiegato da Amazon per rendere disponibile un volume FSx per l'accesso in sola lettura è proporzionale alla quantità di metadati dei file archiviati nel backup. I metadati dei file in genere consumano l'1-7% dei dati di backup complessivi, a seconda della dimensione media del file nel set di dati (i set di dati di file di piccole dimensioni consumano più metadati rispetto ai set di dati di file di grandi dimensioni).

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 aggiunge volumi costituenti aggiuntivi per garantire che i componenti siano distribuiti uniformemente.

> **Note**
>
> Amazon FSx non supporta l'accesso in lettura ai dati durante il ripristino di un volume da un backup per entrambi SnapLock i volumi o per qualsiasi volume sui file system di prima generazione. Quando si ripristinano questi backup, il volume diventa disponibile per il montaggio e l'accesso ai dati una volta completato il processo di ripristino e tutti i metadati e i dati vengono caricati sul nuovo volume.

Quando si ripristina un backup, tutti i dati vengono inizialmente scritti sul livello di archiviazione SSD. Durante il ripristino, i dati vengono suddivisi su più livelli nello storage del pool di capacità in base alla politica di suddivisione in più livelli del volume da ripristinare. Poiché i dati vengono scritti per la prima volta sul livello SSD, Amazon FSx sospenderà il processo di ripristino se il file system esaurisce lo spazio di archiviazione SSD. Il ripristino riprende automaticamente non appena diventa disponibile spazio SSD sufficiente per continuare il processo. Se la politica di suddivisione in più livelli del volume ripristinato è quella stabilita`All`, un processo periodico in background suddivide i dati nel pool di

capacità. Se la politica di suddivisione in più livelli del volume ripristinato è `Snapshot Only` o`Auto`, i dati vengono suddivisi in 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 politica di tiering.

Se il carico di lavoro richiede latenze di lettura costanti inferiori al millisecondo durante il ripristino di un backup su un nuovo volume su file system di seconda generazione, consigliamo di impostare la politica di tiering del volume su più livelli all'`None`avvio del ripristino e quindi di attendere che tutti i dati siano stati scaricati completamente sul volume prima di accedervi. Tutti i dati verranno caricati nello storage SSD prima di tentare di accedervi, garantendo un accesso costante a bassa latenza ai dati.

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

Nei file system di seconda generazione è inoltre possibile ripristinare solo un sottoinsieme di dati da un backup senza dover attendere il completamento dell'intera operazione di ripristino. Il ripristino di solo un sottoinsieme dei dati di un backup consente di riprendere le operazioni più rapidamente in caso di eliminazione, modifica o danneggiamento accidentale dei dati. Per ulteriori informazioni, consulta Ripristino di un sottoinsieme di dati.

È possibile monitorare l'avanzamento del ripristino di un backup su un file system di seconda generazione nell'API, e. Console di gestione AWS AWS CLI Per ulteriori informazioni, consulta Monitoraggio dell'avanzamento del ripristino di un backup.

> **Note**
>
> - Non è possibile creare un'istantanea di un volume o eseguire operazioni basate su istantanee come la SnapMirror clonazione, la replica e la creazione di backup di un volume durante il ripristino da un backup.
> - Un volume ripristinato ha sempre lo stesso stile di volume del volume originale. Non è possibile modificare lo stile del volume durante il ripristino.

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 letture e scritture di dati e metadati NFS, CIFS e iSCSI. Tutti i processi in background 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 per lo più 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 per lo più 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 in diversi ripristini simultanei contenenti principalmente file di grandi dimensioni.
- 100 MBps in diversi ripristini simultanei contenenti principalmente file di piccole dimensioni.

Backup di volumi SnapLock

È possibile eseguire il backup SnapLockdei 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, consulta Funzionamento di SnapLock.

Creazione di backup avviati dall'utente

La procedura seguente descrive come 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 Visualizzazione di volumi offline.

Per creare un backup avviato dall'utente (console)

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Vai 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 vedere tutti i tuoi backup nella FSx console Amazon 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. Console di gestione AWS AWS CLI Quando si ripristina un volume su un file system

di seconda generazione, è possibile monitorare l'avanzamento utilizzando l'API Console di gestione AWS, AWS CLI e.

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

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione, scegli Backup, quindi scegli FSx il backup del volume ONTAP che desideri ripristinare.
3. Nel menu Azioni in alto a destra, scegli Ripristina backup. Viene visualizzata la pagina Crea volume da backup.
4. Scegli FSx la macchina virtuale ONTAP File system and Storage su cui desideri ripristinare il backup dai menu a discesa.
5. Nel menu Azioni in alto a destra, scegli Ripristina backup. Viene visualizzata la pagina Crea volume da backup.
6. Scegli FSx la macchina virtuale ONTAP File system and Storage su cui desideri ripristinare il backup dai menu a discesa.
7. 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 (_).
8. Per Dimensione del volume, immettete un numero intero compreso tra 20 e 314572800 per specificare la dimensione in mebibyte (MiB).
9. 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.
10. 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`.
11. Per l'efficienza dello storage, scegli Enabled per abilitare le funzionalità di ONTAP efficienza dello storage (deduplicazione, compressione e compattazione). Per ulteriori informazioni, consulta Efficienza dello storage.
12. Per lo stile di sicurezza Volume, scegli Unix (Linux), NTFS o Mixed. Lo stile di sicurezza di un volume determina se dare la preferenza a NTFS o UNIX ACLs per l'accesso multiprotocollo. La modalità MIXED non è richiesta per l'accesso multiprotocollo ed è consigliata solo per utenti esperti.
13. 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.

14. 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.
15. 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 un volume SnapLock Compliance o di un volume SnapLock Enterprise, consulta Comprendere la conformità SnapLock eComprendere SnapLock Enterprise. Per ulteriori informazioni su SnapLock, consultare Proteggi i tuoi dati con SnapLock.
16. Scegli Conferma per creare il volume.
17. Se stai ripristinando il backup su un file system di seconda generazione, puoi monitorare l'avanzamento del ripristino del backup nella scheda Aggiornamenti della pagina Volume. Per ulteriori informazioni, consulta Monitoraggio dell'avanzamento del ripristino di un backup.

Per ripristinare un backup 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 di ripristino riuscita per ripristinare un backup su un file system di seconda generazione è la seguente. La risposta include l'`"AdministrativeActions"`oggetto che fornisce informazioni sullo stato e sull'avanzamento della richiesta.

  ```
  {
        "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",
  --->    "AdministrativeActions": [
              {
                  "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
                  "RequestTime": 1685729972.069,
                  "Status": "PENDING"
              }
          ]                <----
      }
  }
```

La risposta del sistema a una richiesta di ripristino di un backup su un file system di prima generazione è la seguente.

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

Quando si ripristina un volume su un file system di seconda generazione, è possibile monitorare l'avanzamento utilizzando l'API Console di gestione AWS, AWS CLI e.

Ripristino di un sottoinsieme di dati

È possibile ripristinare un sottoinsieme di dati da un backup mentre viene ripristinato su un nuovo volume su file system di seconda generazione senza dover attendere il ripristino completo dell'intero set di dati di backup.

La procedura seguente elenca i passaggi da eseguire quando è necessario ripristinare un sottoinsieme di dati durante il ripristino di un backup e non è necessario attendere il completamento dell'intero ripristino:

Per ripristinare un sottoinsieme di dati durante il ripristino di un backup

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nella pagina Backup, individua il backup che contiene la versione dei dati che desideri ripristinare.
3. Nel menu Azioni in alto a destra, scegli Ripristina backup. Viene visualizzata la pagina Crea volume da backup.

4. Scegli FSx la macchina virtuale ONTAP File system and Storage su cui desideri ripristinare il backup dai menu a discesa.
5. In Dettagli del volume, configura il volume in base alle tue esigenze.
6. Scegli Conferma per creare il volume.
7. Monitora l'avanzamento del ripristino del backup.
8. Installa il volume da ripristinare quando riporta uno stato del ciclo di vita di. `CREATED`
9. Individua il sottoinsieme di dati sul volume da copiare.
10. Copia i dati nel volume esistente utilizzato dall'applicazione.
11. Dopo aver copiato i dati richiesti dal backup nella posizione di destinazione, è possibile eliminare il volume da ripristinare prima del completamento per ottimizzare l'utilizzo delle risorse del file system.

Monitoraggio dell'avanzamento del ripristino di un backup

È possibile monitorare l'avanzamento del ripristino di un backup di volume su un file system di seconda generazione nell' Console di gestione AWS API, e. AWS CLI Come per tutte le azioni FSx amministrative di Amazon, lo stato di ripristino del backup è disponibile nella console, nella CLI e nell'API per 30 giorni dopo il completamento dell'operazione.

Per monitorare l'avanzamento del ripristino di un backup (console)

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

1. Nel menu di navigazione a sinistra, scegli Volumes.
2. Scegli il volume in cui viene ripristinato il backup.
3. Scegli la scheda Aggiornamenti.
4. Il tipo Backup restore Update fornisce le seguenti informazioni:

   - PENDING indica che i metadati del file vengono scaricati sul volume. Lo stato del ciclo di vita del volume è CREATING.
   - IN_PROGRESS indica che il volume è disponibile e che i client possono montarlo con accesso in sola lettura ai dati. La percentuale di avanzamento mostra la percentuale di dati scaricati nel volume.

- COMPLETATO indica che tutti i dati sono stati scaricati sul volume e che il ripristino del backup è completo. I client ora dispongono di accesso in lettura/scrittura. Per `RW` i volumi, il tipo del volume cambia da `DP` a a questo `RW` punto.

Per monitorare l'avanzamento del ripristino di un backup (CLI)

- Quando ripristini un backup su un nuovo volume su un file system di seconda generazione FSx per ONTAP, puoi monitorare l'avanzamento del ripristino utilizzando il comando `describe-volumes`CLI.

  Quando si ripristina un backup su un file system di seconda generazione, la risposta include l'`AdministrativeActions`oggetto, che fornisce informazioni sullo stato del processo di download dei dati. Il

```
$ aws fsx describe-volumes
{
    “Volumes”: [
        {
            “CreationTime”: 1691686114.674,
            “FileSystemId”: fs-029ff92192bd4d375,
            “LifeCycle”: “CREATING”,
            “Name”: vol1,
            “OntapConfiguration”: {
                   “FlexCacheEndpointType”: “NONE”,
                   “JunctionPath”: “/vol1”,
                   “SizeInMegabytes”: 100000,
                   “StorageEfficiencyEnabled”: true,
                   “StorageVirtualMachineId”: “svm-0ed1d714019426ca9”,
                   “StorageVirtualMachineRoot”: false,
                   “TieringPolicy”: {
                    “Name”: “ALL”
                   },
                   “OntapVolumeType”: “DP”,
                   “SnapshotPolicy”: “default”,
                   “CopyTagsToBackups”: false,
                  },
                  “ResourceARN”: “arn:aws:fsx:us-east-1:630831496844:volume/
fs-08ac75f715c6aec76/fsvol-094c015af930790fa”,
                  “VolumeId”: “fsvol-094c015af930790fa”,
                  “VolumeType”: “ONTAP”,
                  “AdministrativeActions”: [
```

```
                        {
                         “AdministrativeActionType”: “DOWNLOAD_DATA_FROM_BACKUP”,
                         “RequestTime”: 1685729972.069,
                         “Status”: “PENDING”
                        }
                ]
    }
```

Una volta che Amazon FSx carica tutti i metadati dei file sul volume ripristinato, questi campi hanno i seguenti valori:

- `"LifeCycle": "CREATED"`— indica che il volume è pronto per essere montato.
- `"OntapVolumeType": "DP"`— indica che il volume è di sola lettura durante il download dei dati del file.
- `"ProgressPercent`— mostra la percentuale di dati di file caricati nel volume.
- `"Status": "IN_PROGRESS"`— è in corso il download dei dati del file sul volume.

In questa fase del processo di ripristino è possibile montare il volume con accesso in sola lettura a tutti i dati del backup da ripristinare.

Quando Amazon FSx ha completato il download di tutti i dati dei file sul nuovo volume, i client hanno accesso completo in lettura/scrittura se si tratta `RW` di un volume. Gli indicatori hanno i seguenti valori:

- `"LifeCycle": "CREATED"`— invariato
- `"OntapVolumeType": "RW"`— indica che i client dispongono dell'accesso completo in lettura/scrittura.
- `"Status": "COMPLETED"`— indica che il ripristino è completo.

Se il processo di ripristino non riesce, `AdminstrativeAction > Status` avrà un valore di`FAILED`. Nell'`FailureDetails`oggetto viene fornito un messaggio di errore. Per ulteriori informazioni, AdministrativeActionFailureDetailsconsulta Amazon FSx API Reference

Eliminazione di backup

Puoi eliminare sia i backup giornalieri automatici che i backup avviati dall'utente dei tuoi volumi utilizzando la console Amazon FSx , l' FSx API Amazon o (). AWS Command Line Interface AWS CLI

L'eliminazione di un backup è un'azione permanente e irrecuperabile. Vengono eliminati anche tutti i dati contenuti in un backup eliminato. Non eliminate un backup a meno che non siate sicuri di non averne più bisogno in futuro. Non puoi eliminare un backup se il volume di origine è offline.

È possibile eliminare un volume mentre viene ripristinato da un backup su tutti FSx i file system ONTAP. L'eliminazione di un volume durante il ripristino annulla di fatto l'operazione di ripristino in corso.

> **Note**
>
> Amazon FSx non supporta l'eliminazione del `AVAILABLE` backup più recente di un ONTAP volume a meno che tutti gli altri backup del volume non siano stati eliminati.

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

Per eliminare un backup (console)

1. Apri la FSx console Amazon 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 il relativo stato del ciclo di vita con un valore di`DELETED`, che indica che la richiesta ha avuto esito positivo.

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

Protezione dei dati con istantanee

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
- Ripristino di file da istantanee
- Visualizzazione dell'istantanea comune
- Aggiornamento della riserva di istantanee del volume
- Disattivazione delle istantanee automatiche
- Eliminazione di snapshot
- Eliminazione di snapshot
- Riserva per le istantanee

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 politiche integrate per le istantanee per FSx ONTAP:

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

Per impostazione predefinita, ogni volume è associato alla politica di `default` snapshot del file system. 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 di 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). È possibile impostare un fuso orario FSx per il file system ONTAP utilizzando il comando `timezone -timezone` *`time_zone`* ONTAP CLI. Per ulteriori informazioni sull'accesso alla ONTAP CLI, vedere. Utilizzo della CLI NetApp ONTAP

La `default-1weekly` policy funziona allo stesso modo della `default` policy, 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 FSx console Amazon AWS CLI, o nell' FSx API Amazon. Per ulteriori informazioni, consultare Creazione di volumi e Aggiornamento dei volumi.

Ripristino di file da istantanee

Utilizzando le istantanee sul tuo FSx file system Amazon, puoi ripristinare rapidamente le versioni precedenti di singoli file o cartelle.

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

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.

Visualizzazione dell'istantanea comune

L'istantanea comune viene utilizzata per mantenere l'incrementalità tra i backup. Questa procedura spiega come identificare l'istantanea comune sul volume.

Per visualizzare l'istantanea comune di un volume

- Per determinare quale istantanea è l'istantanea comune di un volume, utilizzate il comando CLI volume snapshot showONTAP.

  ```
  volume snapshot show -volume volume-name
  ```

  Nell'output, il nome dell'istantanea comune ha il formato dibackup-*id*, dove *id* è una stringa alfanumerica di 17 cifre, come illustrato nell'esempio seguente:

  ```
  FsxIdabc12345::> volume snapshot show -volume test_vol
                                    ---Blocks---
  Vserver Volume    Snapshot                    Size     Total% Used%
  -------- -------- --------------------------- -------- ------ -----
  dest-svm test_vol
                    snap1                        144KB    0%     3%
                    snap2                        832KB    0%    16%
           --->     backup-abcdef0123456789a    4.87MB    0%    53% <---
                    weekly.2024-05-26_0015      5.02MB    0%    54%
                    weekly.2024-06-02_0015      2.22MB    0%    34%
                    daily.2024-06-04_0010        284KB    0%     6%
                    daily.2024-06-05_0010       4.29MB    0%    50%
                    hourly.2024-06-05_0705       168KB    0%     4%
  8 entries were displayed.
  ```

> **Important**
>
> Non eliminate l'istantanea comune sul volume perché viene utilizzata per mantenere l'incrementalità tra i backup. L'eliminazione dell'istantanea comune di un volume farà sì che il backup successivo sia un backup completo del volume anziché un backup incrementale.

Aggiornamento della riserva di istantanee del volume

È possibile modificare la quantità di riserva di snapshot su un volume utilizzando la NetApp ONTAP CLI o l'API, descritta nella procedura seguente.

1. Per accedere alla ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 `volume modify`ONTAPCLi per modificare la percentuale di spazio su disco utilizzata per la riserva di copie Snapshot. 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.
   - *percent*— la percentuale di spazio su disco che si desidera riservare per le copie delle istantanee.

   ```
   ::> volume modify -vserver svm_name -volume vol_name -percent-snapshot-
   space percent
   ```

   L'esempio seguente modifica la riserva per le istantanee per vol1 al 25% della capacità di archiviazione del volume.

   ```
   ::> volume modify -vserver vs0 -volume vol1 -percent-snapshot-space 25
   ```

Disattivazione delle istantanee automatiche

Le istantanee automatiche sono abilitate dalla politica di snapshot predefinita per i volumi del file system for FSx 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' Console di gestione AWS API AWS CLI e e della ONTAP CLI, come descritto nelle seguenti procedure.

Per disabilitare le istantanee automatiche (console)AWS

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

```
::> 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.
```

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. Poiché le istantanee sono incrementali, non si recupera una quantità di spazio di archiviazione pari alla dimensione dell'istantanea quando la si elimina. È possibile visualizzare la quantità di storage che è possibile recuperare quando si elimina un'istantanea utilizzando il comando volume snapshot compute-reclaimable -vserver ONTAP CLi, utilizzando i dati per sostituire, e. *svm_name vol_name snapshot_name*

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

È possibile eliminare le istantanee creando una politica di eliminazione automatica delle istantanee o eliminando manualmente le istantanee. L'eliminazione di un'istantanea elimina i dati modificati memorizzati nell'istantanea.

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 FSx i backup Amazon, Amazon FSx conserva uno snapshot per il FSx backup Amazon più recente di ogni volume. Queste istantanee vengono utilizzate per mantenere l'incrementalità tra i backup e non devono essere eliminate utilizzando questo metodo. Per ulteriori informazioni, consulta Visualizzazione dell'istantanea comune.

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

Creazione di 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

Riserva per le 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 di istantanee, 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 viene creata un'istantanea quando i dischi sono pieni, l'eliminazione dei file dal livello SSD primario non crea spazio libero perché a tutti quei dati fa riferimento anche l'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 di istantanee del volume.

Protezione dei dati con Autonomous Ransomware Protection

Autonomous Ransomware Protection (ARP) è una funzionalità NetApp ONTAP basata sull'intelligenza artificiale che monitora e protegge i dati dagli attacchi di ransomware e malware in caso di compromissione dei client Windows o Linux. Utilizzando l'apprendimento automatico, ARP acquisisce familiarità con i file system di FSx for ONTAP per rilevare in modo proattivo attività anomale. ARP è disponibile per tutti i file system nuovi ed esistenti FSx di ONTAP in tutti i paesi in cui è disponibile Regioni AWS Amazon FSx for NetApp ONTAP.

Come funziona ARP

È possibile abilitare ARP per volume o per impostazione predefinita su tutti i nuovi volumi in una SVM utilizzando la CLI ONTAP o l'API REST. Per ulteriori informazioni sull'attivazione di ARP, vedere. Attivazione della protezione autonoma dal ransomware

Poiché l'intelligenza artificiale di ARP è addestrata su un set di dati completo, non è necessario un periodo di apprendimento per far funzionare ARP su FlexVol volumi e quindi si avvia immediatamente in modalità attiva. ARP AI è inoltre dotato di una funzionalità di aggiornamento automatico per garantire protezione e resilienza costanti contro le minacce più recenti. In modalità attiva, ARP monitora i dati e le attività in entrata sul volume per identificare potenziali attacchi di ransomware e malware. Per ulteriori informazioni, consulta Cosa cerca ARP. Se ARP rileva un'attività anomala, viene creata automaticamente un'ONTAPistantanea per aiutarvi a recuperare i dati il più vicino possibile al momento del potenziale attacco. L'istantanea avrà il prefisso di`Anti_ransomware_backup`, quindi è facile da identificare. Se viene stabilito che la probabilità di attacco è moderata, ONTAP genererà un messaggio EMS (Events Management System) da esaminare. Per ulteriori informazioni, consultare Come rispondere a un attacco sospetto con ARP e Comprensione degli avvisi EMS per Autonomous Ransomware Protection.

Il sovraccarico prestazionale per ARP è minimo per la maggior parte dei carichi di lavoro. Se i volumi hanno carichi di lavoro ad alta intensità di lettura, consigliamo di proteggere non più NetApp di 150 volumi di questo tipo per file system. Se si supera questo numero, l'IOPS per quel carico di lavoro potrebbe diminuire fino al 4%. Se i volumi hanno carichi di lavoro ad alta intensità di scrittura, consigliamo di proteggere non più NetApp di 60 volumi di questo tipo per file system. In caso contrario, l'IOPS per quel carico di lavoro potrebbe diminuire fino al 10%. Per ulteriori informazioni sulle prestazioni, consultare Amazon FSx per le prestazioni di NetApp ONTAP.

L'abilitazione di ARP sul file system FSx for ONTAP non prevede costi aggiuntivi.

Cosa cerca ARP

ARP cerca segnali che indichino che i client Windows o Linux siano compromessi. In particolare, ARP cerca i seguenti tipi di attività sul volume:

- Variazioni di entropia, ossia differenze nella casualità dei dati in un file.
- Modifiche nei tipi di estensione di file, il che significa che la nuova estensione non è coerente con il tipo di estensione normalmente utilizzato. L'impostazione predefinita è 20 file con estensioni di file non precedentemente osservate nel volume.

- Modifiche negli IOPS dei file, ovvero un aumento dell'attività anomala del volume con dati crittografati.

Se necessario, puoi modificare i parametri di rilevamento del ransomware per il tuo volume. Ad esempio, se il volume ospita molti tipi di estensioni di file. Per ulteriori informazioni, consulta Gestire i parametri di rilevamento degli attacchi di ONTAP Autonomous Ransomware Protection nel NetApp Documentation Center.

> **Note**
>
> ARP non impedisce agli amministratori non autorizzati con credenziali di accedere al file system for ONTAP. FSx AWS consiglia un approccio di sicurezza a più livelli che includa istantanee e. AWS BackupONTAP SnapLock

Come rispondere a un attacco sospetto con ARP

Se ARP rileva un attacco, genererà un'istantanea che può essere utilizzata come punto di ripristino. L'istantanea è bloccata e non può essere eliminata normalmente. A seconda della gravità dell'attacco, genererà anche un avviso EMS che mostra il volume interessato, la probabilità di attacco e la tempistica dell'attacco. Se desideri ricevere avvisi per la creazione di una nuova istantanea o l'osservazione di una nuova estensione di file sul tuo volume, puoi configurare ARP per inviare questi avvisi. Per ulteriori informazioni, consulta Configurare gli avvisi ARP nel Documentation Center. NetApp

È possibile generare un rapporto per visualizzare informazioni dettagliate su un attacco sospetto. Dopo aver esaminato il rapporto, puoi stabilire ONTAP se l'avviso è stato generato da un falso positivo o da un attacco sospetto. Se si etichetta l'avviso come attacco sospetto, è necessario determinare la portata dell'attacco e quindi recuperare i dati dall'istantanea creata da ARP. Se si etichetta l'attacco come falso positivo, l'istantanea creata da ARP viene eliminata automaticamente. Per ulteriori informazioni, consulta Risposta agli avvisi di Autonomous Ransomware Protection.

Consigliamo di monitorare i messaggi EMS del file system e lo stato dei volumi nella ONTAP CLI e nell'API REST. Per ulteriori informazioni sui messaggi EMS per ARP, vedere. Comprensione degli avvisi EMS per Autonomous Ransomware Protection

Argomenti

- Attivazione della protezione autonoma dal ransomware

- Risposta agli avvisi di Autonomous Ransomware Protection
- Comprensione degli avvisi EMS per Autonomous Ransomware Protection

Attivazione della protezione autonoma dal ransomware

Le seguenti procedure spiegano come utilizzare la ONTAP CLI per abilitare la modalità attiva Autonomous Ransomware Protection (ARP) e come verificare che ARP sia abilitato. Per ulteriori informazioni su ARP, vedere. Come funziona ARP

Abilitazione di ARP in modalità attiva

Per abilitare ARP in modalità attiva su un volume esistente utilizzando la CLI ONTAP

- Esegui il comando seguente. Sostituisci *vol_name* e *svm_name* con le tue informazioni.

  ```
  security anti-ransomware volume enable -volume vol_name -vserver svm_name
  ```

  Per ulteriori informazioni su questo comando, vedere `security anti-ransomware volume enable`nel centro NetApp documentazione.

Abilitare ARP per impostazione predefinita a livello SVM

Per abilitare ARP per impostazione predefinita su una SVM esistente utilizzando la CLI ONTAP

- Esegui il comando seguente. Sostituisci *svm_name* con le tue informazioni.

  ```
  vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
  ```

  Per ulteriori informazioni su questo comando, vedere `vserver modify`nel centro NetApp documentazione.

Verifica dello stato di ARP

Per verificare lo stato di ARP utilizzando la CLI ONTAP

- Esegui il comando seguente.

  ```
  security anti-ransomware volume show
  ```

Per ulteriori informazioni su questo comando, consultate `security anti-ransomware volume show`nel centro NetApp documentazione.

È possibile sospendere temporaneamente (e quindi riprendere) ARP se si prevedono eventi con carichi di lavoro pesanti. Per ulteriori informazioni, consulta Pause ONTAP Autonomous Ransomware Protection per escludere gli eventi del carico di lavoro dall'analisi nel Documentation Center. NetApp

Risposta agli avvisi di Autonomous Ransomware Protection

Le seguenti procedure spiegano come utilizzare la ONTAP CLI per visualizzare gli avvisi di Autonomous Ransomware Protection (ARP), generare report sugli attacchi e intervenire sui report. Per ulteriori informazioni su come ARP rileva e risponde agli attacchi, vedere e. Cosa cerca ARP Come rispondere a un attacco sospetto con ARP

Visualizzazione degli avvisi ARP

Per visualizzare un avviso ARP su un volume utilizzando la CLI ONTAP

- Esegui il comando seguente. Sostituisci *svm_name* e *vol_name* con le tue informazioni.

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

Dopo aver eseguito il comando, vedrai un output simile al seguente esempio:

```
Vserver Name: fsx
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

Per ulteriori informazioni su questo comando, consulta `security anti-ransomware volume show`nel centro NetApp documentazione.

Generazione di report ARP

Per generare report ARP utilizzando la CLI ONTAP

- Esegui il comando seguente. Sostituisci *vol_name* e */file_location/* con le tue informazioni. Dopo aver generato il rapporto, è possibile visualizzarlo su un sistema client.

```
security anti-ransomware volume attack generate-report -volume vol_name -dest-
path /file_location/
```

  Per ulteriori informazioni su questo comando, vedere security anti-ransomware volume attack generate-reportnel centro NetApp documentazione.

Intervenire sui report ARP

Per intervenire su un attacco falso positivo proveniente da un rapporto ARP utilizzando la CLI ONTAP

- Esegui il comando seguente. Sostituisci *svm_name vol_name* e *[extension identifiers]* con le tue informazioni.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive true
```

  Per ulteriori informazioni su questo comando, vedere security anti-ransomware volume attack clear-suspectnel centro NetApp documentazione.

  > **Note**
  >
  > Quando contrassegni un avviso come falso positivo, aggiorna il profilo del ransomware. Dopo averlo fatto, non riceverai più alcun avviso su quel particolare scenario.

Per intervenire su un potenziale attacco da un rapporto ARP utilizzando la CLI ONTAP

- Esegui il comando seguente. Sostituisci *svm_name vol_name* e *[extension identifiers]* con le tue informazioni.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive false
```

Per ulteriori informazioni su questo comando, vedere security anti-ransomware volume attack clear-suspectnel centro NetApp documentazione.

Comprensione degli avvisi EMS per Autonomous Ransomware Protection

È possibile utilizzare NetApp ONTAP's Events Management System (EMS) per monitorare gli eventi relativi all'ARP, inclusi i potenziali attacchi. Per ulteriori informazioni su ARP e su come rileva gli attacchi, vedere e. Come funziona ARP Cosa cerca ARP

La tabella seguente contiene tutti gli avvisi relativi a ARP. Per ulteriori informazioni su EMS, vedere. Monitoraggio FSx degli eventi ONTAP EMS

Nome del messaggio EMS	Descrizione del messaggio EMS
`arw.analytics.ext.report`	Questo messaggio viene visualizzato quando l'analisi anti-ransomware genera o aggiorna il rapporto sulle estensioni di file sospette per un volume.
`arw.analytics.high.entropy`	Questo messaggio si verifica quando il numero di messaggi di log di dati ad alta entropia (relativi al rilevamento e all'analisi del ransomware) supera la soglia predefinita per un volume.
`arw.analytics.probability`	Questo messaggio viene visualizzato quando la probabilità di un attacco anti-ransomware cambia da 0 a su un volume. `low` `high`
`arw.analytics.report`	Questo messaggio viene visualizzato quando un rapporto di analisi anti-ransomware viene generato o aggiornato per un volume.

Nome del messaggio EMS	Descrizione del messaggio EMS
`arw.analytics.suspects`	Questo messaggio viene visualizzato quando un elenco di sospetti generato dall'analisi anti-ransomware cresce al punto da richiedere ulteriori indagini.
`arw.new.file.extn.seen`	Questo messaggio viene visualizzato quando viene rilevata una nuova estensione di file in un volume con funzionalità anti-ransomware. Il suo scopo è informare tempestivamente l'utente dell'estensione osservata, il che consente un'indagine tempestiva.
`arw.snapshot.created`	Questo messaggio si verifica quando viene creata una nuova istantanea ARP in un volume con funzionalità anti-ransomware. Inoltre, fornisce informazioni sul motivo per cui l'istanta nea è stata creata.
`arw.volume.state`	Questo messaggio viene visualizzato quando lo stato anti-ransomware di un volume viene modificato.
`arw.vserver.state`	Questo messaggio viene visualizzato quando lo stato anti-ransomware di una SVM viene modificato.

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 conSnapLock. Per ulteriori informazioni, consultare Comprendere la conformità SnapLock e Comprendere SnapLock Enterprise.

Puoi creare SnapLock volumi sui FSx file system 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 aiutarti a soddisfare gli obiettivi normativi e di governance impedendo che i tuoi 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. Nella tabella seguente vengono illustrate alcune delle somiglianze e delle differenze tra queste modalità di conservazione.

Caratteristica SnapLock	Comprendere la conformità SnapLock	Comprendere SnapLock Enterprise
Description	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 di ransomware.	• Promuovere l'integrità dei dati e la conformità interna di un'organizzazione. • Per testare le impostazioni di conservazione prima di utilizzare SnapLock Compliance.
Commit automatico	Sì	Sì
Conservazione basata sugli eventi (EBR)[1]	Sì	Sì
Conservazione legale[1]	Sì	No
Utilizzo dell'eliminazione privilegiata	No	Sì
modalità Volume-append	Sì	Sì
SnapLockvolumi dei registri di controllo	Sì	Sì

> **Note**
>
> [1] Le operazioni EBR e Legal Hold sono supportate nella ONTAP CLI e nell'API REST.

> **Note**
>
> FSx for ONTAP supporta il tiering dei dati nel pool di capacità su tutti i SnapLock volumi, indipendentemente dal tipo. SnapLock Per ulteriori informazioni, consulta Suddivisione dei volumi di dati su più livelli.

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 processi

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

- Eseguire il seguente comando seguente. Sostituisci e con le tue informazioni. *SVM_name* *SnapLockAdmin*

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

Per ulteriori informazioni, consulta ONTAPruoli e utenti.

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 FSx console Amazon, l' FSx API Amazon AWS CLI, l'interfaccia a riga di ONTAP comando e l'API REST.

> **Note**
>
> Un volume di protezione dei dati (DP) non può essere utilizzato come volume di log di SnapLock controllo.

Per attivare il volume del registro di SnapLock controllo con l' FSx API Amazon, usa `AuditLogVolume` in `CreateSnaplockConfiguration`. Nella FSx console Amazon, per Audit log volume, scegli Enabled. Assicurati che il percorso di giunzione sia impostato su`/snaplock_audit_log`.

Accesso ai dati in un SnapLock volume

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).

SnapLocke le operazioni di riduzione della capacità degli SSD

Prima di creare un SnapLock volume, considera questi punti sulle riduzioni degli SSD:

- Amazon FSx rifiuterà le richieste di riduzione della capacità SSD sui file system che contengono SnapLock volumi.
- Non è possibile creare SnapLock volumi durante un'operazione di riduzione della capacità SSD.

Queste limitazioni esistono perché ONTAP impone un periodo di conservazione minimo di 6 mesi per il volume del registro di SnapLock controllo, il che impedirebbe l'eliminazione del file system durante tale periodo se un SnapLock volume venisse spostato come parte di un'operazione di riduzione dell'SSD.

Se è necessario ridurre la capacità SSD su un file system con SnapLock volumi, è necessario migrare i dati su un nuovo file system con una capacità SSD inferiore. Per ulteriori informazioni sulle operazioni di riduzione della capacità degli SSD, comprese le limitazioni e le considerazioni, consulta. Aggiornamento dello storage SSD e degli IOPS del file system

Comprendere la conformità SnapLock

Questa sezione descrive i casi d'uso e le considerazioni relative alla modalità di mantenimento della SnapLock conformità.

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.

Di seguito sono riportati alcuni elementi importanti da considerare sulla modalità di conservazione della SnapLock 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.

Comprendere SnapLock Enterprise

Questa sezione descrive i casi d'uso e le considerazioni relative alla modalità di conservazione SnapLock Enterprise.

È possibile scegliere la modalità di conservazione SnapLock 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.

Di seguito sono riportati alcuni elementi importanti da considerare sulla modalità di conservazione SnapLock 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.

Utilizzo dell'eliminazione privilegiata

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 FSx console Amazon AWS CLI, l' FSx API Amazon e l'API ONTAP CLI e REST. Per attivare l'eliminazione privilegiata, devi prima creare un volume di registro 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' FSx API Amazon, usa `PrivilegedDelete` in. `CreateSnaplockConfiguration` Nella FSx console Amazon, per Privileged Delete, scegli Enabled.

> **Note**
>
> Non puoi 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.

È possibile scegliere di disattivare l'eliminazione con privilegi 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' FSx API Amazon, usa `PrivilegedDelete` in. `CreateSnaplockConfiguration` Nella FSx console Amazon, per Privileged Delete, scegli Disabilitato permanentemente.

Bypassare SnapLock la modalità Enterprise

Se utilizzi la FSx console Amazon o Amazon FSx API, 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.

Comprensione del SnapLock periodo di conservazione

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 per tale file.
- 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.

Tipo	Valore	Note
Secondi	0 - 65.535	

Tipo	Valore	Note
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 1	-	Conserva i file fino a quando non viene impostato un periodo di conservazione. Disponibile solo per la conservazione predefinita.

> **Note**
>
> [1] 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 esegue la transizione dei 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 FSx console Amazon, l' FSx API Amazon AWS CLI, l'interfaccia a riga di ONTAP comando e l'API REST.

Per impostare il periodo di conservazione con l' FSx API Amazon, utilizza la `SnaplockRetentionPeriod`configurazione. Nella FSx console Amazon, per Periodo di conservazione, inserisci i valori per Conservazione predefinita, Conservazione minima e Conservazione massima. Quindi scegli un'unità corrispondente per ciascuna.

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 FSx console Amazon AWS CLI, l' FSx API Amazon 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' FSx API Amazon, usa `AutocommitPeriod` in. `CreateSnaplockConfiguration` Nella FSx console Amazon, per Autocommit, scegli Enabled. Quindi, per il periodo Autocommit, inserisci un valore e scegli l'unità Autocommit corrispondente.

È possibile specificare un valore compreso tra 5 minuti e 10 anni.

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 FSx console Amazon, AWS CLI l' FSx API Amazon e l'API CLI ONTAP e REST.

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' FSx API Amazon, usa in. `VolumeAppendModeEnabled` `CreateSnaplockConfiguration` Nella FSx console Amazon, per la modalità Volume append, scegli Enabled.

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.

Creazione di una politica EBR nella CLI ONTAP

Per creare una politica EBR nella CLI ONTAP

- Eseguire il seguente comando seguente. Sostituisci *p1* e *"10 years"* con le tue informazioni.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

Applicazione di una politica EBR nella CLI ONTAP

Per applicare una politica EBR nella CLI ONTAP

- Eseguire il seguente 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 /
```

Modifica di una politica EBR nella CLI ONTAP

Per modificare una politica EBR nella CLI ONTAP

- Eseguire il seguente comando seguente. Sostituisci *p1* e *"5 years"* con le tue informazioni.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

Eliminazione di una politica EBR nella CLI ONTAP

Per eliminare una politica EBR nella CLI ONTAP

- Eseguire il seguente comando seguente. *p1*Sostituiscila 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 legale

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.

Avvio di una conservazione a fini legali su un file in un volume di SnapLock conformità con la ONTAP CLI

Per avviare una conservazione a fini legali su un file in un volume SnapLock Compliance con la ONTAP CLI

- Eseguire il seguente comando seguente. Sostituisci *`litigation1`* e *`file1`* con le tue informazioni. *`slc_vol1`*

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

Avvio di una conservazione a fini legali su tutti i file in un volume SnapLock Compliance con la ONTAP CLI

Per avviare una conservazione a fini legali su tutti i file in un volume SnapLock Compliance con la ONTAP CLI

- Eseguire il seguente comando seguente. Sostituisci *litigation1* e *slc_vol1* con le tue informazioni.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /
```

Interruzione della conservazione a fini legali di un file in un volume di SnapLock conformità con la ONTAP CLI

Per terminare una conservazione a fini legali su un file in un volume di SnapLock conformità con la ONTAP CLI

- Eseguire il seguente comando seguente. Sostituisci *litigation1* e *file1* con le tue informazioni. *slc_vol1*

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

> **Note**
>
> Ti consigliamo di monitorarli `-operation-status` con il `snaplock legal-hold show` comando quando esegui una conservazione a fini legali per assicurarti che non abbia esito negativo.

Fine del blocco a fini legali su tutti i file in un volume di SnapLock conformità con la ONTAP CLI

Per porre fine alla conservazione a fini legali su tutti i file in un volume SnapLock Compliance con la ONTAP CLI

- Eseguire il seguente 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 monitorarlo `-operation-status` con il `snaplock legal-hold show` comando quando esegui una conservazione a fini legali per assicurarti che non abbia esito negativo.

Comandi correlati disponibili nel NetAppDocumentation Center:

- snaplock legal-hold abort
- file di dump snaplock legal-hold
- controversie legali su snaplock legal-hold dump-
- snaplock legal-hold show

Replica dei dati con FlexCache

FlexCacheè una funzionalità di caching NetApp ONTAP's remoto che avvicina i set di dati ai clienti, migliorando le prestazioni di accesso e riducendo i costi. Semplifica la distribuzione dei file e riduce i costi della WAN. Quando si crea un FlexCache volume, inizialmente vengono copiati solo i metadati dal file system di origine. Questo approccio è più rapido ed efficiente in termini di spazio rispetto a una copia completa dei dati, poiché consuma solo una frazione della capacità di storage.

Funzionamento di FlexCache

Un FlexCache volume è una cache scarsamente popolata che fornisce l'accesso ai dati archiviati in un volume di origine. La cache può essere posizionata in un file system diverso, facoltativamente remoto. Invece di copiare tutti i dati dal volume di origine, FlexCache copia i dati solo se necessario. FlexCachei volumi sono più adatti per flussi di lavoro ad alta intensità di lettura con modifiche dei dati poco frequenti, poiché qualsiasi modifica ai dati di origine richiede l'aggiornamento della cache.

È possibile utilizzare FlexCache with FSx for ONTAP nelle seguenti configurazioni:

Volume Origin	FlexCache volume
In sede NetApp ONTAP	FSx per ONTAP
FSx per ONTAP	In sede NetApp ONTAP
FSx per ONTAP	FSx per ONTAP

FlexCachemodalità di scrittura

FlexCachei volumi supportano due modalità operative per le operazioni di scrittura: modalità write-around e modalità write-back.

In modalità write-around, che è la modalità predefinita, le scritture vengono inoltrate dalla cache al volume di origine. L'operazione di scrittura viene riconosciuta al client solo dopo che i dati sono stati salvati nel volume di origine e l'origine non riconosce la scrittura nella cache. Poiché ogni scrittura deve attraversare la rete tra la cache e l'origine, questa modalità ha una latenza maggiore rispetto alla modalità write-back.

Nella modalità write-back, introdotta nella versione ONTAP 9.15.1, le scritture vengono salvate nella cache e immediatamente riconosciute al client. I dati vengono quindi scritti in modo asincrono nel volume di origine. Questa modalità consente di eseguire le scritture a velocità prossime a quelle locali, il che può migliorare significativamente le prestazioni per i carichi di lavoro distribuiti.

Utilizza la modalità write-back per carichi di lavoro con elevata intensità di scrittura che richiedono scritture nella cache a bassa latenza. Utilizza la modalità write-around per carichi di lavoro pesanti in lettura che non sono sensibili alla latenza o quando il file system di origine ha più di 10 volumi di origine. FlexCache

FlexCachepanoramica sulla creazione di volumi

La creazione di un FlexCache volume prevede i seguenti passaggi:

1. Raccogli le interfacce logiche di origine e di destinazione () LIFs
2. Stabilisci il peering del cluster tra il file system di origine e quello di cache
3. Crea una relazione di peering tra una macchina virtuale di archiviazione (SVM)
4. Crea il FlexCache volume e seleziona una modalità di scrittura
5. Installa il FlexCache volume sui tuoi client

Per istruzioni dettagliate, vedi Creazione di una FlexCache.

Creazione di una FlexCache

Utilizzando le seguenti procedure, creerai un FlexCache volume su un file system Amazon FSx for NetApp ONTAP, supportato da un volume di origine situato in un cluster localeNetApp ONTAP.

Utilizzo della CLI ONTAP

Utilizzerai la ONTAP CLI per creare e gestire una FlexCache configurazione sul tuo file system FSx for ONTAP.

I comandi di queste procedure utilizzano i seguenti alias per cluster, SVM e volume:

- `Cache_ID`— l'ID del cluster di cache (nel formato FSx IDABCDEF1234567890a)
- `Origin_ID`— l'ID del cluster di origine
- `CacheSVM`— il nome SVM della cache
- `OriginSVM`— il nome SVM di origine
- `OriginVol`— il nome del volume di origine
- `CacheVol`— il nome FlexCache del volume

Le procedure in questa sezione utilizzano i seguenti comandi NetApp ONTAP CLI.

- `network interfaces show`
- Comandi `cluster peer`
- `volume flexcache create`

Prerequisiti

Prima di iniziare a utilizzare le procedure descritte nelle sezioni seguenti, accertatevi di aver soddisfatto i seguenti prerequisiti:

- I file system di origine e di destinazione sono collegati nello stesso VPC o si trovano in reti peerizzate che utilizzano Amazon VPC,, o. AWS Transit Gateway Direct Connect Site-to-Site VPN Per ulteriori informazioni, consulta Accesso ai dati dall'interno di Cloud 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 11104 e 11105 per gli endpoint intercluster (). LIFs
- È stata creata una destinazione FSx per il file system ONTAP con un SVM, ma non è stato creato il volume che verrà utilizzato come. FlexCache Per ulteriori informazioni, consulta Creazione di file system.

Registra l'intercluster di origine e destinazione LIFs

1. Per il file system FSx for ONTAP che è il cluster di destinazione:

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

   b. Scegli File system, quindi scegli il FSx file system ONTAP che è il cluster di destinazione per aprire la pagina dei dettagli del file system.

   c. In Amministrazione, individua l'endpoint inter-cluster - Indirizzi IP e registra il valore.

   > **Note**
   >
   > Per i file system con scalabilità orizzontale, sono disponibili due indirizzi IP degli endpoint intercluster per ogni coppia ad alta disponibilità (HA).

2. Per il cluster di origine locale, recupera gli indirizzi IP LIF tra cluster utilizzando il seguente comando CLI: ONTAP

```
Origin::> network interface show -role intercluster
Logical                         Network
Vserver     Interface  Status    Address/Mask
----------- ---------- -------   ------------
OriginSVM
            inter_1     up/up    10.0.0.36/24
            inter_2     up/up    10.0.1.69/24
```

3. `inter_1inter_2` IPSalva gli indirizzi e. A essi si fa riferimento nell'`OriginSVM`alias `origin_inter_1` and `origin_inter_2` e nell'`CacheSVM`alias as and. `cache_inter_1` `cache_inter_2`

Stabilisci il peering del cluster tra l'origine e la cache

Stabilisci una relazione peer del cluster sul Source cluster Cache and utilizzando il comando cluster peer createONTAPCLI. Fornirai gli indirizzi IP tra cluster salvati in precedenza nella procedura. Registra l'intercluster di origine e destinazione LIFs Quando richiesto, ti verrà chiesto di crearne uno *cluster-peer-passphrase* a cui dovrai accedere quando stabilirai il peering del cluster sul cluster. Origin

1. Configura il peering del cluster sul `Cache` cluster (il tuo file system FSx for ONTAP).

   a. Per accedere alla ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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. Utilizzate il seguente comando e registrate la password che avete creato. Per i file system con scalabilità orizzontale, fornite gli indirizzi `inter_2` IP `inter_1` e gli indirizzi IP per ogni coppia HA.

   ```
   FSx-Cache::> cluster peer create -address-family ipv4 -peer-
   addrs origin_inter_1,origin_inter_2

   Enter the passphrase: cluster-peer-passphrase
   Confirm the passphrase: cluster-peer-passphrase
   Notice: Now use the same passphrase in the "cluster peer create" command in the
    other cluster.
   ```

2. Utilizzate il comando seguente per configurare il peering del cluster sul cluster `source` (locale). Dovrai inserire la passphrase che hai creato nel passaggio precedente per autenticarti. Per i file system con scalabilità orizzontale, è necessario fornire l'indirizzo IP tra cluster per ogni coppia HA.

   ```
   Origin::> cluster peer create -address-family ipv4 -peer-
   addrs cache_inter_1,cache_inter_2

   Enter the passphrase: cluster-peer-passphrase
   Confirm the passphrase: cluster-peer-passphrase
   ```

3. Sul `source` cluster, verifica che il peering del cluster sia stato configurato correttamente utilizzando il comando seguente. Nell'output, `Availability` dovrebbe essere impostato su. `Available`

```
Origin::> cluster peer show

Peer Cluster Name     Availability    Authentication
-------------------   -------------   --------------
Cache_ID              Available       ok
```

Se l'output non viene visualizzato`Available`, ripeti i passaggi precedenti sui `cache` cluster `source` and.

Configura il peering della macchina virtuale di archiviazione (SVM)

Dopo aver stabilito correttamente il peering del cluster, il passaggio successivo consiste nel creare una relazione di peering SVM sul cluster di cache (Cache) utilizzando il comando. vserver peer Gli alias aggiuntivi utilizzati nella procedura seguente sono i seguenti:

- *`CacheLocalName`*— il nome utilizzato per identificare la `cache` SVM durante la configurazione del peering SVM sulla SVM. `origin`
- *`OriginLocalName`*— il nome utilizzato per identificare la `origin` SVM durante la configurazione del peering SVM sulla SVM. `cache`

1. Sulla `cache` SVM, utilizzate il seguente comando per creare una relazione di peering SVM.

```
FSx-Cache::> vserver peer create -vserver CacheSVM -peer-vserver OriginSVM -peer-
cluster Origin_ID -local-name OriginLocalName -application flexcache
```

2. Nel cluster di origine, utilizzate il comando seguente per accettare la relazione di peering SVM.

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-
name CacheLocalName
```

3. Nel cluster di origine, accettate la relazione di peering.

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-
name CacheLocalName
```

4. Verificate che il peering SVM sia andato a buon fine utilizzando il seguente comando; `Peer State` dovrebbe essere impostato su `peered` nella risposta.

```
Origin::> vserver peer show

Vserver      Peer Vserver    Peer State    Peering Cluster    Remote Applications

------------ --------------- ------------- ------------------
 ------------------------
OriginSVM    CacheSVM        peered        FSx-Cache          flexcache
```

Create il volume FlexCache

Dopo aver creato correttamente la relazione di peering SVM, il passaggio successivo consiste nel creare il FlexCache volume sulla cache SVM. Il FlexCache volume deve essere un. FlexGroup Sceglierai anche una modalità operativa per il tuo FlexCache volume. Per ulteriori informazioni, consulta FlexCachemodalità di scrittura.

1. Nel cluster di cache, usa il seguente comando ONTAP CLI per creare FlexCache il volume. L'esempio crea un FlexCache volume da 2 TB denominato. *`CacheVol`*

   - Per creare un FlexCache volume di tipo write-around, utilizzate il comando seguente.

   ```
   FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
    -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
   aggr-list aggr1
   ```

   - Per creare un FlexCache volume di riscrittura, utilizzate il comando seguente.

   ```
   FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
    -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
   aggr-list aggr1 -is-writeback-enabled true
   ```

> **Note**
>
> È possibile utilizzare il `volume flexcache config modify -is-writeback-enabled {true|false}`comando per modificare la modalità di scrittura. Prima di

utilizzare questo comando, assicurati di accedere alla modalità avanzata CLI di ONTAP utilizzando `set -privilege advanced`il comando.

2. Verificate la FlexCache relazione tra il FlexCache volume e il volume di origine.

   - Per un volume di FlexCache scrittura, l'output sarà simile all'esempio seguente.

```
FSx-Cache::> volume flexcache show

Vserver   Volume      Size     Origin-Vserver  Origin-Volume  Origin-Cluster
-------   ----------  -------  --------------  -------------  --------------
CacheSVM  CacheVol    2TB      OriginSVM       OriginVol      Origin
```

   - Per un volume FlexCache di riscrittura, l'output sarà simile all'esempio seguente.

```
FSx-Cache::> volume flexcache show

Vserver   Volume      Size     Origin-Vserver  Origin-Volume  Origin-Cluster
 Writeback
-------   ----------  -------  --------------  -------------  --------------
 ---------
CacheSVM  CacheVol    2TB      OriginSVM       OriginVol      Origin
 true
```

Montare il volume FlexCache

Una volta che il FlexCache volume diventa DISPONIBILE NFSv3 NFSv4, i client SMB possono montarlo. Una volta FlexCache montato, i client hanno accesso all'intero set di dati sul volume di origine locale.

- Per creare un punto di montaggio e montare il FlexCache, esegui i seguenti comandi sul client:

```
$ sudo mkdir -p /fsx/CacheVol
$ sudo mount -t nfs management.fs-01d2f606463087f6d.fsx.us-east-1.amazonaws.com:/
CacheVol /fsx/CacheVol
```

Replica dei dati utilizzando NetApp SnapMirror

È possibile utilizzarla 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 SnapMirrorreplica i dati a velocità elevate, in modo da ottenere un'elevata disponibilità dei dati e una replica rapida dei dati su tutti i ONTAP sistemi, indipendentemente dal fatto che si esegua la replica tra due FSx file system Amazon 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 a RPOs (Recovery Point Objectives), RTOs (Recovery Time Objectives) e a considerazioni relative alle prestazioni.

Quando si replicano i dati su sistemi di NetApp storage e si aggiornano continuamente i dati secondari, i dati vengono mantenuti aggiornati e rimangono disponibili ogni volta che è necessario. Non sono necessari server di replica esterni. Per ulteriori informazioni sull'utilizzo NetApp SnapMirror per replicare i dati, consulta Informazioni sulla NetApp replica nella documentazione. NetApp Console

Puoi creare un volume di destinazione per la protezione dei dati (DP) per NetApp SnapMirror utilizzare la FSx console Amazon AWS CLI, l'API Amazon e l' FSx API Amazon, oltre alla NetApp ONTAP CLI e all'API REST. Per informazioni sulla creazione di un volume di destinazione utilizzando la FSx console Amazon e AWS CLI, consultaCreazione di volumi.

È possibile utilizzare NetApp Console o la ONTAP CLI per pianificare la replica per il file system.

> **Note**
>
> Esistono due tipi di SnapMirror replica: a livello di volume SnapMirror e SVM Disaster Recovery (SVMDR). for ONTAP supporta solo la replica a livello di volumeSnapMirror. FSx Synchronous SnapMirror, inclusoStrictSync, non è supportato.

Utilizzo NetApp Console per pianificare la replica

È possibile utilizzare NetApp Console per configurare la replica con il file SnapMirror system FSx for ONTAP. Per ulteriori informazioni, consulta Configurare la replica dei dati nella NetApp replica nella documentazione della console. NetApp

Utilizzo della ONTAP CLI per pianificare la replica

È possibile utilizzare la ONTAP CLI per configurare la replica pianificata dei volumi. Per informazioni, consulta Gestire la replica dei SnapMirror volumi nel Documentation Center. NetApp ONTAP

AWS report di fatturazione e utilizzo FSx per ONTAP

AWS fornisce due report di utilizzo FSx per ONTAP:

- Il rapporto di AWS fatturazione è una visualizzazione di alto livello di tutte le attività utilizzate, inclusa Servizi AWS FSx quella per ONTAP.
- Il rapporto AWS sull'utilizzo è un riepilogo delle attività per un servizio specifico, aggregato per ora, giorno o mese. Include anche tabelle di utilizzo che forniscono una rappresentazione grafica dell'utilizzo di FSx ONTAP.

> **Note**
>
> Come altri Servizi AWS, FSx ONTAP ti addebita solo ciò che utilizzi. Per ulteriori informazioni, consulta la pagina dei prezzi di Amazon FSx for NetApp ONTAP.

Visualizza il report di AWS fatturazione per ONTAP FSx

Puoi visualizzare un riepilogo dell' AWS utilizzo e degli addebiti, elencati per servizio, nella pagina Fatture della console. Gestione dei costi e fatturazione AWS

Per visualizzare il rapporto di AWS fatturazione

1. Accedi a Console di gestione AWS e apri la Gestione dei costi e fatturazione AWS console all'indirizzo https://console.aws.amazon.com/costmanagement/.
2. Nel riquadro di navigazione selezionare Bills (Fatture).
3. Scegli un periodo di fatturazione (ad esempio, agosto 2024).
4. Per visualizzare gli FSx addebiti di Amazon, nella scheda Addebiti per servizio, inserisci FSxil campo di testo del filtro per servizio, quindi espandi FSxper visualizzare gli addebiti per Regione AWS.

   I costi FSx per i file system ONTAP vengono visualizzati nelle voci Amazon:ONTAP FSx CreateFileSystem del rapporto.
5. Per scaricare il rapporto di fatturazione dettagliato in formato CSV, scegli Scarica tutto in CSV nella parte superiore della pagina Fatture.

Per ulteriori informazioni sulla fattura, consulta Visualizzazione della AWS fattura nella Guida per l'utente. AWS Billing

Il rapporto di fatturazione include i seguenti tipi di utilizzo che si applicano FSx ai file system ONTAP:

First generation FSx for ONTAP file systems

Tipo di costo	Unità	Descrizione	
Archiviazione SSD ONTAP Single-AZ	GB/mese	La quantità di storage SSD fornita su un file system Single-AZ ONTAP di prima generazione	
Archiviazione SSD ONTAP Multi-AZ	GB/mese	La quantità di storage SSD fornita su un file system Multi-AZ for ONTAP di prima generazione FSx	
Capacità di throughput ONTAP Single-AZ	MBps-Mese	La quantità di capacità di throughput fornita su un file system FSx Single-AZ per ONTAP di prima generazione	
Capacità di throughput ONTAP Multi-AZ	MBps-Mese	La quantità di capacità di throughput fornita su un file system FSx Multi-AZ for ONTAP di prima generazione	
IOPS SSD ONTAP Single-AZ forniti	IOPS al mese	La quantità di IOPS SSD assegnati su un file system Single-AZ per ONTAP di prima generazione FSx	
IOPS SSD ONTAP Multi-AZ forniti	IOPS al mese	La quantità di IOPS SSD assegnati su un file system Multi-AZ per ONTAP di prima generazione FSx	

Second generation FSx for ONTAP file systems

Tipo di costo	Unità	Descrizione	
Archiviazione SSD ONTAP Single-AZ-2	GB/mese	La quantità di storage SSD fornita su un file system Single-AZ for ONTAP di seconda generazione FSx	
Archiviazione SSD ONTAP Multi-AZ-2	GB/mese	La quantità di storage SSD fornita su un file system Multi-AZ for ONTAP di seconda generazione FSx	
Capacità di throughput ONTAP Single-AZ-2	MBps-Mese	La quantità di capacità di throughput fornita su un file system Single-AZ per ONTAP di seconda generazione FSx	
Capacità di throughput ONTAP Multi-AZ-2	MBps-Mese	La quantità di capacità di throughput fornita su un file system Multi-AZ per ONTAP di seconda generazione FSx	
IOPS SSD ONTAP Single-AZ -2 forniti	IOPS al mese	La quantità di IOPS SSD assegnati su un file system Single-AZ per ONTAP di seconda generazione FSx	
IOPS SSD ONTAP Multi-AZ-2 forniti	IOPS al mese	La quantità di IOPS SSD assegnati su un file system Multi-AZ per ONTAP di seconda generazione FSx	

All FSx for ONTAP filesystems

Tipo di costo	Unità	Descrizione	
Storage in pool con capacità standard ONTAP	GB/mese	La quantità di storage del pool di capacità utilizzata dal file system FSx for ONTAP.	
Archiviazione di backup ONTAP	GB/mese	La quantità di capacità di archiviazione utilizzata per i backup	
SnapLock utilizzo	GB/mese	La quantità di capacità di archiviazione utilizzata da SnapLock volumi	
Leggi le richieste nello storage del pool di capacità standard ONTAP	Operazioni	Il numero di richieste di lettura effettuate allo storage con pool di capacità standard su un file system FSx for ONTAP	
Scrivi le richieste su ONTAP Standard Capacity Pool Storage	Operazioni	Il numero di richieste di scrittura effettuate sullo storage con pool di capacità standard su un file system FSx for ONTAP	

Visualizza il report AWS sull'utilizzo di FSx ONTAP

AWS fornisce un rapporto FSx sull'utilizzo più dettagliato del rapporto di fatturazione. Il rapporto sull'utilizzo fornisce dati di utilizzo aggregati per ora, giorno o mese ed elenca le operazioni per regione e tipo di utilizzo.

Per visualizzare il rapporto sull' AWS utilizzo

1. Accedi a Console di gestione AWS e apri la Gestione dei costi e fatturazione AWS console all'indirizzo https://console.aws.amazon.com/costmanagement/.
2. Nel pannello di navigazione, scegliere Cost Explorer.
3. Nella sezione Parametri del rapporto, scegli l'intervallo di date e la granularità del rapporto.
4. Lascia la dimensione Raggruppa per > impostata su Servizio.
5. In Filtri > Servizio, scegli FSx
6. Scegli il tipo di utilizzo. Consulta la tabella che segue questa procedura per un elenco dei tipi di FSx utilizzo di ONTAP.
7. Effettua eventuali selezioni di filtri aggiuntivi per il rapporto.
8. Per scaricare i dettagli del rapporto in un file, scegli Scarica come CSV.

La tabella seguente elenca i tipi di utilizzo di ONTAP che puoi utilizzare FSx per filtrare il rapporto e visualizzare i dati di utilizzo per i file system ONTAP. Per ulteriori informazioni sull'utilizzo di Cost Explorer, consulta la sezione Analisi dei costi e dell'utilizzo AWS Cost Explorer nella Guida per l' AWS Cost Management utente.

First generation FSx for ONTAP file systems

Tipo di utilizzo	Unità	Descrizione
region-storage.saz_2n: SSD	GB/mese	La quantità di storage SSD fornita su un file system Single-AZ for ONTAP di prima generazione. FSx
region- storage.maz: SSD	GB/mese	La quantità di storage SSD fornita su un file system Multi-AZ for ONTAP di prima generazione. FSx
*region*ThroughputCapacity - .SAZ_2N	MiBps-No	La quantità di capacità di throughput fornita su un file system Single-AZ FSx for ONTAP di prima generazione.

Tipo di utilizzo	Unità	Descrizione
*region*ThroughputCapacity- .MAZ	MiBps-No	La quantità di capacità di throughput fornita su un file system Multi-AZ FSx for ONTAP di prima generazione.
region- SSDIOPS.SAZ_2N fornito	IOPS-MO	La quantità di IOPS SSD fornita superiore a 3 IOPS per GiB di storage SSD su un file system Single-AZ for ONTAP di prima generazione. FSx
region- SSDIOPS.maz fornito	IOPS-MO	La quantità di IOPS SSD fornita superiore a 3 IOPS per GiB di storage SSD su un file system Multi-AZ for ONTAP di prima generazione. FSx

Second generation FSx for ONTAP file systems

Tipo di utilizzo	Unità	Descrizione
region-storage.SAZ_2N2: SSD	GB/mese	La quantità di storage SSD fornita su un file system Single-AZ for ONTAP di seconda generazione. FSx
region-Archiviazione. MAZ2-Archiviazione. ----SEP----:SSD	GB/mese	La quantità di storage SSD fornita su un file system Multi-AZ for ONTAP di seconda generazione. FSx
*region*ThroughputCapacity - .SAZ_2N2	MiBps-No	La quantità di capacità di throughput fornita su un file system FSx Single-AZ for ONTAP di seconda generazione.

Tipo di utilizzo	Unità	Descrizione
region-ThroughputCapacity.MAZ2	MiBps-No	La quantità di capacità di throughput fornita su un file system FSx Multi-AZ for ONTAP di seconda generazione.
region- SSDIOPS.SAZ_2N2 fornito	IOPS-MO	La quantità di IOPS SSD fornita superiore a 3 IOPS per GiB di storage SSD su un file system Single-AZ for ONTAP di seconda generazione. FSx
region- DIOPS SSD forniti. MAZ2	IOPS-MO	La quantità di IOPS SSD fornita superiore a 3 IOPS per GiB di storage SSD su un file system Multi-AZ for ONTAP di seconda generazione. FSx

All FSx for ONTAP file systems

Tipo di utilizzo	Unità	Descrizione
*region*CPool-storage.SAZ_2N: Standard	Gb-mese	La quantità di storage in pool a capacità standard utilizzata su un file system Single-AZ FSx for ONTAP di prima o seconda generazione.
region-Storage.maz: Standard CPool	Gb-mese	La quantità di storage in pool a capacità standard utilizzata su un file system Multi-AZ FSx for ONTAP di prima o seconda generazione.
region-BackupUsage	GB/mese	La quantità di capacità di storage utilizzata per i backup.

Tipo di utilizzo	Unità	Descrizione
region-SnaplockUsage	GB/mese	La quantità di capacità di archiviaz ione utilizzata da SnapLock volumi.
region-richieste.saz_2n: CPool StdRd	Operazioni	Il numero di richieste di lettura effettuate allo storage in pool di capacità standard su un file system Single-AZ for ONTAP. FSx
region-Requests.SAZ_2N: CPool StdWr	Operazioni	Il numero di richieste di scrittura effettuate sullo storage in pool di capacità standard su un file system Single-AZ for ONTAP. FSx
region-Requests.maz: CPool StdRd	Operazioni	Il numero di richieste di lettura effettuate allo storage in pool di capacità standard su un file system Multi-AZ FSx for ONTAP.
region-Requests.maz: CPool StdWr	Operazioni	Il numero di richieste di scrittura effettuate su un pool di storage a capacità standard su un file system Multi-AZ FSx for ONTAP.

Monitoraggio di Amazon FSx per NetApp ONTAP

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 di ONTAP in metriche leggibili. FSx 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 Data Infrastructure Insights: è possibile monitorare le metriche di configurazione, capacità e prestazioni per i file system FSx for ONTAP utilizzando il servizio Data Infrastructure Insights. NetApp Puoi anche creare avvisi in base a condizioni metriche.
- NetApp Harvest e NetApp Grafana: puoi monitorare il tuo file system FSx for ONTAP utilizzando Harvest NetApp e Grafana. NetApp NetApp Harvest monitora i file system ONTAP raccogliendo le metriche relative a prestazioni, capacità e hardware dai file system ONTAP. FSx Grafana fornisce una dashboard in cui è possibile visualizzare le metriche Harvest raccolte.
- AWS CloudTrail— Puoi 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 for NetApp 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. FSx per impostazione predefinita, i dati metrici per ONTAP vengono inviati automaticamente a CloudWatch intervalli di 1 minuto. Per ulteriori informazioni su CloudWatch, consulta What is Amazon CloudWatch? nella Amazon CloudWatch User Guide.

> **Note**
>
> Per impostazione predefinita, FSx per ONTAP invia i dati delle metriche CloudWatch a periodi di 1 minuto, ad eccezione delle seguenti metriche che vengono inviate a intervalli di 5 minuti:
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

CloudWatch le metriche FSx per 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: parametri relativi File-system-level alle prestazioni e alla capacità di archiviazione.
- Metriche del file server: metriche. File-server-level
- Metriche dettagliate di aggregazione del file system: metriche dettagliate del file system per aggregato.
- Metriche dettagliate del file system: parametri di File-system-level storage 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 FSx per ONTAP vengono pubblicate nel namespace in. `AWS/FSx` CloudWatch

Argomenti

Accesso alle CloudWatch metriche

Puoi visualizzare i CloudWatch parametri Amazon per Amazon FSx nei seguenti modi:

- La FSx console Amazon
- La CloudWatch console Amazon
- Il AWS Command Line Interface (AWS CLI) per CloudWatch
- L' CloudWatch API

La procedura seguente spiega come visualizzare le CloudWatch metriche del file system con la FSx console Amazon.

Per visualizzare le CloudWatch metriche per il tuo file system utilizzando la console Amazon FSx

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli File system, quindi scegli il 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 le CloudWatch metriche relative al volume utilizzando la console Amazon FSx

1. Apri la FSx console Amazon 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 FSx i parametri del file system ONTAP a una dashboard nella console Amazon CloudWatch .

Per aggiungere metriche a una console Amazon CloudWatch

1. Scegli il set di parametri (Riepilogo, Archiviazione o Prestazioni) nel pannello Monitoraggio e prestazioni della FSx console Amazon.
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 API GetMetricStatistics. Per ulteriori informazioni, consulta Amazon CloudWatch API Reference.

Monitoraggio nella FSx console Amazon

Le CloudWatch metriche riportate da Amazon FSx forniscono informazioni preziose sui tuoi file system e volumi FSx for ONTAP.

Argomenti

- Monitoraggio dei parametri del file system nella console Amazon FSx
- Monitoraggio delle metriche del volume nella console Amazon FSx
- Avvertenze e raccomandazioni sulle prestazioni
- Creazione di CloudWatch allarmi Amazon per monitorare 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 FSx console Amazon per visualizzare le metriche descritte nella tabella seguente. Per ulteriori informazioni, consulta Accesso alle CloudWatch metriche.

Monitoraggio e prestazioni	Come posso...	Grafico	Metriche pertinenti
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 del client (byte/sec)	SUM (`DataReadBytes +DataWriteBytes`) /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/ `DataWriteOperationTime DataWriteOperations` Latenza media dei metadati: * 1000/ `Metadata0`

Monitoraggio e prestazioni	Come posso...	Grafico	Metriche pertinenti
			`perationTime` `MetadataOperations`
	... 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`
Storage	... determinare la quantità di storage principale disponibile?	Capacità di archiviazione principale disponibile (byte)	`StorageCapacity {SSD} - StorageUsed {SSD}`

Monitoraggio e prestazioni	Come posso...	Grafico	Metriche pertinenti
	... determinare la percentuale di storage principale utilizzato per il mio file system?	Utilizzo della capacità di storage principale (percentuale)	`StorageUsed {SSD} * 100/ StorageCapacity {} SSD`
Prestazioni del file server	... determinare se il mio file system si sta avvicinando al limite di velocità di trasmissione della 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`

Monitoraggio e prestazioni	Come posso...	Grafico	Metriche pertinenti
	... determinare se il mio file system si sta avvicinando al limite di IOPS SSD dei relativi file server?	IOPS del disco: utilizzo (percentuale)	`FileServerDiskIopsUtilization`
	... 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 NVMe lettura del mio file system?	Rapporto di accesso alla cache (percentuale)	`FileServerCacheHitRatio`

Monitoraggio e prestazioni	Come posso...	Grafico	Metriche pertinenti
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 FSx console Amazon per visualizzare ulteriori metriche prestazionali. Per ulteriori informazioni, consulta Accesso alle CloudWatch metriche.

Monitoraggio	Come posso...	Grafico	Metriche pertinenti
	... determinare la capacità di archiviazione disponibile del mio volume?	Capacità di archiviazione	`StorageCapacity`

Monitoraggio	Come posso...	Grafico	Metriche pertinenti
		disponibile	
	... 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` Operazioni di scrittura: `CapacityPoolWriteOperations`

Monitoraggio	Come posso...	Grafico	Metriche pertinenti
	... 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`

Avvertenze e raccomandazioni sulle prestazioni

FSx for ONTAP visualizza un avviso relativo alle 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 FSx sulle prestazioni di Amazon 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 delle metriche.

Puoi creare CloudWatch allarmi per qualsiasi parametro 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 capacità di archiviazione SSD massima. Per ulteriori informazioni, consulta Aggiornamento della capacità di archiviazione e provisioning degli IOPS. 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. Bilanciamento dei carichi di lavoro tra coppie HA Se attualmente stai eseguendo un'operazione di riduzione dell'SSD e l'utilizzo supera l'80% sul nuovo set di dischi, puoi suddividere i dati nel pool di capacità, eliminare i dati dai volumi che sono stati reindirizzati ai nuovi dischi o inviare una richiesta per aumentare la capacità dell'SSD durante l'operazione di riduzione

Sezione Dashboard	Se è presente un avviso per questa metrica	Esegui questa operazione
		. Amazon FSx darà priorità alla richiesta di aumento prima di riprendere l'operazione di riduzione. Per ulteriori informazioni, consulta Per ridurre la capacità di archiviazione SSD per un file system (console).
Prestazioni del file server	Throughput di rete	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. Aggiornamento della 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. Bilanciamento dei carichi di lavoro tra coppie HA
	Velocità effettiva del disco	
	IOPS del disco	
	Utilizzo CPU	

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. Aggiornamento della capacità di archiviazione e provisioning degli IOPS 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. Bilanciamento dei carichi di lavoro tra coppie HA

> **Note**
>
> Durante un'operazione di riduzione delle prestazioni di un SSD, i carichi di lavoro con elevati livelli di scrittura potrebbero subire un temporaneo peggioramento delle prestazioni in quanto l'operazione consuma le risorse del disco e della rete. Per ridurre al minimo l'impatto sulle prestazioni, prima di avviare un'operazione di riduzione dell'SSD, è consigliabile mantenere un margine di crescita adeguato assicurandosi che i carichi di lavoro continui non consumino costantemente più del 50% della CPU, del 50% della velocità di trasmissione del disco o del 50% di IOPS SSD.
> Potrebbero verificarsi brevi I/O pause fino a 60 secondi per ogni volume quando l'accesso del client viene reindirizzato al nuovo set di dischi. Queste pause sono previste e sono normali durante la fase di cutover dell'operazione.

Per ulteriori informazioni sulle prestazioni del file system, vedere. Amazon FSx per le prestazioni di NetApp 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 una singola metrica 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 FSx console Amazon o dalla CloudWatch console Amazon.

Le seguenti procedure descrivono come creare allarmi utilizzando la FSx console Amazon, AWS Command Line Interface (AWS CLI) e l'API.

Per impostare allarmi utilizzando la console Amazon FSx

1. Apri la FSx console Amazon all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel riquadro di navigazione a sinistra, scegli File system, quindi scegli il 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 Seleziona metrica.
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. Scegli Next (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 allarmi utilizzando la FSx console Amazon, a partire dal passaggio 6.

Per impostare una sveglia utilizzando il AWS CLI

- Chiama il put-metric-alarmcomando CLI. 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 API PutMetricAlarm. 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 `FileSystemId` e`StorageTier`. `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 per 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 archiviazione). `DiskReadBytes`

Argomenti

- Metriche di rete I/O

- Metriche del file server
- I/O Metriche del disco
- Parametri della capacità di archiviazione
- Metriche dettagliate del file system

Metriche di rete I/O

Tutte queste metriche hanno una sola dimensione,. `FileSystemId`

Metrica	Description
`NetworkThroughputUtilization`	La percentuale di utilizzo del throughput di rete per il file system. Tieni presente che questa metrica riflette la direzione, ad esempio in entrata o in uscita, che ha il flusso di traffico più elevato. Per visualizzare le singole metriche per ogni direzione, consulta le metriche and. NetworkReceivedBytes NetworkSentBytes 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.

Metrica	Description
	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. 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`

Metrica	Description
`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`
`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 I/O operazioni avvenute in un periodo specifica to. 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`

Metrica	Description
`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 I/O operazioni avvenute in un periodo specifica to. 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 sui metadati (I/O di rete) da parte dei client al file system. La `Sum` statistica è il numero totale di I/O operazioni avvenute in un periodo specifica to. 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`

Metrica	Description
`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`
`DataWriteOperationTime`	La somma del tempo totale impiegato all'interno 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`

Metrica	Description
`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`

Metrica	Description
`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`

Metrica	Description
`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`

Metrica	Description
`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`

Metrica	Description
`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.

Metrica	Description
	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 periodo specificato. 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`

Metrica	Description
`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 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`

Metrica	Description
`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 il cui provisioning è dotato di una capacità di throughput 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`

Metrica	Description
`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`

Metrica	Description
`FileServerCacheHitRatio`	La percentuale di tutte le richieste di lettura servite dai dati presenti nella RAM e nelle NVMe cache del file system. Una percentua le 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`

I/O Metriche del disco

Tutte queste metriche hanno una sola dimensione,. `FileSystemId`

Metrica	Description
`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.

Metrica	Description
	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`

Metrica	Description
`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`

Metrica	Description
`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`

Metrica	Description
`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, in 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.

Metrica	Description
	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`

Metrica	Description
`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.

Metrica	Description
`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

Metrica	Description
	Statistiche valide:`Average`,, e `Minimum` `Maximum`
`StorageCapacity`	La capacità di archiviazione totale del livello primario (SSD). Unità: byte Statistiche valide: `Maximum`

Metrica	Description
`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 di seconda generazione

Le seguenti metriche sono fornite FSx per i file system ONTAP di seconda generazione. 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 rete I/O

Tutte queste metriche assumono due dimensioni, `FileSystemId` e. `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.

Metrica	Description
`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`

Metrica	Description
	`ceivedBytes` in percentuale della capacità di trasmissione di rete di una coppia HA per il file system. In questa metrica viene considera to 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 `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`

Metrica	Description
`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`

Metrica	Description
`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`

Metrica	Description
`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.

Metrica	Description
	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`

Metrica	Description
`FileServerDiskIopsUtilization`	L'utilizzo IOPS della capacità IOPS disponibile su disco per il file server, come percentuale del limite IOPS del disco. Ciò si differenzia 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`

Metrica	Description
`FileServerCacheHitRatio`	La percentuale di tutte le richieste di lettura fornite dai dati che risiedono nella RAM o nelle NVMe cache 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. I/O Viene preso in considerazione tutto, comprese le attività in background (come SnapMirror la suddivisi one in più livelli 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`

I/O Metriche del disco

Tutte queste metriche assumono due dimensioni, `FileSystemId` e. `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.

Metrica	Description
`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. Durante le operazioni di riduzione della capacità dell'SSD, questa metrica viene riportata sia per l'aggregato originale () che per il nuovo aggregato più `aggr1_old` piccolo (). `aggr1` La `Sum` statistica è il numero totale di byte letti ogni minuto dall'aggregato dato 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.

Metrica	Description
	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`

Metrica	Description
`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. Durante le operazioni di riduzione della capacità dell'SSD, questa metrica viene riportata sia per l'aggregato originale () che per il nuovo aggregato più `aggr1_old` piccolo (). `aggr1` La `Sum` statistica è il numero totale di byte scritti nell'aggregato dato nel periodo specificato. 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`

Metrica	Description
`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 `FileServerDiskIopsUtilization` 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 supportato 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. Durante le operazioni di riduzione della capacità dell'SSD, questa metrica viene riportata sia per l'aggregato originale () che per il nuovo aggregato più `aggr1_old` piccolo (). `aggr1` 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

Metrica	Description
	Statistiche valide:, e `Average` `Minimum` `Maximum`

Metrica	Description
`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. Durante le operazioni di riduzione della capacità dell'SSD, questa metrica viene riportata sia per l'aggregato originale () che per il nuovo aggregato più `aggr1_old` piccolo (). `aggr1` 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, utilizza la `Average` statistica e dividi il risultato per 60 (secondi). Unità: numero Statistiche valide:`Sum`,`Average`, e `Minimum` `Maximum`

Metrica	Description
`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. Durante le operazioni di riduzione della capacità dell'SSD, questa metrica viene riportata sia per l'aggregato originale () che per il nuovo aggregato più `aggr1_old` piccolo (). `aggr1` 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.

Metrica	Description
`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.

Metrica	Description
	La `Maximum` statistica è la quantità massima di utilizzo della capacità di storage per un dato aggregato nel periodo specificato. Durante le operazioni di riduzione della capacità dell'SSD, questa metrica viene riportata sia per l'aggregato originale () che per il nuovo aggregato più `aggr1_old` piccolo (). `aggr1` Unità: percentuale Statistiche valide:, e `Average` `Minimum` `Maximum`

Metrica	Description
`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. Durante le operazioni di riduzione della capacità dell'SSD, questa metrica viene riportata sia per l'aggregato originale () che per il nuovo aggregato più piccolo (`aggr1_old`). `aggr1` Unità: byte Statistiche valide:, e `Average` `Minimum` `Maximum`

Metrica	Description
`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. Durante le operazioni di riduzione della capacità dell'SSD, questa metrica viene riportata sia per l'aggregato originale () che per il nuovo aggregato più piccolo (`aggr1_old`). `aggr1` Unità: byte

Metrica	Description
	Statistiche valide:, e `Average` `Minimum` `Maximum`

Parametri di volume

Il tuo file system Amazon FSx for NetApp ONTAP può avere uno o più volumi in cui archiviare i tuoi dati. Ciascuno di questi volumi ha una serie di CloudWatch 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 rete I/O

Tutte queste metriche assumono due dimensioni, `FileSystemId` e. `VolumeId`

Metrica	Description
`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

Metrica	Description
	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) 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

Metrica	Description
`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 I/O operazioni (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`

Metrica	Description
`DataReadOperationTime`	La somma del tempo totale impiegato all'interno 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'interno 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`

Metrica	Description
`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`

Metrica	Description
`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`

Metrica	Description
`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`

Metrica	Description
`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: `Average`
`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: `Average`
`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.

Metrica	Description
`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`

Metrica	Description
`StorageCapacityUtilization`	La percentuale di spazio fisico su disco utilizzato dal volume. Unità: percentuale Statistiche valide: `Maximum`

Monitoraggio FSx degli eventi ONTAP EMS

È possibile monitorare FSx gli eventi del file system 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 una capacità FlexGroup quasi esaurita, il trasferimento manuale online 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 FSx per i file system 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: nome e 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/DD/YYYY 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 *sev_level* valore, 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 *ems_sev_level* valore, 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 *`text`* valore. La fonte è in genere un modulo software.
`-message-name` *`message_name`*	Seleziona gli eventi che corrispondono al *`message_name`* valore. I nomi dei messaggi sono descrittivi, 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. *`text`* 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 *integer* valore. Solo gli eventi che provengono dal kernel hanno numeri di generazione del kernel.
`-kernel-sequence-num` *integer*	Seleziona gli eventi che corrispondono al valore. *integer* Solo gli eventi che provengono dal kernel hanno numeri di sequenza del kernel.
`-action` *text*	Seleziona gli eventi che corrispondono al valore. *text* Il `action` campo descrive le eventuali azioni correttiv e da intraprendere per porre rimedio alla situazione.
`-description` *text*	Seleziona gli eventi che corrispondono al *text* valore. Il `description` campo descrive perché l'evento si è verificato e cosa significa.
`-filter-name` *filter_name*	Seleziona gli eventi che corrispondono al *filter_name* valore. Vengono visualizzati solo gli eventi inclusi dai filtri esistenti che corrispondono a questo valore.

Opzione evento	Descrizione
`-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 l'utente Utilizzo della CLI NetApp ONTAP 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.

> **Note**
>
> La destinazione Syslog deve trovarsi nella sottorete principale utilizzata dal file system.

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 l'utente Utilizzo della CLI NetApp ONTAP 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. Se hai selezionato TCP come*transport_protocol*, puoi utilizzare 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 Data Infrastructure Insights

NetApp Data Infrastructure Insights (precedentemente 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 Data Infrastructure Insights, puoi monitorare le metriche di configurazione, capacità e prestazioni nel tempo per comprendere le tendenze del tuo carico di lavoro e pianificare le esigenze future in termini di prestazioni e capacità di storage. Puoi anche creare avvisi basati su condizioni metriche che possono integrarsi con i flussi di lavoro e gli strumenti di produttività esistenti.

> **Note**
>
> Data Infrastructure Insights non è supportato per i file system di seconda generazione con più di una coppia HA.

Data Infrastructure Insights offre:

- Un'ampia gamma di metriche e log: raccogli 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 più efficiente per ONTAP. FSx Puoi anche utilizzare queste informazioni per pianificare quando saranno necessarie maggiori prestazioni o capacità per l'implementazione di for ONTAP. FSx

Per ulteriori informazioni, consulta la documentazione di Data Infrastructure Insights nella documentazione del prodotto NetApp ONTAP.

Monitoraggio 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 FSx per misurare le prestazioni e l'utilizzo della capacità di archiviazione del file system ONTAP.

Puoi monitorare il tuo file system Amazon FSx for NetApp ONTAP utilizzando Harvest eGrafana. NetApp Harvestmonitora i data ONTAP center raccogliendo parametri relativi a prestazioni, capacità e hardware dai file system FSx ONTAP. Grafanafornisce una dashboard in cui è possibile visualizzare le Harvest metriche raccolte.

Dashboard Harvest supportati

Amazon FSx for NetApp ONTAP espone un set di parametri diverso rispetto a quello locale. NetApp ONTAP Pertanto, solo le seguenti out-of-the-box Harvest dashboard contrassegnate con `fsx` sono attualmente supportate per l'uso con ONTAP. FSx In alcuni pannelli di queste dashboard potrebbero mancare informazioni non supportate.

- Raccolta: metadati
- ONTAP: Aggregato
- ONTAP: cDOT
- ONTAP: Cluster
- ONTAP: Conformità
- ONTAP: centro dati
- ONTAP: protezione dei dati
- KONTAP: LUN
- ONTAP: rete
- ONTAP: Nodo
- ONTAP: Qtree
- ONTAP: Sicurezza
- ONTAP: SnapMirror
- ONTAP: Destinazioni SnapMirror
- ONTAP: Fonti SnapMirror
- ONTAP: SVM
- ONTAP: Volume
- ONTAP: Volume di SVM
- ONTAP: analisi approfondita del volume

Le seguenti Harvest dashboard sono supportate da FSx for ONTAP, ma non sono abilitate per impostazione predefinita in. Harvest

- ONTAP: FlexCache
- SUL TOCCO: FlexGroup

- ONTAP: client NFS
- ONTAP: monitor Storepool NFSv4
- ONTAP: risoluzione dei problemi NFS
- ONTAP: namespace NVMe
- ONTAP: SMB
- ONTAP: carico di lavoro

Dashboard non supportati Harvest

I seguenti Harvest dashboard non sono supportati da FSx for ONTAP.

- ONTAP: disco
- ONTAP: funzionamento di un servizio esterno
- ONTAP: Analisi dei file system (FSA)
- ONTAP: spazio per la testa
- ONTAP: Health
- ONTAP: Richiesta MAV
- ONTAP: MetroCluster
- ONTAP: alimentazione
- ONTAP: Mensola
- ONTAP: archivi di oggetti S3

CloudFormation modello

Per iniziare, puoi implementare un CloudFormation modello che avvii automaticamente un' EC2 istanza Amazon che esegue Harvest e Grafana. Come input per il CloudFormation modello, specifichi l'`fsxadmin`utente e l'endpoint di FSx gestione Amazon 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 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 fsx-ontap-harvest-grafanatemplate.template. 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 EC2 istanze Amazon

Quando configuri il modello, fornisci il tipo di EC2 istanza Amazon. NetAppper la dimensione dell'istanza, la raccomandazione di s dipende dal numero di file system monitorati e dal numero di parametri che scegli 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 EC2 istanze Amazon, consulta la sezione Istanze generiche nella Amazon EC2 User Guide.

Regole della porta dell'istanza

Quando configuri l' EC2 istanza Amazon, 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 per il DNS. TCP/UDP Inoltre, per raggiungere l'endpoint è necessaria la porta 443 TCP per HTTPS e Internet Access.

Procedura di distribuzione

La procedura seguente configura e implementa la Harvest/Grafana soluzione. 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 AWS tuo account e le informazioni sui parametri per il modello elencato di seguito. Per ulteriori informazioni sulla creazione di un file system, consulta. Creazione di file system

Per avviare lo Harvest/Grafana stack di soluzioni

1. Scarica il fsx-ontap-harvest-grafanatemplate.template. CloudFormation 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**
   >
   > 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 FSx endpoint e le quote di Amazon 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 EC2 istanza Amazon. Di seguito sono riportati i tipi di `t3` istanza. • `t3.micro` • `t3.small` • `t3.medium` • `t3.large`

Parametro	Predefinito	Descrizione
		• `t3.xlarge` • `t3.2xlarge` Per l'elenco completo dei valori dei tipi di EC2 istanza Amazon consentiti per questo parametro, consulta fsx-ontap-harvest-grafana .template.
KeyPair	Nessun valore predefinito	La coppia di chiavi utilizzata per accedere all' EC2 istanza Amazon.
SecurityGroup	Nessun valore predefinito	L'ID del gruppo di sicurezza per l' Harvest/Grafana istanza. 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.

Parametro	Predefinito	Descrizione
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 Amazon VPC User Guide.
Sottorete	Nessun valore predefinito	Specificate la stessa sottorete della sottorete preferita del file system Amazon FSx for NetApp ONTAP. Puoi trovare l'ID di sottorete preferito del file system nella FSx console Amazon, 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.

Parametro	Predefinito	Descrizione
FSxEndPoint	Nessun valore predefinito	L'indirizzo IP dell'endpoint di gestione del file system. Puoi trovare l'indirizzo IP dell'endpoint di gestione del file system nella FSx console Amazon, nella scheda Amministrazione della pagina dei dettagli del file system FSx for ONTAP.
SecretName	Nessun valore predefinito	Gestione dei segreti AWS nome segreto contenent e la password per l'utente del file system. `fsxadmin` Questa è la password che hai fornito quando hai creato il file system.

3. Scegli Next (Successivo).
4. Per Opzioni, scegli Avanti.
5. Per Revisione, rivedi e conferma le impostazioni. È necessario selezionare la casella di controllo per confermare che il modello crea risorse IAM.
6. Scegli Crea per distribuire lo stack.

Puoi visualizzare lo stato dello stack nella 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 di Harvest e Grafana o hai problemi a configurare Harvest e Grafana FSx con ONTAP, consulta i seguenti argomenti per una potenziale soluzione.

Argomenti

I dashboard SVM e Volume sono vuoti

Se lo CloudFormation stack è stato distribuito correttamente e può contattare Grafana ma i dashboard SVM e volume sono vuoti, usa la seguente procedura per risolvere i problemi del tuo ambiente. Avrai bisogno dell'accesso SSH all' EC2 istanza Amazon su cui sono distribuiti Harvest e Grafana.

1. Accedi tramite SSH all' EC2 istanza Amazon 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 la tua 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' EC2 istanza distribuita dallo stack. CloudFormation

1. Ridistribuisci lo CloudFormation stack, assicurandoti che il rollback automatico sia disabilitato.
2. Accedi tramite SSH all' EC2 istanza Amazon 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.

Monitoraggio FSx delle chiamate API ONTAP con AWS CloudTrail

Amazon FSx è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon FSx. CloudTrail acquisisce tutte le chiamate FSx API Amazon per Amazon FSx for NetApp ONTAP come eventi. Le chiamate acquisite includono le chiamate dalla FSx console Amazon e le chiamate in codice alle operazioni delle FSx API Amazon.

Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon. FSx Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che 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 CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

FSx Informazioni su Amazon in CloudTrail

CloudTrail è abilitato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività dell'API in Amazon FSx, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nel tuo AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Amazon FSx, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il trail registra gli eventi di tutte le AWS regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente

e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente AWS CloudTrail :

- Creare un percorso per il tuo Account AWS
- AWS integrazioni di servizi con Logs CloudTrail
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le chiamate FSx API Amazon vengono registrate da CloudTrail. Ad esempio, le chiamate alle `TagResource` operazioni `CreateFileSystem` and generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity nella Guida per l'AWS CloudTrail utente.

Comprendere le voci dei file di FSx registro di Amazon

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra il `TagResource` funzionamento quando viene creato un tag per un file system dalla console.

```
{
```

```
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'`UntagResource`azione che si verifica quando un tag per un file system viene eliminato dalla console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
```

```
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

Utilizzo di Microsoft Active Directory in FSx ONTAP

Amazon FSx collabora 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 FSx for ONTAP (SVMs) 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 i file e le cartelle esistenti e le relative configurazioni degli elenchi di controllo degli accessi di sicurezza (ACL) su Amazon FSx senza alcuna modifica.

Se l'infrastruttura del dominio Microsoft Active Directory non è disponibile, è possibile configurare un server Server Message Block (SMB) in un gruppo di lavoro su una SVM come alternativa all'aggiunta di una SVM a Microsoft Active Directory. Per ulteriori informazioni, consulta Configurazione di un server SMB in un gruppo di lavoro.

Quando ti iscrivi ad Amazon FSx for NetApp ONTAP a un Active Directory, unisci il file system SVMs ad Active Directory in modo indipendente. Ciò significa che puoi avere un file system con alcuni SVMs che sono uniti a un Active Directory e altri SVMs 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 una 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.

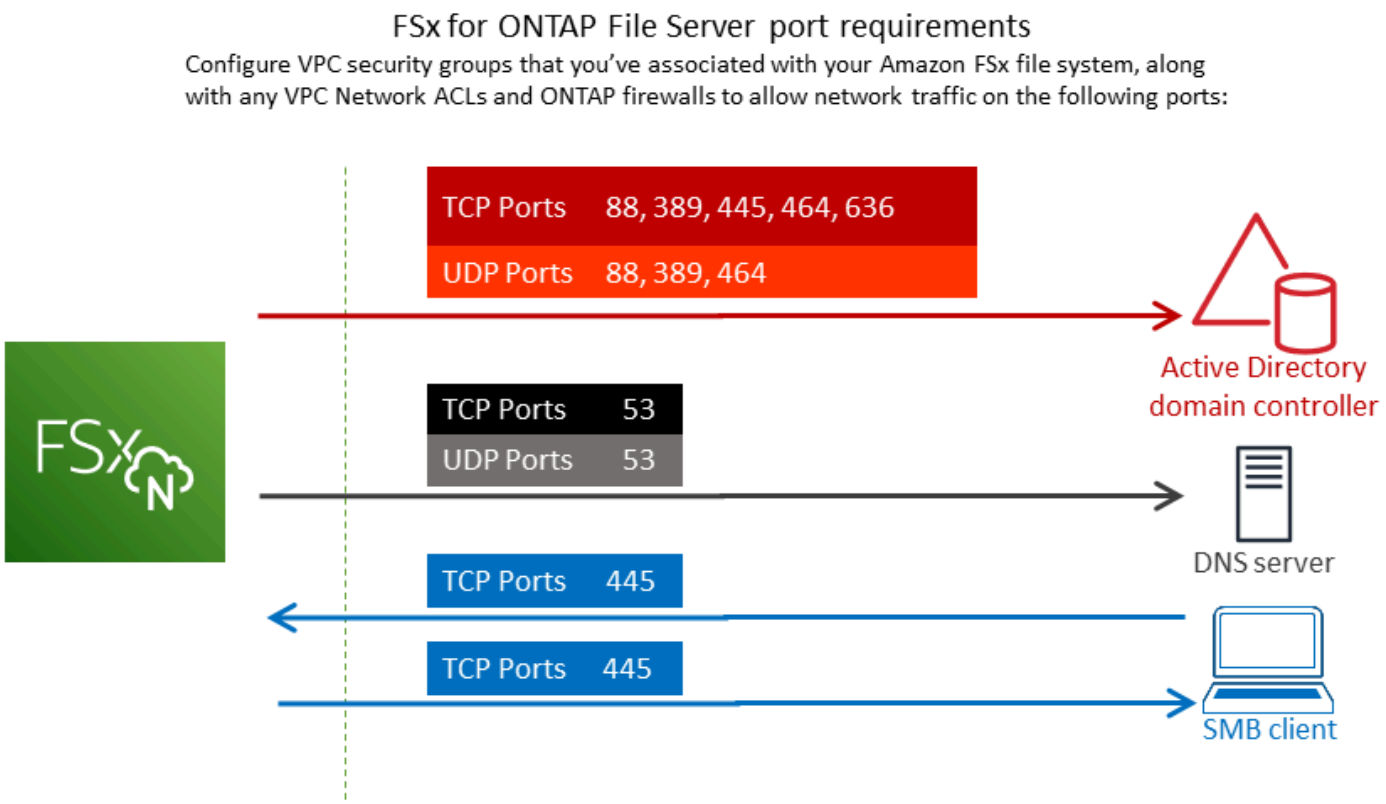
> **Note**
>
> Se lo utilizzi Directory Service, FSx for ONTAP non supporta l'accesso a Simple Active Directory. SVMs

Requisiti relativi alla configurazione della rete

Assicurati di avere a disposizione le seguenti configurazioni di rete e le informazioni associate.

> **Important**
>
> Affinché una SVM possa unirsi 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 ()) sull'SVM. LIFs

- 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 Direct Connect, Site-to-Site VPNo. AWS Transit Gateway
- Il gruppo di sicurezza e la rete VPC ACLs 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
TCP	636	Lightweight Directory Access Protocol over TLS/SSL (LDAPS)

- Queste regole del traffico devono inoltre essere rispecchiate nei firewall che si applicano a ciascuno dei controller di dominio, server DNS, client e amministratori di Active Directory. FSx 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 delle reti VPC richiedono che le porte siano aperte in ACLs 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.

Puoi memorizzare le credenziali del tuo account del servizio Active Directory in Gestione dei segreti AWS (consigliato) e fornire ad Amazon FSx un ARN segreto per unirti al tuo Active Directory oppure puoi fornire credenziali in testo semplice.

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 FSx file system Amazon. 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 NetApp al software ONTAP. Mantieni aggiornate le informazioni di configurazione di Active Directory con Amazon FSx, incluse le credenziali dell'account di servizio. Per ulteriori informazioni, consulta Mantenere aggiornata la configurazione di Active Directory con Amazon FSx.

Se è la prima volta che utilizzi AWS e FSx per ONTAP, assicurati di completare i passaggi di configurazione iniziali prima di iniziare l'integrazione con Active Directory. Per ulteriori informazioni, consulta Configurazione FSx per ONTAP.

> **Important**
>
> Non spostare oggetti informatici creati da Amazon FSx nell'unità organizzativa dopo la SVMs creazione, né eliminare Active Directory mentre la SVM vi è aggiunta. In questo modo potresti non SVMs essere configurato correttamente.

Procedure consigliate per l'utilizzo di Active Directory

Ecco alcuni suggerimenti e linee guida da prendere in considerazione quando ti iscrivi ad Amazon FSx for NetApp ONTAP SVMs alla tua Microsoft Active Directory autogestita. Tieni presente che sono consigliate come best practice, ma non obbligatorie.

Argomenti

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 Amazon FSx SVMs 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 al dominio solo le autorizzazioni necessarie FSx per iscriversi a SVMs ONTAP.

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 del 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 che Amazon FSx crea nell'unità organizzativa dopo la creazione SVMs dei tuoi. In questo modo potresti non SVMs essere configurato correttamente.

Mantenere aggiornata la configurazione di Active Directory con Amazon FSx

Per una disponibilità ininterrotta di Amazon FSx SVMs, aggiorna la configurazione Active Directory (AD) autogestita di una SVM quando modifichi la configurazione di 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 FSx console Amazon, FSx l'API Amazon 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 delle configurazioni SVM Active Directory esistenti utilizzando l'API Console di gestione AWS, 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, consulta 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 FSx file system Amazon. Per ulteriori informazioni, consulta Controllo degli accessi ai file system con Amazon VPC.

Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS

È possibile utilizzarlo per Gestione dei segreti AWS archiviare e gestire in modo sicuro le credenziali dell'account del servizio di accesso al dominio Microsoft Active Directory. Questo approccio elimina la necessità di archiviare credenziali sensibili in testo semplice nel codice dell'applicazione o nei file di configurazione, rafforzando il livello di sicurezza.

Puoi anche configurare le policy IAM per gestire l'accesso ai tuoi segreti e impostare policy di rotazione automatica per le tue password.

Archivia le credenziali di Active Directory in Gestione dei segreti AWS (Console)

Passaggio 1: creare una chiave KMS

Crea una chiave KMS per crittografare e decrittografare le credenziali di Active Directory in Secrets Manager.

Come creare una chiave

> **Note**
>
> Per la chiave di crittografia, crea una nuova chiave, non utilizzare la chiave KMS predefinita. AWS Assicurati di crearla AWS KMS key nella stessa regione che contiene la SVM a cui desideri aggiungere ad Active Directory.

1. Apri la AWS KMS console in /kms. https://console.aws.amazon.com
2. Scegli Crea chiave.
3. In Tipo di chiave, scegli Simmetrica.

4. In Utilizzo delle chiavi, scegli Crittografa e decrittografa.
5. Per le opzioni avanzate, procedi come segue:
   a. In Origine materiale chiave, scegli KMS.
   b. Per Regionalità, scegli la chiave Single-Region e scegli Avanti.
6. Scegli Next (Successivo).
7. In Alias, fornisci un nome per la chiave KMS.
8. (Facoltativo) In Descrizione, immetti una descrizione per la chiave KMS.
9. (Facoltativo) Per i tag, fornisci un tag per la chiave KMS e scegli Avanti.
10. (Facoltativo) Per gli amministratori chiave, fornisci gli utenti e i ruoli IAM autorizzati a gestire questa chiave.
11. Per l'eliminazione della chiave, mantieni selezionata la casella Consenti agli amministratori chiave di eliminare questa chiave e scegli Avanti.
12. (Facoltativo) Per gli utenti chiave, fornisci gli utenti e i ruoli IAM autorizzati a utilizzare questa chiave nelle operazioni crittografiche. Scegli Next (Successivo).
13. Per Politica chiave, scegli Modifica e includi quanto segue nella dichiarazione sulla politica per consentire FSx ad Amazon di utilizzare la chiave KMS e scegli Avanti. Assicurati di *us-west-2* sostituirlo nel Regione AWS luogo in cui è distribuito il file system e nel tuo *123456789012* Account AWS ID.

```
{
    "Sid": "Allow FSx to use the KMS key",
    "Version": "2012-10-17",
    "Effect": "Allow",
    "Principal": {
        "Service": "fsx.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
        "kms:DescribeKey"
    ],
    "Resource": "arn:aws:kms:us-west-2:123456789012:key/*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "secretsmanager.us-west-2.amazonaws.com",
            "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
```

```
            "aws:SourceArn": [
                "arn:aws:fsx:us-west-2:123456789012:file-system/*",
                "arn:aws:fsx:us-west-2:123456789012:storage-virtual-machine/fs-*/
svm-*"
            ]
        }
    }
}
```

14. Scegli Fine.

> **Note**
>
> Puoi impostare un controllo degli accessi più granulare modificando `aws:SourceArn` i campi `Resource` e in modo da indirizzarli a segreti e file system specifici.

Fase 2: Creare un segreto Gestione dei segreti AWS

Per creare un segreto

1. Apri la console Secrets Manager all'indirizzo https://console.aws.amazon.com/secretsmanager/.
2. Scegli Archivia un nuovo segreto.
3. Per Secret type (Tipo di segreto), scegli Other type of secret (Altro tipo di segreto).
4. Per le coppie chiave/valore, effettuate le seguenti operazioni per aggiungere le due chiavi:
   a. Per la prima chiave, immetti `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`.
   b. Per il valore della prima chiave, immetti solo il nome utente (senza il prefisso di dominio) dell'utente AD.
   c. Per la seconda chiave, immetti `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`.
   d. Per il valore della seconda chiave, immetti la password creata per l'utente AD nel dominio.
5. Per Chiave di crittografia, inserisci l'ARN della chiave KMS che hai creato in un passaggio precedente e scegli Avanti.
6. In Nome del segreto, inserisci un nome descrittivo che semplifichi l'individuazione del segreto in un secondo momento.
7. (Facoltativo) In Descrizione, inserisci una descrizione per il nome del segreto.
8. Per l'autorizzazione della risorsa, scegli Modifica.

Aggiungi la seguente politica alla politica di autorizzazione per consentire FSx ad Amazon di utilizzare il segreto, quindi scegli Avanti. Assicurati di *us-west-2* sostituirlo nel Regione AWS luogo in cui è distribuito il file system e *123456789012* nel tuo Account AWS ID.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "fsx.amazonaws.com"
            },
            "Action": [
                "secretsmanager:GetSecretValue",
                "secretsmanager:DescribeSecret"
            ],
            "Resource": "arn:aws:secretsmanager:us-west-2:123456789012:secret:*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "123456789012"
                },
                "ArnLike": {
                    "aws:SourceArn": [
                        "arn:aws:fsx:us-west-2:123456789012:file-system/*",
                        "arn:aws:fsx:us-west-2:123456789012:storage-virtual-
machine/fs-*/svm-*"
                    ]
                }
            }
        }
    ]
}
```

9. (Facoltativo) È possibile configurare Secrets Manager per ruotare automaticamente le credenziali. Scegli Next (Successivo).
10. Scegli Fine.

Archivia le credenziali di Active Directory in Gestione dei segreti AWS (CLI)

Fase 1: Creare una chiave KMS

Crea una chiave KMS per crittografare e decrittografare le credenziali di Active Directory in Secrets Manager.

Per creare una chiave KMS, usa il comando create-key. AWS CLI

In questo comando, imposta il `--policy` parametro per specificare la politica chiave che definisce le autorizzazioni per la chiave KMS. La politica deve includere quanto segue:

- Il principale servizio per Amazon FSx, che è`fsx.amazonaws.com`.
- Azioni KMS richieste: `kms:Decrypt` e`kms:DescribeKey`.
- Schema ARN delle risorse per il tuo account Regione AWS .
- Chiavi condizionali che limitano l'utilizzo delle chiavi:
  - `kms:ViaService`per garantire che le richieste arrivino tramite Secrets Manager.
  - `aws:SourceAccount`da limitare al tuo account.
  - `aws:SourceArn`per limitarsi a specifici FSx file system Amazon.

L'esempio seguente crea una chiave KMS di crittografia simmetrica con una politica che consente ad Amazon FSx di utilizzare la chiave per le operazioni di decrittografia e descrizione delle chiavi. Il comando recupera automaticamente l' Account AWS ID e la regione, quindi configura la politica delle chiavi con questi valori per garantire controlli di accesso adeguati tra Amazon FSx, Secrets Manager e la chiave KMS. Assicurati che il tuo AWS CLI ambiente si trovi nella stessa regione della SVM che entrerà a far parte di Active Directory.

```
# Set region and get Account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Create Key
KMS_KEY_ARN=$(aws kms create-key --policy "{
  \"Version\": \"2012-10-17\",
  \"Statement\": [
    {
      \"Sid\": \"Enable IAM User Permissions\",
      \"Effect\": \"Allow\",
      \"Principal\": {
```

```
        \"AWS\": \"arn:aws:iam::$ACCOUNT_ID:root\"
      },
      \"Action\": \"kms:*\",
      \"Resource\": \"*\"
    },
    {
      \"Sid\": \"Allow FSx to use the KMS key\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"Service\": \"fsx.amazonaws.com\"
      },
      \"Action\": [
        \"kms:Decrypt\",
        \"kms:DescribeKey\"
      ],
      \"Resource\": \"*\",
      \"Condition\": {
        \"StringEquals\": {
          \"kms:ViaService\": \"secretsmanager.$REGION.amazonaws.com\",
          \"aws:SourceAccount\": \"$ACCOUNT_ID\"
        },
        \"ArnLike\": {
          \"aws:SourceArn\": [
            \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\",
            \"arn:aws:fsx:$REGION:$ACCOUNT_ID:storage-virtual-machine/fs-*/svm-*\"]
        }
      }
    }
  ]
}" --query 'KeyMetadata.Arn' --output text)

echo "KMS Key ARN: $KMS_KEY_ARN"
```

> **Note**
>
> È possibile impostare un controllo degli accessi più granulare modificando `aws:SourceArn` i campi `Resource` and in modo da indirizzarli a segreti e file system specifici.

Fase 2: Creare un segreto Gestione dei segreti AWS

Per creare un codice segreto per consentire FSx ad Amazon di accedere al tuo Active Directory, usa il AWS CLI comando create-secret e imposta i seguenti parametri:

- `--name`: L'identificatore del tuo segreto.
- `--description`: Una descrizione dello scopo del segreto.
- `--kms-key-id`: L'ARN della chiave KMS che hai creato nel passaggio 1 per crittografare il segreto inattivo.
- `--secret-string`: Una stringa JSON contenente le tue credenziali AD nel seguente formato:
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`: nome utente dell'account del servizio AD senza il prefisso del dominio, ad esempio. `svc-fsx` Non fornire il prefisso del dominio, ad esempio. `CORP\svc-fsx`
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`: la password dell'account del servizio AD
- `--region`: Il Regione AWS luogo in cui verrà creato il tuo SVM. Se non è impostata, l'impostazione predefinita `AWS_REGION` è la regione configurata.

Dopo aver creato il segreto, allega una politica delle risorse utilizzando il put-resource-policycomando e imposta i seguenti parametri:

- `--secret-id`: il nome o l'ARN del segreto a cui allegare la policy. L'esempio seguente utilizza **`FSxSecret`** come. `--secret-id`
- `--region`: Uguale Regione AWS al tuo segreto.
- `--resource-policy`: un documento di policy JSON che concede ad Amazon FSx l'autorizzazione ad accedere al segreto. La politica deve includere quanto segue:
  - Il principale servizio per Amazon FSx, che è**`fsx.amazonaws.com`**.
  - Azioni richieste di Secrets Manager: `secretsmanager:GetSecretValue` `esecretsmanager:DescribeSecret`.
  - Schema ARN delle risorse per il tuo account Regione AWS .
  - Le seguenti chiavi condizionali che limitano l'accesso:
    - `aws:SourceAccount`da limitare al tuo account.
    - `aws:SourceArn`per limitarsi a specifici FSx file system Amazon.

L'esempio seguente crea un segreto con il formato richiesto e allega una politica delle risorse che consente FSx ad Amazon di utilizzare il segreto. Questo esempio recupera automaticamente il tuo Account AWS ID e la tua regione, quindi configura la politica delle risorse con questi valori per garantire controlli di accesso adeguati tra Amazon FSx e il segreto.

Assicurati di sostituirlo `KMS_KEY_ARN` con l'ARN della chiave creata nel passaggio 1 e `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD` con le credenziali `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME` dell'account del servizio Active Directory. Inoltre, verificate che l' AWS CLI ambiente sia configurato per la stessa regione della SVM che entrerà a far parte di Active Directory.

```
# Set region and get account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Replace with your KMS key ARN from Step 1
KMS_KEY_ARN="arn:aws:kms:us-east-2:123456789012:key/1234542f-d114-555b-9ade-
fec3c9200d8e"

# Replace with your Active Directory credentials
AD_USERNAME="Your_Username"
AD_PASSWORD="Your_Password"

# Create the secret
SECRET_ARN=$(aws secretsmanager create-secret \
  --name "FSxSecret" \
  --description "Secret for FSx access" \
  --kms-key-id "$KMS_KEY_ARN" \
  --secret-string "{\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME\":\"$AD_USERNAME\",
\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD\":\"$AD_PASSWORD\"}" \
  --region "$REGION" \
  --query 'ARN' \
  --output text)

echo "Secret created with ARN: $SECRET_ARN"

# Attach the resource policy with proper formatting
aws secretsmanager put-resource-policy \
  --secret-id "FSxSecret" \
  --region "$REGION" \
  --resource-policy "{
    \"Version\": \"2012-10-17\",
```

```
    \"Statement\": [
      {
        \"Effect\": \"Allow\",
        \"Principal\": {
          \"Service\": \"fsx.amazonaws.com\"
        },
        \"Action\": [
          \"secretsmanager:GetSecretValue\",
          \"secretsmanager:DescribeSecret\"
        ],
        \"Resource\": \"$SECRET_ARN\",
        \"Condition\": {
          \"StringEquals\": {
            \"aws:SourceAccount\": \"$ACCOUNT_ID\"
          },
          \"ArnLike\": {
            \"aws:SourceArn\": [
              \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\",
              \"arn:aws:fsx:$REGION:$ACCOUNT_ID:storage-virtual-machine/fs-*/svm-*\"]
          }
        }
      }
    ]
  }"

echo "Resource policy attached successfully"
```

> **Note**
>
> È possibile impostare un controllo degli accessi più granulare modificando `aws:SourceArn` i campi `Resource` and in modo da indirizzarli a segreti e file system specifici.

Come funziona l' SVMs accesso 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 il tuo dominio Active Directory SVMs direttamente al tuo dominio Active Directory esistente nei seguenti modi:

- Unirsi SVMs a un nuovo utente di Active Directory al momento della creazione:

  - Utilizzando l'opzione di creazione Standard nella FSx console Amazon per creare un nuovo file system FSx for ONTAP, puoi aggiungere la SVM predefinita a un'Active Directory autogestita. Per ulteriori informazioni, consulta Per creare un file system (console).
  - Utilizzo della FSx console Amazon o dell' FSx API Amazon per creare una nuova SVM su un file system esistente FSx per ONTAP. AWS CLI Per ulteriori informazioni, consulta Creazione di macchine virtuali di archiviazione (SVM).
- Unire un sistema esistente SVMs a un Active Directory:
  - Utilizzo dell'API Console di gestione AWS AWS CLI, e per aggiungere una SVM a un'Active Directory e per ritentare l'aggiunta di 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 quelle SVMs che sono già state aggiunte 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 Aggiornamento delle configurazioni SVM Active Directory tramite la CLI NetApp.

> **Important**
>
> - Amazon registra i record DNS per una SVM FSx solo se utilizzi Microsoft DNS come servizio DNS predefinito. Se utilizzi un DNS di terze parti, devi configurare manualmente le voci DNS per Amazon FSx SVMs dopo averle create.
> - Se lo utilizzi AWS Managed Microsoft AD, devi specificare un gruppo come Amministratori delegati, FSx Amministratori AWS delegati o un gruppo personalizzato con autorizzazioni AWS delegate all'unità organizzativa.

Quando si aggiunge una SVM FSx for ONTAP direttamente a un'Active Directory autogestita, la 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 aggiunge 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
- Credenziali per un account del servizio Active Directory che Amazon FSx utilizza per aggiungere SVM al tuo dominio. Puoi fornirle in uno dei seguenti modi:
  - Opzione 1: ARN Gestione dei segreti AWS segreto: il segreto contenente il nome utente e la password per un account di servizio nel dominio Active Directory. Per ulteriori informazioni, consulta Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.
  - Opzione 2: credenziali in chiaro
    - Nome utente dell'account di servizio: il nome utente dell'account di servizio nel Microsoft 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.
- (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 Directory Service creata per gli oggetti di directory a cui sono correlati. AWS Questo perché 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' FSx API Console di gestione AWS AWS CLI, 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 SVMs da un Active Directory

Per rimuovere una SVM da un Active Directory, è necessario utilizzare l' NetApp ONTAP CLI.

Argomenti

- Accesso SVMs ad Active Directory utilizzando l'API e Console di gestione AWS AWS CLI
- Aggiornamento delle configurazioni SVM Active Directory esistenti utilizzando l'API Console di gestione AWS, e AWS CLI
- Aggiornamento delle configurazioni SVM Active Directory tramite la CLI NetApp

Accesso SVMs ad Active Directory utilizzando l'API e Console di gestione AWS AWS 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 ()Console di gestione AWS

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

2. Scegli la SVM a cui 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 funzionalità disponibili SVMs, nel riquadro di navigazione a sinistra, espandi ONTAP e scegli Storage virtual machines. Viene visualizzato un elenco di tutte le informazioni presenti SVMs nel 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 del server DNS: gli IPv4 o IPv6 gli indirizzi dei server DNS del tuo dominio.
   - Credenziali dell'account di servizio: scegli come fornire le credenziali del tuo account di servizio:
     - Opzione 1: ARN Gestione dei segreti AWS segreto: il segreto contenente il nome utente e la password per un account di servizio nel dominio Active Directory. Per ulteriori informazioni, consulta Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.
     - Opzione 2: credenziali in chiaro
       - Nome utente dell'account di servizio: il nome utente dell'account di servizio nel Microsoft 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.

- Gestito in Secrets Manager (impostazione predefinita): fornisci l'ARN di un segreto di Secrets Manager che contiene le credenziali del tuo account di servizio. Il segreto deve contenere le coppie chiave-valore e. `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME` `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`
- (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 Amministratori delegati, FSx Amministratori AWS delegati o un gruppo personalizzato AWS 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 una 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 archiviazione, Amazon FSx restituisce la descrizione in formato JSON, come mostrato 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 delle configurazioni SVM Active Directory esistenti utilizzando l'API Console di gestione AWS, e AWS CLI

Utilizzare la procedura seguente per aggiornare la configurazione di Active Directory di una SVM già unita a un Active Directory.

Per aggiornare una configurazione SVM Active Directory ()Console di gestione AWS

1. Apri la FSx console Amazon 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 funzionalità SVMs 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 IPv4 o IPv6 gli indirizzi dei server DNS del tuo dominio.
   - Credenziali dell'account di servizio: scegli come fornire le credenziali del tuo account di servizio:

- Opzione 1: ARN Gestione dei segreti AWS segreto: il segreto contenente il nome utente e la password per un account di servizio nel dominio Active Directory. Per ulteriori informazioni, consulta Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.
- Opzione 2: credenziali in chiaro
  - Nome utente dell'account di servizio: il nome utente dell'account di servizio nel Microsoft 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.

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"]}'
```

Aggiornamento delle configurazioni 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 aggiungere file esistenti SVMs 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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. *`svm_name`*Sostituiscilo 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 unire la SVM ad Active Directory, esegui il comando seguente. 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` Per esempio`-OU`, inserisci il nome a cui vuoi OUs 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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) della 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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
```

Migrazione ad Amazon FSx per ONTAP NetApp

Le seguenti sezioni forniscono informazioni su come migrare i file system NetApp ONTAP esistenti su Amazon FSx for NetApp ONTAP.

> **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 for ONTAP utilizzando FSx NetApp SnapMirror

Puoi migrare i tuoi file system NetApp ONTAP su Amazon FSx for NetApp ONTAP utilizzando. NetApp SnapMirror

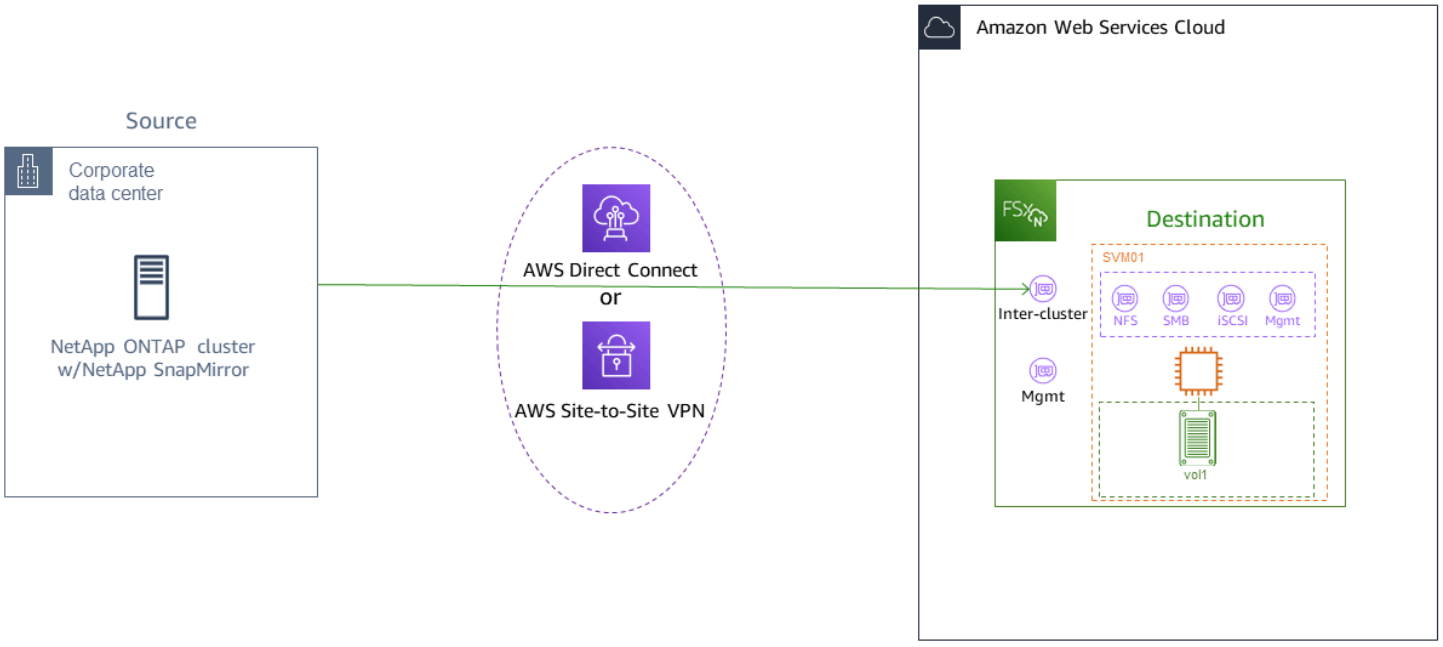
NetApp SnapMirror utilizza la replica a livello di blocco tra due file system ONTAP, replicando i dati da un volume di origine specificato a un volume di destinazione. Si consiglia di SnapMirror utilizzarlo per migrare i file system ONTAP NetApp on-premise a for ONTAP. FSx NetApp SnapMirrorla replica 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 ONTAP locali a FSx for NetApp ONTAP comporta le seguenti attività di alto livello:

1. Crea il volume di destinazione in Amazon FSx.
2. Raccogli le interfacce logiche di origine e destinazione (LIFs).
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. Passa al tuo 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, assicurati di aver soddisfatto i seguenti prerequisiti:

- FSx for ONTAP dà priorità al traffico dei clienti 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 assicurarsi 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 Site-to-Site VPN Per ulteriori informazioni, consulta Accesso ai dati dall'interno di Cloud 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 intercluster (). LIFs
- Verificate 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 stata creata una destinazione FSx per il file system ONTAP con una SVM, ma non è stato creato un volume di destinazione. Per ulteriori informazioni, consulta Creazione di file system.

I comandi di queste procedure utilizzano i seguenti alias di cluster, SVM e volume:

- *FSx-Dest*— l'ID del cluster destination (FSx) (nel formato FSx IDABCDEF1234567890a).
- *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 CLI di ONTAP.

Le procedure in questa sezione utilizzano i seguenti comandi NetApp ONTAP CLI.

- comando volume create
- comandi cluster
- comandi vserver peer
- comandi snapmirror

Utilizzerai la CLI NetApp ONTAP per creare e gestire SnapMirror una configurazione sul FSx tuo file system for ONTAP. Per ulteriori informazioni, consulta Utilizzo della CLI NetApp ONTAP.

Crea il volume di destinazione

Puoi creare un volume di destinazione per la protezione dei dati (DP) utilizzando la FSx console Amazon AWS CLI, l' FSx API Amazon, oltre all' NetApp ONTAP CLI e all'API REST. Per informazioni sulla creazione di un volume di destinazione utilizzando la FSx console Amazon e AWS CLI, consultaCreazione di volumi.

> **Note**
>
> ONTAPnon preserva i risparmi di compressione post-elaborazione ottenuti all'origine nel volume DP di destinazione quando la politica di suddivisione in più livelli del volume di destinazione è. `All` Per preservare i risparmi sulla compressione post-elaborazione, è necessario impostare la politica di suddivisione in più livelli del volume di destinazione `Auto` e abilitarla inactive-data-compression sul file system di destinazione per riapplicare i risparmi di compressione post-elaborazione alla destinazione.

Nella procedura seguente, utilizzerai la CLI NetApp ONTAP per creare un volume di destinazione sul FSx tuo file system 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 l'intercluster di origine e destinazione LIFs

SnapMirror utilizza interfacce logiche intercluster (LIFs), ciascuna con un indirizzo IP univoco, per facilitare il trasferimento dei dati tra i cluster di origine e di destinazione.

1. Per la destinazione FSx dei file system ONTAP, puoi recuperare gli endpoint inter-cluster - indirizzi IP dalla FSx console Amazon accedendo alla scheda Amministrazione nella pagina dei dettagli del tuo 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 Single-AZ di seconda generazione, 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 Single-AZ di seconda generazione, 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 Single-AZ di seconda generazione, 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 di. SVMs 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 l'origine e la destinazione. SVMs

```
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 dell'origine e della destinazione SVMs, 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".
```

Trasferisci i dati sul file system for ONTAP FSx

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. Puoi anche pianificare aggiornamenti orari o giornalieri prima di completare la migrazione e trasferire i tuoi client a FSx for ONTAP. È possibile stabilire una pianificazione degli SnapMirror aggiornamenti utilizzando il `snapmirror modify`comando.

   ```
   FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
   ```

Passando ad Amazon FSx

Per prepararti al trasferimento del file system FSx for ONTAP, procedi come segue:

- 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 FSx file system ONTAP, esegui 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 su`all`, 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 di FSx for ONTAP.

Migrazione a FSx for ONTAP utilizzando AWS DataSync

Consigliamo di AWS DataSync utilizzarlo FSx per trasferire dati tra file system ONTAP e file system non ONTAP, inclusi FSx Lustre, OpenZFS, FSx FSx Windows File Server, Amazon EFS, Amazon S3 e filer locali. Se trasferisci file tra ONTAP e ONTAP, ti consigliamo di utilizzare. FSx NetApp NetApp SnapMirror AWS DataSync è 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 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 FSx per i file system ONTAP e anche per spostare i dati su un file system di un altro account. Regione AWS AWS È inoltre possibile utilizzare DataSync with FSx for ONTAP file system per altre attività. Ad esempio, puoi eseguire migrazioni di dati una tantum, inserire 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 for ONTAP. FSx Per informazioni su scenari di trasferimento specifici, consulta Lavorare con le posizioni nella Guida per l'AWS DataSync utente.

> **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 MBps acceleratore di 200 in genere bilancia le velocità di trasferimento e 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 DataSync utente.

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.
- Crea un’attività .
- Eseguire l'attività per trasferire i file dall'origine alla destinazione.

Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente AWS DataSync :

- Trasferimento di dati tra storage autogestito e AWS
- Creare una sede per Amazon FSx for NetApp ONTAP

Sicurezza in Amazon FSx per NetApp ONTAP

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 maggiori informazioni sui programmi di conformità applicabili ad Amazon FSx for NetApp ONTAP, consulta AWS Services in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria 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 per FSx soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue FSx risorse Amazon.

Argomenti

- ONTAPruoli e utenti

Protezione dei dati in Amazon FSx per NetApp ONTAP

Il modello di responsabilità AWS condivisa Modello si applica alla protezione dei dati in Amazon FSx per 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 maggiori informazioni sulla privacy dei dati, consulta le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al AWS Modello di responsabilità condivisa e GDPR nel AWS Blog sulla sicurezza.

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. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon FSx o altri Servizi AWS utenti utilizzando la console, l'API o

AWS SDKs. AWS CLI 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 si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati in FSx 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 FSx file system Amazon. 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 Crittografia dei dati a riposo eCrittografia dei dati in transito.

Crittografia dei dati a riposo

Tutti i file system e i backup di 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. Tutti i backup vengono crittografati automaticamente al momento della creazione e decrittografati automaticamente quando il backup viene ripristinato su un nuovo volume. Questi processi sono gestiti in modo trasparente da Amazon FSx, quindi non devi modificare le tue applicazioni.

Amazon FSx utilizza un algoritmo di crittografia AES-256 standard di settore per crittografare dati e metadati Amazon FSx inattivi. 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.

In che modo Amazon FSx utilizza 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 e i backup di qualsiasi volume. Scegli la chiave KMS utilizzata per crittografare e decrittografare i file system e i backup di volumi (sia dati che 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 utilizzare 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 FSx chiave di Amazon per AWS KMS

Le policy chiave sono lo strumento principale per controllare l'accesso alle chiavi KMS. Per ulteriori informazioni sulle politiche chiave, consulta la sezione Utilizzo delle politiche chiave AWS KMS nella Guida per gli AWS Key Management Service sviluppatori.L'elenco seguente descrive tutte le autorizzazioni AWS KMS relative supportate da Amazon FSx per i file system e i backup 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: GenerateDataKeyWithoutPlaintext — (Obbligatorio) Restituisce una chiave di crittografia dei dati crittografata con una chiave KMS. Questa autorizzazione è inclusa nella politica delle chiavi predefinita in kms: *. GenerateDataKey
- kms: CreateGrant — (Obbligatorio) Aggiunge una concessione a una chiave per specificare chi può utilizzare la chiave e in quali condizioni. I grant sono meccanismi di autorizzazioni alternative alle policy sulle chiavi. Per ulteriori informazioni sulle 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 FSx i file system 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.
- IPseccrittografia basata 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.

Ci sono 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 file system in Regione AWS cui è in esecuzione determina se è possibile utilizzare o meno la crittografia basata su Amazon Nitro. Per ulteriori informazioni, consulta Crittografia dei dati in transito con AWS Nitro System.

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 di Kerberos o della crittografia. 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 modalità peering VPCs, 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'uso di Kerberos o della crittografia ha un impatto sulle prestazioni della rete. IPsec 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.

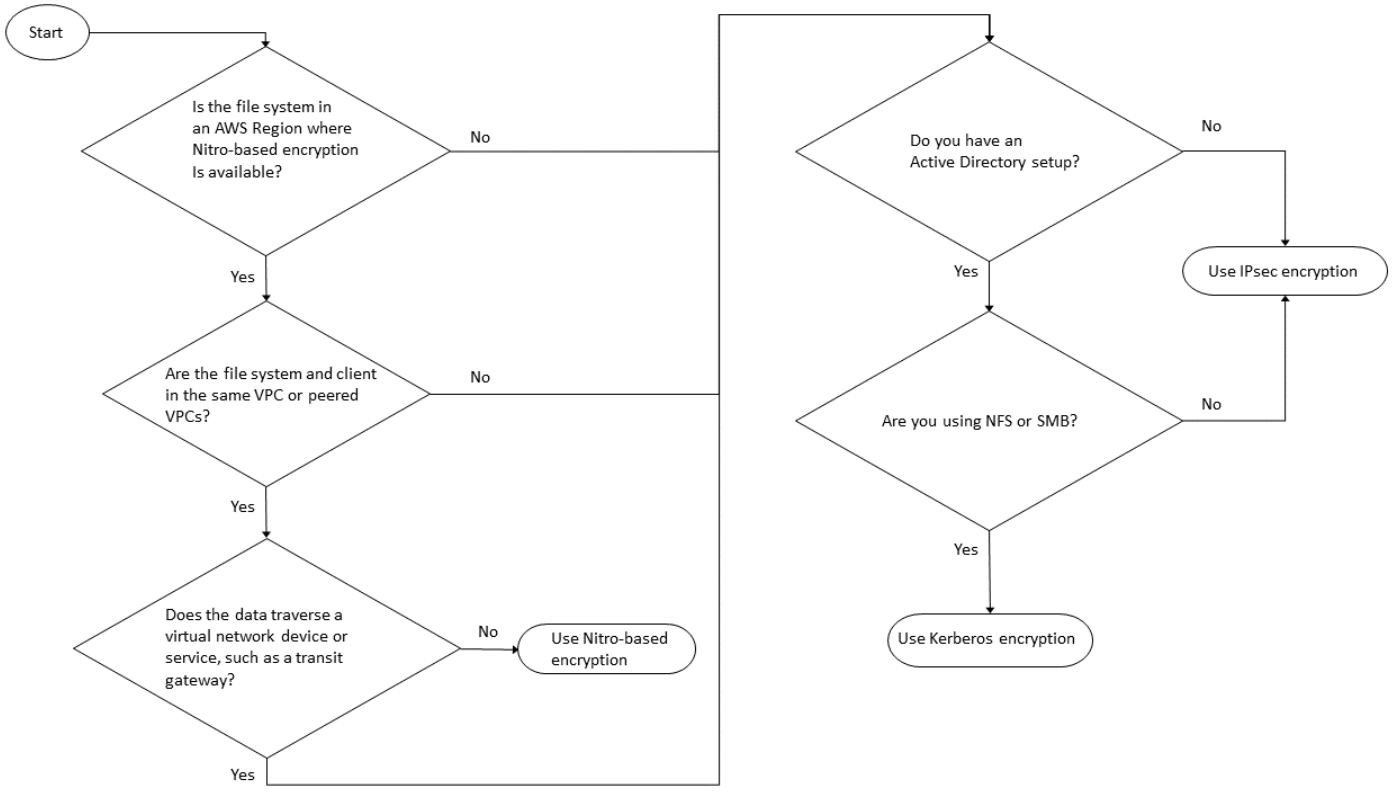
Protocollo dati

Puoi utilizzare la crittografia e IPsec la crittografia basate su Amazon Nitro 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.



IPsec la crittografia 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 Regioni AWS di istanze Linux o Windows supportati di Amazon EC2, laddove sono disponibili FSx su per ONTAP.

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 tabella seguente descrive in dettaglio in Regioni AWS che modo è disponibile la crittografia basata su Nitro.

Support per la crittografia basata su Nitro

Generazione	Tipi di implementazione	Regione AWS
File system di prima generazione 1	AZ singolo 1 Multi-AZ 1	Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (Oregon), Europa (Irlanda)
File system di seconda generazione	AZ singolo 2 Multi-AZ 2	Stati Uniti orientali (Virginia settentrionale), Stati Uniti orientali (Ohio), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon), Europa (Francoforte), Europa (Irlanda), Asia Pacifico (Sydney)

[1] I file system di prima generazione creati a partire dal 28 novembre 2022 supportano la crittografia in transito basata su NITRO tra quelli elencati. Regioni AWS

Per ulteriori informazioni su Regioni AWS dove FSx è disponibile ONTAP, consulta i prezzi di Amazon FSx for NetApp ONTAP.

Per ulteriori informazioni sulle specifiche prestazionali FSx per i file system ONTAP, consulta. Impatto della capacità di throughput sulle prestazioni

Crittografia dei dati in transito con la crittografia basata su Kerberos

Se utilizzi Microsoft Active Directory, puoi utilizzare la crittografia basata su Kerberos sui protocolli NFS e SMB per crittografare i dati in transito per i volumi figlio che SVMs sono uniti a Microsoft Active Directory.

Crittografia dei dati in transito tramite NFS utilizzando Kerberos

La crittografia dei dati in transito tramite Kerberos è supportata da e protocolli. NFSv3 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 abilitata, 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 per 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 FSx per ONTAP SVMs e i volumi. 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 SVMs con la ONTAP CLI

Per istruzioni su come abilitare la crittografia SMB su un SVM o un volume, consulta. Abilitazione della crittografia SMB dei dati in transito

Crittografia dei dati in transito con crittografia IPsec

FSx for ONTAP supporta l'utilizzo del IPsec protocollo in modalità di trasporto per garantire che i dati siano costantemente sicuri e crittografati durante il transito. IPsec offre end-to-end la crittografia dei dati in transito tra i client e FSx per i file system ONTAP per tutto il traffico IP supportato: protocolli NFS, iSCSI e SMB. Con IPsec la crittografia, si stabilisce un IPsec tunnel tra un SVM FSx for ONTAP configurato come IPsec abilitato e un IPsec client 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 io e il client non SVMs siamo uniti a un Active Directory, necessario per la crittografia basata su Kerberos. IPsec la crittografia 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 IPsec l'autenticazione, è possibile utilizzare chiavi precondivise () o certificati. PSKs Se utilizzi un PSK, il IPsec client che utilizzi deve supportare Internet Key Exchange versione 2 (IKEv2) con un PSK. I passaggi di alto livello per configurare la IPsec crittografia sia per ONTAP che FSx per il 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, consulta Configure IP security (IPsec) over wire encryption nel centro di NetApp ONTAP documentazione.

Per ulteriori informazioni su come configurare l' IPsec utilizzo dei certificati, vedereConfigurazione tramite autenticazione tramite certificato IPsec.

Abilitazione della 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 modifyNetApp 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 showNetApp 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 SVMs con la ONTAP CLI

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 createle 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 createle 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 removele 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 showle pagine man del comando NetApp ONTAP CLI.

Configurazione IPsec tramite autenticazione PSK

Se si utilizza PSK per l'autenticazione, i passaggi per configurare la IPsec crittografia sia per ONTAP che FSx per il 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 IPsec tramite PSK, consulta Configurare la sicurezza IP (IPsec) sulla crittografia via cavo nel centro di NetApp ONTAP documentazione.

Configurazione tramite autenticazione tramite certificato IPsec

I seguenti argomenti forniscono istruzioni per configurare la IPsec crittografia utilizzando l'autenticazione dei certificati su un file system FSx for ONTAP e su un client che esegue Libreswan. IPsec Questa soluzione utilizza AWS Certificate Manager e crea un'autorità AWS Autorità di certificazione privata di certificazione privata e per generare i certificati.

I passaggi di alto livello per configurare la IPsec crittografia utilizzando l'autenticazione dei certificati FSx per i file system ONTAP e i client connessi sono i seguenti:

1. Disponi 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. Configurazione 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 Autorità di certificazione privata la configurazione di un'autorità di certificazione privata e la generazione dei certificati da installare sul file system e sul client. Utilizzando AWS Autorità di certificazione privata, è possibile creare una gerarchia interamente

AWS ospitata di autorità di certificazione principali e subordinate (CAs) 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 Autorità di certificazione privata 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 Autorità di certificazione privata utente.
4. Utilizzate il comando create-certificate-authority AWS Private CA CLI 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 risultanteca.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 Autorità di certificazione privata

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.

```
$ passphrase=$(cat passphrase.txt | base64)
cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
```

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 su IPsec 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 IPsec in un passaggio successivo, queste proprietà potrebbero essere contrassegnate senza queste impostazioni. Ti suggeriamo 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. Verifica la IPsec configurazione.

```
$ sudo ipsec verify
```

Verifica che la versione che `Libreswan` hai installato 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 IPsec configurazione utilizzando l'editor di testo preferito.

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

Aggiungi 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
```

IPsec Inizierai dal client dopo la configurazione IPsec sul tuo file system.

Configurazione IPsec sul file system

Questa sezione fornisce istruzioni sull'installazione del certificato sul file system FSx for ONTAP e sulla configurazione. IPsec

Per installare il certificato sul tuo 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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, inclusi sia lato TAP che lato client, per la gestione dei ONTAP certificati CAs, 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. IPsec

   Utilizzate il seguente comando per installare il certificato root.

   ```
   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 assicurarti che la CA installata rientri nel percorso di ricerca IPsec CA durante l'autenticazione, aggiungi la gestione dei ONTAP certificati CAs al IPsec modulo 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 IPsec politica 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. Utilizzate il comando seguente per mostrare la IPsec politica da confermare per il 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
```

Inizia IPsec sul client

Ora IPsec è configurato sia sul file system FSx for ONTAP che IPsec sul client, puoi iniziare dal client.

1. Connect al sistema client tramite SSH.
2. Inizia 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. Verifica la IPsec configurazione 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 IPsec per più client

Quando è necessario sfruttare un numero limitato di clienti IPsec, è sufficiente utilizzare una singola voce SPD per ogni cliente. Tuttavia, quando è necessario sfruttare centinaia o addirittura migliaia di client IPsec, si consiglia di utilizzare una configurazione con IPsec più client.

FSx for ONTAP supporta la connessione di più client su più reti a un singolo indirizzo IP SVM se abilitato. IPsec 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 specificarla nel formato di sottorete. `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 a quello CAs installato nel relativo trust store locale. FSx for ONTAP supporta anche il controllo della lista di revoca dei certificati (CRL).

1. Per accedere alla ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 *`sample`* i valori 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 IPsec abilitato per SVM, 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 *`sample`* i valori 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 NetApp ONTAP

AWS Identity and Access Management (IAM) è un programma 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 Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso tramite policy
- Come funziona Amazon FSx for NetApp ONTAP con IAM
- Esempi di policy basate sull'identità per Amazon for ONTAP FSx NetApp
- Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon FSx for NetApp ONTAP
- Utilizzo di ruoli collegati ai servizi per Amazon FSx
- Usare i tag con Amazon FSx

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon FSx for NetApp ONTAP)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come funziona Amazon FSx for NetApp ONTAP con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate sull'identità per Amazon for ONTAP FSx NetApp)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/ Facebook Per ulteriori informazioni sull'accesso, consulta Come accedere all' Account AWS nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta AWS Signature Version 4 per le richieste API nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta Attività che richiedono le credenziali dell'utente root nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta Che cos'è il Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee nella Guida per l'utente IAM.

Un gruppo IAM specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta Casi d'uso per utenti IAM nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo passando da un ruolo utente a un ruolo IAM (console) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta Metodi per assumere un ruolo nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scegliere tra policy gestite e policy in linea nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio specificare un'entità principale.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in. AWS Organizations Per ulteriori informazioni, consultare Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .

- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta Politiche di controllo delle risorse (RCPs) nella Guida per l'AWS Organizations utente.
- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta 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 NetApp ONTAP

Funzionalità IAM	FSx Assistenza Amazon
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì

Funzionalità IAM	FSx Assistenza Amazon
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come Amazon FSx e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta AWS i servizi che funzionano con IAM nella IAM User Guide.

Politiche basate sull'identità per Amazon FSx

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente di IAM.

Con le policy basate sull'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. 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 IAM.

Esempi di policy basate sull'identità per Amazon FSx

Per visualizzare esempi di politiche FSx basate sull'identità di Amazon, consulta. Esempi di policy basate sull'identità per Amazon for ONTAP FSx NetApp

Politiche basate sulle risorse all'interno di Amazon FSx

Supporta le policy basate su risorse: no

Azioni politiche per Amazon FSx

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di FSx azioni Amazon, consulta Azioni definite da Amazon FSx nel Service Authorization Reference.

Le azioni politiche in Amazon FSx utilizzano il seguente prefisso prima dell'azione:

```
fsx
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Per visualizzare esempi di politiche FSx basate sull'identità di Amazon, consulta. Esempi di policy basate sull'identità per Amazon for ONTAP FSx NetApp

Risorse relative alle policy per Amazon FSx

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità 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. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di FSx risorse Amazon e relativi ARNs, consulta Resources defined by Amazon FSx nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon. FSx

Per visualizzare esempi di politiche FSx basate sull'identità di Amazon, consulta. Esempi di policy basate sull'identità per Amazon for ONTAP FSx 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. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di FSx condizione di Amazon, consulta Condition keys for Amazon FSx 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 politiche FSx basate sull'identità di Amazon, consulta. Esempi di policy basate sull'identità per Amazon for ONTAP FSx NetApp

Elenchi di controllo degli accessi (ACLs) in Amazon FSx

Supporti ACLs: No

Controllo degli accessi basato sugli attributi (ABAC) con Amazon FSx

Supporta ABAC (tag nelle policy): sì

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire 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 Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Per ulteriori informazioni sull'etichettatura FSx delle risorse Amazon, consultaEtichettare le 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 FSx risorse Amazon.

Utilizzo di credenziali temporanee con Amazon FSx

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un accesso a breve termine alle AWS risorse e vengono create automaticamente quando utilizzi la federazione o cambi ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza temporanee in IAM e Servizi AWS compatibili con IAM nella Guida per l'utente IAM.

Sessioni di accesso diretto per Amazon FSx

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale chiamante e Servizio AWS, in combinazione con la richiesta, di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per Amazon FSx

Supporta i ruoli di servizio: no

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'operazione 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 al servizio, ma non modificarle.

Per dettagli sulla creazione o la gestione di ruoli FSx collegati ad Amazon Service, consulta. Utilizzo di ruoli collegati ai servizi per Amazon FSx

Esempi di policy basate sull'identità per Amazon for ONTAP FSx NetApp

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare FSx risorse Amazon. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM (console) nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da Amazon FSx, incluso il formato di ARNs per ogni tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon FSx nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della FSx console Amazon
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare FSx risorse Amazon nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando si creano o modificano policy basate sull'identità, seguire 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 maggiori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente di IAM.

- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle 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 CloudFormation. Per maggiori informazioni, consultare la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare Convalida delle policy per il Sistema di analisi degli accessi IAM nella Guida per l'utente di 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, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare Protezione dell'accesso API con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della FSx console Amazon

Per accedere alla console Amazon FSx for NetApp ONTAP, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle FSx risorse Amazon presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la FSx console Amazon, allega anche la policy `AmazonFSxConsoleReadOnlyAccess` AWS gestita alle entità. Per maggiori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente di IAM.

Puoi vedere le politiche `AmazonFSxConsoleReadOnlyAccess` e le altre politiche dei servizi FSx gestiti di Amazon inAWS politiche gestite per Amazon FSx for NetApp ONTAP.

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 collegate 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 relativi all'identità e all'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
- Voglio consentire a persone esterne Account AWS a me di accedere alle mie FSx risorse Amazon

Non sono autorizzato a eseguire un'azione in Amazon FSx

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `fsx:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `fsx:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon FSx.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon FSx. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne Account AWS a me di accedere alle mie FSx risorse Amazon

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon FSx supporta queste funzionalità, consultaCome funziona Amazon FSx for NetApp ONTAP con IAM.
- Per scoprire come fornire l'accesso alle tue risorse attraverso Account AWS le risorse di tua proprietà, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.

- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente di IAM.

Utilizzo di ruoli collegati ai servizi per Amazon FSx

Amazon FSx utilizza ruoli collegati ai servizi AWS Identity and Access Management (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ad Amazon. FSx I ruoli collegati ai servizi sono predefiniti da Amazon FSx e includono tutte le autorizzazioni richieste dal servizio per chiamare altri AWS servizi per tuo conto.

Un ruolo collegato al servizio semplifica la configurazione di Amazon FSx perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Amazon FSx definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Amazon FSx può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato al servizio solo dopo avere eliminato le risorse correlate. In questo modo proteggi le tue FSx risorse Amazon perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni 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 policy, consulta Amazon FSx ServiceRolePolicy.

Dettagli delle autorizzazioni

Le autorizzazioni dei AWSService RoleForAmazon FSx ruoli sono definite dalla policy FSx ServiceRolePolicy AWS gestita da Amazon. AWSServiceRoleForAmazonFSx Dispone delle seguenti autorizzazioni:

> **Note**
>
> AWSServiceRoleForAmazonFSx Viene utilizzato da tutti i tipi di FSx file system di Amazon; alcune delle autorizzazioni elencate non sono applicabili a FSx ONTAP.

- `ds`— Consente FSx ad Amazon di visualizzare, autorizzare e non autorizzare le applicazioni nella tua directory. Directory Service
- `ec2`— Consente FSx ad Amazon di effettuare le seguenti operazioni:
  - Visualizza, crea e dissocia le interfacce di rete associate a un FSx file system Amazon.
  - Visualizza uno o più indirizzi IP elastici associati a un FSx file system Amazon.
  - Visualizza Amazon VPCs, i gruppi di sicurezza e le sottoreti associati a un FSx file system Amazon.
  - Assegna IPv6 indirizzi alle interfacce di rete dei clienti che dispongono di un tag. `AmazonFSx.FileSystemId`
  - Annulla l'assegnazione IPv6 degli indirizzi dalle interfacce di rete dei clienti che dispongono di un tag. `AmazonFSx.FileSystemId`
  - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
  - Crea un'autorizzazione per un utente AWS autorizzato a eseguire determinate operazioni su un'interfaccia di rete.
- `cloudwatch`— Consente FSx ad Amazon di pubblicare punti dati metrici nello CloudWatch spazio dei FSx nomi AWS/.
- `route53`— Consente FSx ad Amazon di associare un Amazon VPC a una zona ospitata privata.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
```

```
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
```

```
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
```

```
            }
        }
    ]
}
```

Eventuali aggiornamenti a questa politica sono descritti inFSx Aggiornamenti Amazon alle politiche AWS gestite.

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato al servizio nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Amazon FSx

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un file system nella CLI Console di gestione AWS IAM o nell'API IAM, Amazon FSx crea il ruolo collegato al servizio per te.

> **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 al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un file system, Amazon FSx crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato ai servizi per Amazon FSx

Amazon FSx non consente di modificare il ruolo AWSService RoleForAmazon FSx collegato al servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile 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 FSx servizio Amazon utilizza il ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Usa la console IAM, la CLI IAM oppure l'API IAM per eliminare il ruolo collegato al servizio AWSServiceRoleForAmazonFSx. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati FSx ai servizi Amazon

Amazon FSx supporta l'utilizzo di ruoli collegati ai servizi in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta AWS Regioni ed endpoint.

Usare i tag con Amazon FSx

Puoi utilizzare i tag per controllare l'accesso alle FSx risorse Amazon e implementare il controllo degli accessi basato sugli attributi (ABAC). Per applicare tag alle FSx risorse Amazon durante la creazione, gli utenti devono disporre di determinate autorizzazioni AWS Identity and Access Management (IAM).

Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione

Con alcune azioni FSx Amazon API per la creazione di risorse, puoi specificare i tag quando crei la risorsa. Puoi utilizzare questi tag di risorsa 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 di autorizzazioni esplicite a utilizzare l'azione `fsx:TagResource`.

La seguente politica di esempio consente agli utenti di creare file system e macchine virtuali di archiviazione (SVMs) 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 politica 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 FSx delle risorse Amazon, consultaEtichettare le risorse Amazon FSx. Per ulteriori informazioni sull'uso dei tag per controllare l'accesso alle FSx risorse di Amazon, consultaUtilizzo dei tag per controllare l'accesso alle FSx risorse Amazon.

Utilizzo dei tag per controllare l'accesso alle FSx risorse Amazon

Per controllare l'accesso alle FSx risorse e alle azioni di Amazon, puoi utilizzare le policy IAM basate sui tag. È possibile fornire il controllo in due modi:

- Puoi controllare l'accesso alle FSx risorse Amazon in base ai tag presenti su tali risorse.
- Puoi controllare quali tag possono essere trasferiti in una condizione di richiesta IAM.

Per informazioni su come utilizzare i tag per controllare l'accesso alle AWS risorse, consulta Controlling access using tags nella IAM User Guide. Per ulteriori informazioni sull'etichettatura FSx delle risorse Amazon al momento della creazione, consultaConcessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione. Per ulteriori informazioni sull'assegnazione di tag alle risorse, consulta Etichettare le 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 FSx risorsa Amazon, puoi utilizzare i tag sulla risorsa. Ad esempio, è possibile consentire o negare operazioni API specifiche su una risorsa di gateway di file in base alla coppia chiave-valore del tag sulla risorsa.

Example Politica di esempio: crea un file system 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 for NetApp ONTAP con un tag specifico

Questa policy consente agli utenti di creare backup solo FSx per i volumi ONTAP etichettati con la coppia chiave-valore,. `key=Department` `value=Finance` Il backup viene creato con il tag. `Department=Finance`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 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`

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
```

```
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333: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`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
```

```
            "Resource": "arn:aws:fsx:us-east-1:111122223333: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`.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
            "Condition": {
                "StringEquals": {
```

```
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

AWS politiche gestite per Amazon FSx for NetApp ONTAP

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 Si consiglia pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i propri 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 AWS nella Guida per l'utente di IAM.

Amazon FSx ServiceRolePolicy

Consente FSx ad Amazon di gestire AWS le risorse per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

AWS politica gestita: Amazon FSx DeleteServiceLinkedRoleAccess

Non è possibile collegare `AmazonFSxDeleteServiceLinkedRoleAccess`alle entità IAM. Questa politica è collegata a un servizio e utilizzata solo con il ruolo collegato al servizio per quel servizio. Non è possibile collegare, scollegare, modificare o eliminare questa policy. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

Questa politica concede autorizzazioni amministrative che consentono FSx ad Amazon di eliminare il suo Service Linked Role per l'accesso ad Amazon S3, utilizzato solo da Amazon FSx for Lustre.

Dettagli delle autorizzazioni

Questa policy include le autorizzazioni `iam` per consentire FSx ad Amazon di visualizzare, eliminare e visualizzare lo stato di eliminazione per i FSx Service Linked Roles for Amazon S3 access.

Per visualizzare le autorizzazioni per questa politica, consulta Amazon FSx DeleteServiceLinkedRoleAccess nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx FullAccess

Puoi collegare Amazon FSx FullAccess alle tue entità IAM. Amazon attribuisce questa politica FSx anche a un ruolo di servizio che consente FSx ad Amazon di eseguire azioni per tuo conto.

Fornisce accesso completo ad Amazon FSx e accesso ai AWS servizi correlati.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai mandanti l'accesso completo per eseguire tutte le FSx azioni di Amazon, ad eccezione `BypassSnaplockEnterpriseRetention` di.
- `ds`— Consente ai dirigenti di visualizzare le informazioni sulle Directory Service directory.
- `ec2`
  - Consente ai mandanti di creare tag nelle condizioni specificate.
  - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
- `iam`— Consente ai principi di creare un ruolo collegato al FSx servizio Amazon per conto dell'utente. Ciò è necessario affinché Amazon FSx possa gestire AWS le risorse per conto dell'utente.
- `firehose`— Consente ai mandanti di scrivere record su un Amazon Data Firehose. Ciò è necessario FSx per consentire agli utenti di monitorare l'accesso al file system di Windows File Server inviando registri di accesso di controllo a Firehose.
- `logs`— Consente ai responsabili di creare gruppi di log, flussi di log e scrivere eventi nei flussi di log. Ciò è necessario FSx per consentire agli utenti di monitorare l'accesso al file system di Windows File Server inviando i registri di accesso di controllo a Logs. CloudWatch

Per visualizzare le autorizzazioni per questa politica, consulta Amazon FSx FullAccess nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx ConsoleFullAccess

È possibile allegare la policy `AmazonFSxConsoleFullAccess` alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo ad Amazon FSx e l'accesso ai AWS servizi correlati tramite. Console di gestione AWS

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai responsabili di eseguire tutte le azioni nella console di FSx gestione Amazon, ad eccezione `BypassSnaplockEnterpriseRetention` di.
- `cloudwatch`— Consente ai responsabili di visualizzare CloudWatch allarmi e metriche nella console di gestione Amazon FSx .
- `ds`— Consente ai responsabili di elencare le informazioni su una directory. Directory Service
- `ec2`
  - Consente ai mandanti di creare tag sulle tabelle di routing, elencare le interfacce di rete, le tabelle di routing, i gruppi di sicurezza, le sottoreti e il VPC associato a un file system Amazon. FSx
  - Consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
  - Consente ai responsabili di visualizzare le interfacce di rete elastiche associate a un FSx file system Amazon.
- `kms`— Consente ai principali di elencare gli alias per le chiavi. AWS Key Management Service
- `s3`— Consente ai responsabili di elencare alcuni o tutti gli oggetti in un bucket Amazon S3 (fino a 1000).
- `secretsmanager`— Consente ai responsabili di elencare i segreti per la selezione delle credenziali degli Gestione dei segreti AWS account del servizio di accesso al dominio.
- `iam`— Concede l'autorizzazione a creare un ruolo collegato al servizio che consente FSx ad Amazon di eseguire azioni per conto dell'utente.

Per visualizzare le autorizzazioni per questa politica, consulta Amazon FSx ConsoleFullAccess nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx ConsoleReadOnlyAccess

È possibile allegare la policy `AmazonFSxConsoleReadOnlyAccess` alle identità IAM.

Questa politica concede autorizzazioni di sola lettura ad FSx Amazon e ai servizi AWS correlati in modo che gli utenti possano visualizzare le informazioni su questi servizi in. Console di gestione AWS

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai responsabili di visualizzare le informazioni sui FSx file system Amazon, inclusi tutti i tag, nella Console di FSx gestione Amazon.
- `cloudwatch`— Consente ai responsabili di visualizzare CloudWatch allarmi e metriche nella Console di gestione Amazon FSx .
- `ds`— Consente ai responsabili di visualizzare le informazioni su una Directory Service directory nella Console di FSx gestione Amazon.
- `ec2`
  - Consente ai responsabili di visualizzare interfacce di rete, gruppi di sicurezza, sottoreti e il VPC associato a un FSx file system Amazon nella Console di gestione Amazon. FSx
  - Consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
  - Consente ai responsabili di visualizzare le interfacce di rete elastiche associate a un FSx file system Amazon.
- `kms`— Consente ai mandanti di visualizzare gli alias per le AWS Key Management Service chiavi nella Console di FSx gestione Amazon.
- `log`— Consente ai responsabili di descrivere i gruppi di log di Amazon CloudWatch Logs associati all'account che effettua la richiesta. Ciò è necessario per consentire ai responsabili di visualizzare la configurazione esistente di controllo degli accessi ai file per un file system FSx per Windows File Server.
- `secretsmanager`— Consente ai responsabili di elencare i segreti per la selezione delle credenziali degli Gestione dei segreti AWS account del servizio di accesso al dominio.
- `firehose`— Consente ai mandanti di descrivere i flussi di distribuzione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano

visualizzare la configurazione esistente di controllo dell'accesso ai file per un file system FSx per Windows File Server.

Per visualizzare le autorizzazioni per questa politica, consulta Amazon FSx ConsoleReadOnlyAccess nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx ReadOnlyAccess

È possibile allegare la policy `AmazonFSxReadOnlyAccess` alle identità IAM.

- `fsx`— Consente ai responsabili di visualizzare le informazioni sui FSx file system Amazon, inclusi tutti i tag, nella Console di FSx gestione Amazon.
- `ec2`— Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.

Per visualizzare le autorizzazioni per questa politica, consulta Amazon FSx ReadOnlyAccess nella AWS Managed Policy Reference Guide.

FSx Aggiornamenti Amazon alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon FSx da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS sulla pagina Amazon FSx Cronologia dei documenti per Amazon FSx for NetApp ONTAP.

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `secretsmanager:ListSecrets` che consente ai responsabili di elencare i segreti Gestione dei segreti AWS per la selezione delle credenziali dell'account del servizio di accesso al dominio.	5 novembre 2025

Modifica	Descrizione	Data
Amazon FSx ConsoleReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `secretsmanager:ListSecrets` che consente ai responsabili di elencare i segreti Gestione dei segreti AWS per la selezione delle credenziali dell'account del servizio di accesso al dominio.	3 novembre 2025
Amazon FSx ServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:AssignIpv6Addresses` che consente ai mandanti di assegnare IPv6 indirizzi alle interfacce di rete dei clienti dotate di un tag. `AmazonFSx.FileSystemId`	22 luglio 2025
Amazon FSx ServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:UnassignIpv6Addresses` che consente ai mandanti di annullare l'assegnazione IPv6 degli indirizzi dalle interfacce di rete dei clienti che dispongono di un tag. `AmazonFSx.FileSystemId`	22 luglio 2025

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:CreateAndAttachS3AccessPoint` che consente ai responsabili di creare un punto di accesso S3 e collegarlo a un FSx volume.	25 giugno 2025
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:DescribeS3AccessPointAttachments` che consente ai responsabili di elencare tutti i punti di accesso S3 Account AWS in un colpo solo. Regione AWS	25 giugno 2025
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:DetachAndDeleteS3AccessPoint` che consente ai responsabili di eliminare un punto di accesso S3.	25 giugno 2025
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:CreateAndAttachS3AccessPoint` che consente ai responsabili di creare un punto di accesso S3 e collegarlo a un FSx volume.	25 giugno 2025

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:DescribeS3AccessPointAttachments` che consente ai responsabili di elencare tutti i punti di accesso S3 Account AWS in un colpo solo. Regione AWS	25 giugno 2025
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `fsx:DetachAndDeleteS3AccessPoint` che consente ai responsabili di eliminare un punto di accesso S3.	25 giugno 2025
Amazon FSx ConsoleReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:DescribeNetworkInterfaces` che consente ai responsabili di visualizzare le interfacce di rete elastiche associate al proprio file system.	25 febbraio 2025
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:DescribeNetworkInterfaces` che consente ai responsabili di visualizzare le interfacce di rete elastiche associate al proprio file system.	07 febbraio 2025

Modifica	Descrizione	Data
Amazon FSx ServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx ReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx ConsoleReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica dei dati tra regioni e account FSx per i file system OpenZFS.	20 dicembre 2023
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica dei dati tra regioni e account FSx per i file system OpenZFS.	20 dicembre 2023

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica su richiesta dei volumi FSx per i file system OpenZFS.	26 novembre 2023
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica su richiesta dei volumi FSx per i file system OpenZFS.	26 novembre 2023
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare, abilitare e disabilitare il supporto VPC condiviso FSx per i file system ONTAP Multi-AZ.	14 novembre 2023
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare, abilitare e disabilitare il supporto VPC condiviso FSx per i file system ONTAP Multi-AZ.	14 novembre 2023

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx gestire le configurazioni di rete FSx per i file system OpenZFS Multi-AZ.	9 agosto 2023
AWS politica gestita: Amazon FSx ServiceRolePolicy — Aggiornamento a una politica esistente	Amazon ha FSx modificato l'`cloudwatch:PutMetricData` autorizzazione esistente in modo che Amazon FSx pubblichi le CloudWatch metriche nel namespace. `AWS/FSx`	24 luglio 2023
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiornato la politica per rimuovere l'`fsx:*`autorizzazione e aggiungere `fsx` azioni specifiche.	13 luglio 2023
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiornato la politica per rimuovere l'`fsx:*`autorizzazione e aggiungere `fsx` azioni specifiche.	13 luglio 2023
Amazon FSx ConsoleReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare metriche di prestazioni migliorate e azioni consigliate FSx per i file system Windows File Server nella console Amazon FSx .	21 settembre 2022

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare metriche di prestazioni migliorate e azioni consigliate FSx per i file system Windows File Server nella console Amazon FSx .	21 settembre 2022
Amazon FSx ReadOnlyAccess — Avviata la politica di tracciamento	Questa politica garantisce l'accesso in sola lettura a tutte le FSx risorse Amazon e a tutti i tag ad esse associati.	4 febbraio 2022
Amazon FSx DeleteServiceLinkedRoleAccess — Avviata la politica di tracciamento	Questa politica concede autorizzazioni amministrative che consentono FSx ad Amazon di eliminare il suo Service Linked Role per l'accesso ad Amazon S3.	7 gennaio 2022
Amazon FSx ServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx gestire le configurazioni di rete per i file system Amazon FSx for NetApp ONTAP.	2 settembre 2021
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare tag sulle tabelle di routing EC2 per chiamate con ambito limitato.	2 settembre 2021

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx creare file system Amazon FSx for NetApp ONTAP Multi-AZ.	2 settembre 2021
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare tag sulle tabelle di routing EC2 per chiamate con ambito limitato.	2 settembre 2021
Amazon FSx ServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx descrivere e scrivere su CloudWatch Logs i flussi di log. Ciò è necessario per consentire agli utenti di visualizzare i registri di controllo degli accessi ai file FSx per i file system Windows File Server utilizzando Logs. CloudWatch	08 giugno 2021

Modifica	Descrizione	Data
Amazon FSx ServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx descrivere e scrivere nei flussi di distribuzione di Amazon Data Firehose. Ciò è necessario per consentire agli utenti di visualizzare i log di controllo degli accessi ai file FSx per un file system Windows File Server utilizzando Amazon Data Firehose.	08 giugno 2021
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere e creare gruppi di log di CloudWatch Logs, log stream e scrivere eventi nei flussi di log. Ciò è necessario affinché i responsabili possano visualizzare i log di controllo degli accessi ai file FSx per i file system di Windows File Server utilizzando Logs. CloudWatch	08 giugno 2021

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere e scrivere record su Amazon Data Firehose. Ciò è necessario per consentir e agli utenti di visualizzare i log di controllo degli accessi ai file FSx per un file system Windows File Server utilizzan do Amazon Data Firehose.	08 giugno 2021
Amazon FSx ConsoleFu llAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere i gruppi di log di Amazon CloudWatch Logs associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano scegliere un gruppo di log CloudWatc h Logs esistente durante la configurazione del controllo dell'accesso ai file per un FSx file system per Windows File Server.	08 giugno 2021

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere i flussi di distribuzione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano scegliere un flusso di distribuzione Firehose esistente durante la configurazione del controllo dell'accesso ai file per FSx un file system Windows File Server.	08 giugno 2021
Amazon FSx ConsoleReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere i gruppi di log di Amazon CloudWatch Logs associati all'account che effettua la richiesta. Ciò è necessario per consentire ai responsabili di visualizzare la configurazione esistente di controllo dell'accesso ai file per un file system FSx per Windows File Server.	08 giugno 2021

Modifica	Descrizione	Data
Amazon FSx ConsoleReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere i flussi di distribuzione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario per consentire ai responsabili di visualizzare la configurazione esistente di controllo dell'accesso ai file per un FSx file system per Windows File Server.	08 giugno 2021
Amazon FSx ha iniziato a tracciare le modifiche	Amazon FSx ha iniziato a tracciare le modifiche alle sue politiche AWS gestite.	08 giugno 2021

Controllo degli accessi ai file system con Amazon VPC

Accedi ai tuoi file system Amazon FSx for NetApp ONTAP SVMs 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 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 associati e. SVMs È possibile 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 tuo FSx file system Amazon, 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 FSx file del tuo file system Amazon su una cartella sull'istanza di calcolo supportata.

Per ulteriori informazioni sulle regole dei gruppi di sicurezza, consulta le regole del gruppo di sicurezza nella 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 in https://console.aws.amazon.com /ec2.
2. Fare clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
3. Scegliere Create Security Group (Crea un gruppo di sicurezza).
4. Specificare un nome e una descrizione per il gruppo di sicurezza.
5. Per VPC, scegli 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 di origine, devi 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, and/or macOS che accedono ai dati del file system tramite NFS, SMB o iSCSI.

- Qualsiasi file ONTAP systems/clusters che invierai al tuo file system (ad esempio, da utilizzare o). SnapMirror SnapVault FlexCache
- Qualsiasi client che utilizzerai per accedere all'API REST, alla CLI ZAPIs o all'interfaccia a riga di comando di ONTAP (ad esempio, Harvest/Grafana un'istanza NetApp , un connettore NetApp o una console).

Protocollo	Porte	Ruolo
Tutte le regole ICMP	Tutti	Eseguire il 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 intercluster LIFs
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 inbound/outbound regole.

Convalida della conformità per Amazon FSx for ONTAP NetApp

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. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta la Documentazione AWS sulla sicurezza.

Amazon FSx per NetApp ONTAP e endpoint VPC di interfaccia ()AWS PrivateLink

Puoi migliorare il livello di sicurezza del tuo VPC configurando FSx Amazon per utilizzare un endpoint VPC di interfaccia. Gli endpoint VPC di interfaccia sono basati su una tecnologia che consente di AWS PrivateLinkaccedere ad FSx APIs Amazon in modo privato senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare con Amazon. FSx APIs Il traffico tra il tuo VPC e Amazon FSx non esce dalla AWS rete.

Ogni endpoint VPC di interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti. Un'interfaccia di rete fornisce un indirizzo IP privato che funge da punto di ingresso per il traffico verso l' FSx API Amazon. Amazon FSx supporta endpoint VPC configurati con IPv4 e tipi di indirizzi IP Dualstack (IPv4 e). IPv6 Per ulteriori informazioni, consulta Creazione di un endpoint VPC di interfaccia nella Amazon VPC User Guide.

Considerazioni sugli endpoint VPC con FSx interfaccia Amazon

Prima di configurare un endpoint VPC di interfaccia per Amazon FSx, assicurati di esaminare le proprietà e le limitazioni dell'endpoint VPC dell'interfaccia nella Amazon VPC User Guide.

Puoi chiamare qualsiasi operazione dell' FSx API Amazon dal tuo VPC. Ad esempio, puoi creare un file system FSx for ONTAP chiamando l' CreateFileSystem API dall'interno del tuo VPC. Per l'elenco completo di Amazon FSx APIs, consulta Actions in Amazon FSx API Reference.

Considerazioni sul peering VPC

Puoi connetterne altri VPCs al VPC con endpoint VPC di interfaccia utilizzando il peering VPC. Il peering VPC è una connessione di rete tra due. VPCs Puoi stabilire una connessione peering VPC tra i tuoi due VPCs o con un VPC in un altro. Account AWS VPCs Possono essere disponibili anche in due versioni diverse. Regioni AWS

Il traffico tra utenti VPCs peer rimane sulla AWS rete e non attraversa la rete Internet pubblica. Una volta eseguito il peering dei VPC, risorse come le istanze Amazon Elastic Compute Cloud (Amazon EC2) in entrambe possono VPCs accedere all' FSx API Amazon tramite endpoint VPC di interfaccia creati in uno dei. VPCs

Creazione di un endpoint VPC di interfaccia per Amazon API FSx

Puoi creare un endpoint VPC per l' FSx API Amazon utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta Creazione di un endpoint VPC di interfaccia nella Amazon VPC User Guide.

Per creare un endpoint VPC di interfaccia per Amazon FSx, usa uno dei seguenti:

- **`com.amazonaws.`*`region`*`.fsx`**— Crea un endpoint per le operazioni delle FSx API Amazon.
- **`com.amazonaws.`*`region`*`.fsx-fips`**— Crea un endpoint per l' FSx API Amazon conforme al Federal Information Processing Standard (FIPS) 140-2.

Per utilizzare l'opzione DNS privato, devi impostare `enableDnsSupport` gli attributi `enableDnsHostnames` e del tuo VPC. Per ulteriori informazioni, consulta Visualizzazione e aggiornamento del supporto DNS per il tuo VPC nella Amazon VPC User Guide.

Ad eccezione Regioni AWS della Cina, se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API ad Amazon FSx con l'endpoint VPC utilizzando il suo nome DNS predefinito per, ad esempio. Regione AWS`fsx.us-east-1.amazonaws.com` Per la Cina (Pechino) e la Cina (Ningxia) Regioni AWS, puoi effettuare richieste API con l'endpoint VPC utilizzando e, rispettivamente. `fsx-api.cn-north-1.amazonaws.com.cn` `fsx-api.cn-northwest-1.amazonaws.com.cn`

Per ulteriori informazioni, consulta Accesso a un servizio tramite un endpoint VPC di interfaccia nella Amazon VPC User Guide.

Creazione di una policy sugli endpoint VPC per Amazon FSx

Per controllare l'accesso all' FSx API Amazon, 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 FSx per ONTAP NetApp

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. 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 è possibile 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 aiutarti a supportare le tue esigenze di resilienza e backup dei dati.

Backup e ripristino

Amazon FSx crea e salva backup automatici dei volumi nel tuo file system Amazon FSx for NetApp ONTAP. Amazon FSx crea backup automatici dei tuoi volumi durante la finestra di backup del tuo file system Amazon FSx for NetApp ONTAP. Amazon FSx salva i backup automatici dei tuoi volumi in base al periodo di conservazione dei backup da te 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 Protezione dei dati con backup di volume.

Snapshot

Amazon FSx crea copie istantanee dei volumi Amazon FSx for NetApp ONTAP. 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 Protezione dei dati con istantanee.

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 replica FSx 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, durabilità e opzioni di implementazione.

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, durabilità e opzioni di implementazione.

Sicurezza dell'infrastruttura in Amazon FSx per NetApp ONTAP

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 tramite 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.

Usa NetApp ONTAP Vscan con FSx per ONTAP

È possibile utilizzare la funzionalità NetApp ONTAP's Vscan per eseguire il software antivirus di terze parti supportato. Per ulteriori informazioni, consulta le seguenti risorse per ciascuna delle soluzioni supportate.

- Deep Instinct: soluzioni partner Vscan e documentazione Deep Instinct [1]
- SentinelOne — Soluzioni partner Vscan e Singularity Cloud Data Security SentinelOne
- Symantec: soluzioni partner Vscan e Symantec Protection Engine
- Trellix (in precedenza) — soluzioni partner Vscan e Trellix Product McAfee Docs
- Trend Micro — Soluzioni partner Vscan

> **Note**
>
> [1] È necessario accedere al portale di Deep Instinct per visualizzare la relativa documentazione.

ONTAPruoli e utenti

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. Assegni ruoli agli utenti allo scopo di controllarne l'accesso alle FSx risorse For ONTAP quando

usi l'API ONTAP REST e la CLI. Sono disponibili ONTAP ruoli separati per gli utenti del file system ONTAP e FSx per gli utenti della macchina virtuale di archiviazione (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 degli amministratori 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 FSx file system 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 ONTAP
`fsxadmin-readonly`	tutto	`security login password`

Nome ruolo	Livello di accesso	Ai seguenti comandi o directory di comandi
		Solo per gestire il proprio account utente, la password locale e le informazioni chiave
	nessuno	`security`
	sola lettura	Tutte le altre directory di comandi disponibili in FSx ONTAP

Ruoli e utenti degli amministratori 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 LUNs • Esegui SnapLock operazioni, ad eccezione dell'eliminazione con privilegi • Configurazione dei protocolli: NFS, SMB e iSCSI

Nome ruolo	Funzionalità
	• Configura i servizi: DNS, LDAP e NIS • Monitoraggio dei processi • Monitora le connessioni di rete e l'interfaccia di rete • 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 LUNs • 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 LUNs • 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

Nome ruolo	Funzionalità
`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 volumi e informazioni di rete
`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 processi • 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 i volumi e LUNs • Visualizza servizi e protocolli

Per ulteriori informazioni su come creare un nuovo ruolo SVM, vedereCreazione di ruoli 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 a 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 Come funziona l' SVMs accesso 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 utenti ONTAP

Argomenti

Creazione di utenti 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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. Usa il comando `security login create` ONTAP CLI per creare un nuovo account utente sul tuo file system FSx for ONTAP o SVM.

   Inserite i dati relativi ai 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`— Specifica 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 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 SVMs.

```
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 ruoli 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 -vserver vs1.example.com -role vol_role -
   cmddirname volume
   ```

2. Specificate i seguenti parametri obbligatori nel comando:

   - `-vserver`il nome della SVM
   - `-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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 della 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 obbligatori 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	Description
`-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`
`-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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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
```

Quote

Di seguito, puoi scoprire le quote quando lavori con Amazon FSx for NetApp ONTAP.

Argomenti

Quote che è possibile incrementare

Di seguito sono riportate le quote per Amazon FSx for NetApp ONTAP per ciascuna Account AWS unità Regione AWS che puoi aumentare.

Risorsa	Di default	Description
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 FSx Amazon 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	Di default	Description
		Amazon FSx for NetApp ONTAP che puoi avere in questo account.
ONTAPbackup	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 un. Account AWS
Punti di accesso Amazon S3	10.000	Il numero massimo di punti di accesso Amazon S3 per tutti i tipi di origini dati supportati (ad esempio, FSx per NetApp ONTAP) che puoi creare per regione in un. Account AWS Questo è anche il numero massimo di punti di accesso S3 che puoi collegare a un singolo file system o volume FSx per NetApp ONTAP. Questa quota è una quota di servizio Amazon S3 e può essere regolata tramite Service Quotas.

Richiesta di un aumento delle quote

1. Aprire la pagina Supporto AWS, 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 FSx quota che desideri aumentare e il valore a cui desideri 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 for NetApp 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 di archiviazione SSD minima per avviare un'operazione di riduzione	1.126 GiB per coppia HA
Percentuale minima di diminuzione delle unità SSD	9% in meno rispetto alla capacità attuale
Capacità massima di archiviazione SSD	• File system Single-AZ di seconda generazione: 512 TiB per coppia HA, fino a 1 PiB • File system Multi-AZ di seconda generazione: 512 TiB • File system di prima generazione: 192 TiB

Risorsa	Limite per file system
Utilizzo massimo consigliato dell'SSD	80% per prestazioni ottimali e funzionalità di suddivisione in più livelli
Utilizzo massimo dell'SSD per ridurre le operazioni	80% prima e dopo l'operazione di riduzione
Numero massimo di IOPS SSD	File system di seconda generazione: • 200.000 per coppia HA (fino a 12 coppie) per Single-AZ • 200.000 in totale per Multi-AZ File system di prima generazione: • 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 Regioni AWS paesi in cui è disponibile ONTAP FSx
Capacità di throughput minima	• File system di seconda generazione (1 coppia HA): 384 MBps • File system di seconda generazione (2 o più coppie HA): 1.536 per coppia HA MBps • File system di prima generazione: 128 MBps

Risorsa	Limite per file system
Capacità di throughput massima	File system di seconda generazione: • 73.728 1 MBps per Single-AZ • 6.144 per Multi-AZ MBps File system di prima generazione: • 4.096 MBps [2] nella regione Stati Uniti orientali (Ohio), nella regione Stati Uniti orientali (Virginia settentrionale), nella regione Stati Uniti occidentali (Oregon) ed Europa (Irlanda) • 2.048 in tutti gli altri paesi MBps in cui è disponibile ONTAP Regioni AWS FSx
Numero massimo di volumi	• File system di seconda generazione (1 coppia HA): 500 • File system di seconda generazione (2 o più coppie HA): 1.000 • File system di prima generazione: 500 Quando si utilizzano punti di accesso S3 con il file system: • File system di seconda generazione (1 coppia HA): 491 • File system di seconda generazione (2 o più coppie HA): 975 per 2 coppie HA (903 per 12 coppie HA) • File system di prima generazione: 491

Risorsa	Limite per file system
Numero massimo di istantanee	1.023 per volume 3
Numero massimo di backup	4.091 per volume 4

Risorsa	Limite per file system
Numero massimo di SVMs	File system di seconda generazione con una coppia HA e IPv4 solo tipo di rete: • 6 (384 MBps della capacità di throughput) • 6 (768 MBps della capacità di throughput) • 14 (1.536 MBps della capacità di throughput) • 14 (3.072 MBps della capacità produttiva) • 24 (6.144 MBps della capacità di throughput) File system di seconda generazio ne con una coppia HA e tipo di rete dual-stack: • 6 (384 della capacità di throughput) MBps • 6 (768 MBps della capacità di throughput) • 11 (1.536 MBps della capacità di throughput) • 11 (3.072 MBps della capacità produttiva) • 11 (6.144 MBps della capacità di throughput) File system di seconda generazione con 2—12 coppie HA e tipo di rete solo o dual-stack: IPv4

Risorsa	Limite per file system
	• 11 File system di prima generazione con tipo di rete -only: IPv4 • 6 (128 MBps capacità di throughput) • 6 (capacità di MBps trasmissione 256) • 14 (512 MBps capacità di trasmissione) • 14 (capacità di MBps trasmissione 1.024) • 24 (capacità di trasmissione di 2.048 MBps) • 24 (MBps 4.096 capacità di trasmissione) File system di prima generazione con tipo di rete dual-stack: • 6 (128 capacità di trasmissione) MBps • 6 (capacità di MBps trasmissione 256) • 11 (capacità di MBps trasmissione 512) • 11 (capacità di MBps trasmissione 1.024) • 11 (capacità di throughput di 2.048 MBps)

Risorsa	Limite per file system
	• 11 (MBps 4.096 capacità di trasmissione)
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]
Numero massimo di connessioni client per file server [6]	100.000

Note

[1] Su un file system Single-AZ di seconda generazione con 12 coppie HA (6.144 MBps per coppia HA). Per ulteriori informazioni, consulta Gestione delle coppie ad alta disponibilità (HA).

[2] Per fornire il 4% GBps della capacità di throughput, il file system di prima generazione di FSx for ONTAP richiede una configurazione del numero massimo di IOPS SSD (160.000) e un minimo di 5.120 GiB di capacità di archiviazione SSD in un ambiente supportato. Regione AWS Per ulteriori informazioni su quali dispositivi supportano 4.096 di capacità di throughput, vedere. Regioni AWS MBps 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 route SVMs 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 SVMs nel file system) * (tabelle di routing associate al file system).

[6] Una connessione client è definita come una singola connessione TCP a un determinato file server. Esiste un file server attivo per coppia HA in un file system. Un client può avere più connessioni TCP a un file server. Ad esempio, se un client utilizza multipathing.

Risoluzione dei problemi di Amazon FSx for NetApp ONTAP

Utilizza le seguenti sezioni per facilitare la risoluzione dei problemi relativi ai file system FSx ONTAP.

Argomenti

Il file system 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 ONTAP. FSx
- L'account del proprietario ha smesso di condividere la sottorete VPC.

Se l'account proprietario ha interrotto la condivisione della sottorete VPC, nella console del file system in questione 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 FSx per i file system 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 ONTAP. FSx
- L'account del proprietario ha smesso di condividere la sottorete VPC.

Per risolvere il problema, devi contattare l'account proprietario che ha condiviso con te la sottorete VPC. Per ulteriori informazioni, vedere Creazione FSx per i file system ONTAP in sottoreti condivise per ulteriori informazioni.

Il livello di archiviazione SSD del file system è pieno per oltre il 90%

Il livello di storage SSD del file system Single-AZ o Multi-AZ è attualmente pieno per oltre il 90%. Ti consigliamo di non superare l'80% di utilizzo del livello di storage SSD su base continuativa. Se non liberate spazio nel livello di archiviazione SSD prima della prossima finestra di manutenzione del file system, FSx for ONTAP ridurrà temporaneamente la velocità di trasmissione del file system per tutta la durata dell'operazione di patching. Questo viene fatto per garantire che i processi di manutenzione in background possano essere completati entro un periodo di tempo ragionevole. Per evitare ciò, riduci l'utilizzo del livello di archiviazione SSD al di sotto del 90%. È possibile ridurre l'utilizzo degli SSD in diversi modi, tra cui:

- Aumentare la capacità di archiviazione SSD del file system.
- Eliminando i dati non necessari.
- Eliminando istantanee di volume non necessarie.

Per ulteriori informazioni, consulta Gestione della capacità di archiviazione.

Non puoi accedere al tuo file system

Questa sezione descrive i problemi e le risoluzioni relativi all'impossibilità di accedere al file system.

Argomenti

Nel file system Multi-AZ mancano i tag della tabella di percorso

Amazon FSx gestisce le tabelle di routing VPC per i file system Multi-AZ utilizzando l'autenticazione basata su tag. In una o più tabelle di routing associate al tuo file system mancano attualmente questi tag delle tabelle di routing. Queste tabelle di percorso sono contrassegnate con`Key: AmazonFSx;`

`Value: ManagedByAmazonFSx`. Se non si aggiungono manualmente questi tag prima della finestra di manutenzione successiva, tutti i client nelle sottoreti associate alle tabelle di routing a cui mancano i tag perderanno temporaneamente l'accesso al file system per tutta la durata dell'operazione di applicazione delle patch. Per evitare ciò, aggiungi manualmente i tag mancanti della tabella delle rotte.

Per ulteriori informazioni, consulta Aggiornamento dei file system.

Il tuo file system ha più di 50 percorsi

Al file system sono attualmente associate più di 50 rotte. Se non si rimuovono alcune di queste route prima della successiva finestra di manutenzione programmata del file system, il processo di failover potrebbe richiedere più tempo del normale. Per evitare ciò, riduci il numero di percorsi a meno di 50. Di seguito sono riportati i passaggi che è possibile eseguire per ridurre il numero di percorsi associati al file system:

- Eliminazione di eventuali percorsi in eccesso
- Riduzione del numero di file SVMs associati al file system
- Riduzione del numero di tabelle di routing associate al file system

Per ulteriori informazioni, consultare Aggiornamento dei file system e Eliminazione di macchine virtuali di archiviazione (SVM).

Nel file system mancano le route verso uno o più file server

Al momento nel file system mancano le route verso uno o più file server e le tabelle di routing esistenti non dispongono di spazio sufficiente per aggiungere nuove voci della tabella di routing. Se non si aggiungono le route mancanti prima della successiva finestra di manutenzione programmata del file system, tutti i client connessi verranno disconnessi per tutta la durata dell'operazione di applicazione delle patch. Per evitare ciò, aggiungi le rotte mancanti.

Per ulteriori informazioni, consultare Aggiornamento dei file system e Quote.

L'interfaccia elastic network del file system è stata modificata o eliminata

Non è necessario modificare o eliminare nessuna 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 FSx rete Amazon. 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 scollega FSx automaticamente qualsiasi indirizzo IP elastico, che è un indirizzo IP pubblico raggiungibile da Internet che viene collegato all'interfaccia di rete elastica di un file system. 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 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 FSx da utilizzare per Amazon quando crei il tuo file system.

Se riesci a eseguire il ping dell'endpoint Intercluster del tuo file system ma non riesci a eseguire il ping dell'endpoint di gestione del file system (vedi Risorse del file system per maggiori 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 dei file system

Amazon non FSx può aggiornare la tabella di routing per i file system Multi-AZ creati utilizzando CloudFormation

Amazon FSx gestisce le tabelle di routing VPC per i file system Multi-AZ utilizzando l'autenticazione basata su tag. Queste tabelle di routing sono contrassegnate con. `Key: AmazonFSx; Value: ManagedByAmazonFSx` Durante la creazione o l'aggiornamento FSx per l'utilizzo di file system ONTAP Multi-AZ, si CloudFormation consiglia di aggiungere il `Key: AmazonFSx; Value: ManagedByAmazonFSx` tag manualmente.

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 non FSx può aggiornare tali tabelle di routing per indirizzare 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 dei 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 interrotto 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 interrotto la condivisione della sottorete VPC.

Se l'account proprietario ha interrotto la condivisione della sottorete VPC, nella console del file system in questione 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 di FSx for ONTAP.

La macchina virtuale di archiviazione (SVM) è in uno stato `MISCONFIGURED`

Esistono diverse cause potenziali per cui una macchina virtuale di storage entra in `MISCONFIGURED` uno stato, ognuna con la propria risoluzione, come segue.

La tua SVM ha un volume offline

Il file system contiene un volume che si trova in uno stato offline. Si consiglia di mantenere i volumi online su base continuativa. Se non metti online questo volume prima della prossima finestra di manutenzione del file system, Amazon FSx lo metterà temporaneamente online per tutta la durata dell'operazione di patching. Per evitare che ciò accada, accedi online o elimina il volume.

Per riportare online un volume offline, utilizzate il comando `volume online`ONTAPCLI, come illustrato nell'esempio seguente. Se esiste solo un SVM (Vserver), non è necessario specificare il parametro. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

La SVM dispone di un volume offline con un LUN iSCSI o un namespace NVMe/TCP

Il file system contiene un volume che si trova in uno stato limitato. Si consiglia di mantenere i volumi online su base continuativa. Se non metti online questo volume prima della prossima finestra di manutenzione del file system, Amazon FSx lo metterà temporaneamente online per tutta la durata dell'operazione di patching. Per evitare che ciò accada, accedi online o elimina il volume.

Per riportare online un volume offline, utilizzate il comando `volume online`ONTAPCLI, come illustrato nell'esempio seguente. Se esiste solo un SVM (Vserver), non è necessario specificare il parametro. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

La chiave Gestione dei segreti AWS segreta o KMS non è configurata correttamente

Amazon non FSx può stabilire una connessione con il controller o i controller di dominio Microsoft Active Directory. Questo perché il tuo account Gestione dei segreti AWS segreto o non AWS KMS key è configurato correttamente. Per ulteriori informazioni, consulta Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.

Per risolvere l'errore di configurazione, procedi come segue:

- Verifica che l'ARN segreto sia corretto e segua il formato corretto:. `arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`
- Verifica che il segreto contenga entrambi i campi obbligatori con valori non vuoti:
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`— Il nome utente dell'account del servizio AD.
  - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`— La password dell'account del servizio AD.
- Verifica che il segreto e la chiave abbiano una politica basata sulle risorse che conceda al servizio FSx Amazon l'autorizzazione `fsx.amazonaws.com` principale per recuperare il valore segreto.

Risoluzione dei problemi di riduzione del funzionamento degli SSD

Questa sezione descrive i problemi e le risoluzioni comuni relativi alle operazioni di riduzione della capacità degli SSD.

Argomenti

- L'operazione di riduzione dell'SSD è sospesa a causa dell'elevato utilizzo dell'SSD
- L'operazione di riduzione dell'SSD è sospesa a causa di relazioni FlexClone

- Il reindirizzamento dell'accesso client per i volumi non è riuscito durante la riduzione dell'SSD
- L'operazione di riduzione dell'SSD sta impiegando più tempo del previsto

L'operazione di riduzione dell'SSD è sospesa a causa dell'elevato utilizzo dell'SSD

Se il livello di archiviazione SSD supera l'80% di utilizzo durante un'operazione di riduzione, Amazon sospende FSx automaticamente l'operazione. Potresti visualizzare un messaggio di azioni amministrative simile a:

```
Your file system has insufficient free space in aggr_1. Please free up space or
 increase your file system's storage capacity.
```

L'operazione riprenderà quando l'utilizzo sarà inferiore all'80%. Per risolvere questo problema, puoi fare quanto segue:

- Eliminare i dati non necessari dai volumi che sono già stati spostati sui nuovi dischi.
- Inserisci più dati nel pool di capacità modificando le politiche di suddivisione in più livelli dei volumi.
- Invia una richiesta per aumentare la capacità dell'SSD chiamando `update-file-system`con un nuovo valore target.

È necessario aggiornare la capacità di archiviazione SSD del file system in modo che la capacità SSD risultante del file system non superi l'80% di utilizzo dopo l'operazione di riduzione. Per ulteriori dettagli, consultare Aggiornamento dello storage SSD e degli IOPS del file system.

È possibile identificare quali volumi sono stati spostati sui nuovi dischi controllando il `Message` campo nell'azione amministrativa. `STORAGE_OPTIMIZATION`

Puoi anche chiamare `describe-volumes`se l'aggregato è `aggr1` o. `aggr1_old`

L'operazione di riduzione dell'SSD è sospesa a causa di relazioni FlexClone

Se FlexClone i volumi vengono creati dopo l'avvio di un'operazione di riduzione dell'SSD, Amazon FSx sospende l'operazione fino all'eliminazione dei cloni. Questo perché ONTAP divide le relazioni tra i cloni durante lo spostamento dei volumi, il che comporterebbe la duplicazione dello storage sui nuovi dischi. Per risolvere questo problema, è possibile identificare ed eliminare tutti i FlexClone volumi creati dopo l'avvio dell'operazione di riduzione.

Dopo aver eliminato tutti i FlexClone volumi, l'operazione di riduzione riprenderà automaticamente.

Il reindirizzamento dell'accesso client per i volumi non è riuscito durante la riduzione dell'SSD

Durante un'operazione di riduzione degli SSD, Amazon FSx deve reindirizzare l'accesso dei client dai vecchi dischi ai nuovi dischi per ogni volume. Se questo processo non riesce, potresti visualizzare un messaggio di azioni amministrative simile a:

```
Redirecting client access for volume(s) fsvol-123 has failed due to insufficient SSD
 IOPS, throughput capacity, or because the volume is full.
```

Per risolvere questo problema, puoi fare quanto segue:

- Controlla i parametri di utilizzo delle risorse del tuo file system su Amazon CloudWatch per assicurarti che il tuo carico di lavoro non consumi più del 50% delle seguenti risorse:
  - `NetworkThroughputUtilization`
  - `FileServerDiskThroughputUtilization`
  - `FileServerDiskIopsUtilization`
  - `CPUUtilization`
  - `DiskIopsUtilization`
- Se il volume è pieno, aumenta la capacità di archiviazione del volume.
- Riducete il carico di lavoro sul file system durante l'operazione di riduzione.

Dopo aver risolto questi problemi, Amazon FSx riproverà automaticamente a reindirizzare l'accesso del cliente una volta all'ora.

L'operazione di riduzione dell'SSD sta impiegando più tempo del previsto

Il tempo necessario per completare un'operazione di riduzione dell'SSD dipende da diversi fattori, tra cui la quantità di dati archiviati nel file system, l'attività continua del carico di lavoro e le risorse di sistema disponibili. Se l'operazione richiede più tempo del previsto, è possibile effettuare le seguenti operazioni:

- Verificate che il file system disponga di risorse adeguate (meno del 50% di CPU, velocità effettiva del disco e utilizzo degli IOPS SSD).

- Riduci i carichi di lavoro che richiedono molta scrittura durante l'operazione per ridurre al minimo il conflitto di risorse.

È possibile tenere traccia dello stato di avanzamento dell'operazione controllando la `ProgressPercent` proprietà nell'azione amministrativa. `STORAGE_OPTIMIZATION`

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. Come funziona l' SVMs accesso 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 non FSx può connettersi ai controller di dominio Active Directory perché il nome NetBIOS di SVM è già in uso
- Amazon non FSx può accedere alle credenziali del tuo account del servizio Active Directory in Gestione dei segreti AWS
- Amazon non è FSx in grado di comunicare con i tuoi controller di dominio Active Directory
- Amazon non FSx riesce a connettersi al tuo Active Directory a causa dei requisiti di porta o delle autorizzazioni degli account di servizio non soddisfatti
- Amazon non FSx può connettersi ai controller di dominio Active Directory perché le credenziali dell'account di servizio non sono valide
- Amazon non FSx riesce a connettersi ai controller di dominio Active Directory a causa delle credenziali degli account di servizio insufficienti
- Amazon non è in FSx grado di comunicare con i tuoi server DNS o controller di dominio Active Directory
- Amazon non FSx può comunicare con il tuo Active Directory a causa di un nome di dominio Active Directory non valido.
- L'account del servizio non può accedere al gruppo di amministratori specificato nella configurazione SVM Active Directory

- Amazon non FSx 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 non FSx 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 Accesso SVMs ad Active Directory utilizzando l'API e Console di gestione AWS AWS CLI Per riprovare a unire la SVM ad Active Directory. 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 non FSx è in grado di stabilire una connessione al tuo 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 descritto di seguito:

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 Accesso SVMs ad Active Directory utilizzando l'API e Console di gestione AWS AWS CLI per riprovare a unire la SVM alla nuova Active Directory.

Amazon non FSx può connettersi ai controller di dominio Active Directory perché il nome NetBIOS di SVM è già in uso

La creazione di una SVM unita all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon non FSx 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 Accesso SVMs ad Active Directory utilizzando l'API e Console di gestione AWS AWS 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 non FSx può accedere alle credenziali del tuo account del servizio Active Directory in Gestione dei segreti AWS

Le seguenti sezioni descrivono i problemi più comuni e come risolverli.

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
You can't provide both username/password and a domain join service account secret to connect to your Active Directory. Provide only one set of credentials.
```

Per risolvere questo problema

1. Scegli se fornire le credenziali archiviate in un segreto di Secrets Manager o in testo semplice.
2. Quando entri in Active Directory, fornisci solo uno di questi parametri e non entrambi.

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
The domain join service account secret ARN format you entered isn't valid. Use the format: arn:partition:secretsmanager:region:account-id:secret:secret-name-6chars
```

Per risolvere questo problema

1. Verificare Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.
2. Verifica che il formato ARN che stai inserendo sia corretto. Un esempio di formato corretto è`arn:aws:secretsmanager:us-east-1:123456789012:secret:MyDatabaseSecret-Ab3d5f`.

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
Amazon FSx can't access the domain join service account secret [ARN]. Add a resource permission to the secret that grants the FSx service principal (fsx.amazonaws.com) permission to access it.
```

Per risolvere questo problema

1. Verificare Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.
2. Verifica che il segreto di Secrets Manager che stai fornendo abbia le politiche corrette che consentano FSx ad Amazon di utilizzare il segreto.

L'aggiunta di una SVM alla tua Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
You don't have permission to access the domain join service account secret [ARN]. A resource permission needs to be added to the secret to grant you access.
```

Per risolvere questo problema

- Il proprietario o l'amministratore del segreto di Secrets Manager deve consentire l'accesso all'account per utilizzare questo segreto. Per ulteriori informazioni, consulta Politiche basate sull'identità.

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
The domain join service account secret format or content isn't valid. Make
sure the secret includes both CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME
and CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD fields with non-empty
values.
```

Per risolvere questo problema

1. Verificare Archiviazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS.
2. Verifica che il segreto di Secrets Manager che stai fornendo contenga entrambi i campi obbligatori.

Amazon non è FSx in grado di comunicare con i tuoi controller di dominio Active Directory

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon non FSx è in grado di comunicare con il tuo Active Directory. Per risolvere questo problema, assicurati che il traffico di rete sia consentito tra Amazon FSx e i tuoi 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 FSx che Amazon sarà in grado di comunicare con il tuo AD, segui la procedura descritta in Accesso SVMs ad Active Directory utilizzando l'API e Console di gestione AWS AWS CLI e riprova a collegare la SVM all'AD.

Amazon non FSx riesce a connettersi al tuo Active Directory a causa dei requisiti di porta o delle autorizzazioni degli account di servizio non soddisfatti

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon non FSx è in grado di stabilire una connessione con Active Directory. Ciò è dovuto al mancato rispetto dei requisiti di porta per Active Directory oppure all'account di servizio fornito non è consentito 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 archiviazione dopo aver risolto eventuali problemi di autorizzazioni con porte e account di servizio, come consigliato nella guida per FSx l'utente di Amazon.

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 Active Directory utilizzando l'unità organizzativa specificata.
3. Dopo aver apportato modifiche alle autorizzazioni della porta o all'account di servizio, seguite la procedura descritta in Accesso SVMs ad Active Directory utilizzando l'API e Console di gestione AWS AWS CLI e riprovate ad aggiungere la SVM all'AD.

Amazon non FSx può connettersi ai controller di dominio Active Directory perché le credenziali dell'account di servizio non sono valide

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon non FSx è in grado di stabilire una connessione con i tuoi 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 tua macchina virtuale di archiviazione con un account di servizio valido.

Per risolvere questo problema, utilizzare la procedura descritta in Aggiornamento delle configurazioni SVM Active Directory esistenti utilizzando l'API Console di gestione AWS, 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 non FSx riesce a connettersi ai controller di dominio Active Directory a causa delle credenziali degli 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 non FSx è in grado di stabilire una connessione con i tuoi controller di dominio Active Directory. Ciò è dovuto al mancato rispetto dei requisiti di porta per Active Directory oppure all'account di servizio fornito non è consentito 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 non è in FSx grado di comunicare con i tuoi server DNS o controller di dominio Active Directory

L'aggiunta di una SVM all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

Amazon non FSx è in grado di comunicare con il tuo Active Directory. Questo perché Amazon non FSx riesce a raggiungere i server DNS forniti o i controller di dominio per il tuo dominio. Per risolvere questo problema, aggiorna la configurazione Active Directory della macchina virtuale di archiviazione con server DNS validi e una configurazione di rete che consenta il flusso del traffico dalla macchina virtuale di archiviazione 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 ONTAP CLI, stabilisci una sessione SSH sulla porta di gestione del file system Amazon FSx for NetApp ONTAP o SVM 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 di Active Directory della SVM utilizzando gli indirizzi IP corretti per i server DNS di Active Directory.

Amazon non FSx può comunicare con il tuo Active Directory a causa di un nome di dominio Active Directory non valido.

L'aggiunta di una SVM all'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'Active Directory a cui stai tentando di accedere soddisfi tale requisito.
2. Utilizza la procedura descritta in Accesso SVMs ad Active Directory utilizzando l'API e Console di gestione AWS AWS CLI e riprova a unire la SVM a un Active Directory. Assicuratevi di utilizzare il formato corretto per l'FQDN del dominio Active Directory.

L'account del 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 non FSx è in grado di applicare la tua 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 di amministratori di dominio Active Directory.
2. Utilizzate la procedura descritta in Accesso SVMs ad Active Directory utilizzando l'API e Console di gestione AWS AWS CLI e riprovate a unire la SVM a un AD.

Amazon non FSx 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 non FSx 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 la SVM ad Active Directory utilizzando questa procedura con l'unità organizzativa corretta.

Non è possibile eliminare una macchina virtuale o un volume di archiviazione

Ciascun file system FSx for ONTAP può contenere una o più macchine virtuali di storage (SVMs) 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 FSx console Amazon, l'API e la CLI. Puoi eliminare i volumi utilizzando la FSx console Amazon, l'API o la CLI solo se il volume ha i FSx backup Amazon abilitati.

Per proteggere i dati e la configurazione, Amazon FSx impedisce l'eliminazione di volumi SVMs e di dati in determinate circostanze. Se tenti di eliminare una SVM o un volume e la tua richiesta di eliminazione non ha esito positivo, Amazon ti FSx fornisce informazioni nella AWS console, AWS Command Line Interface (AWS CLI) e nell'API sul motivo per cui la risorsa non è stata eliminata. Dopo aver risolto la causa dell'errore di eliminazione, puoi riprovare la richiesta di eliminazione.

Argomenti

Identificazione delle eliminazioni non riuscite

Quando elimini una FSx SVM o un volume Amazon, in genere vedi la transizione dello `Lifecycle` stato della risorsa fino a `DELETING` qualche minuto prima che la risorsa scompaia dalla FSx console Amazon, dalla CLI e dall'API.

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.

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

Il file system Each FSx for ONTAP crea una o più voci della tabella di routing per consentire il failover automatico e il failback tra le zone di disponibilità. Per impostazione predefinita, queste voci della tabella di routing vengono create nella tabella di routing predefinita del VPC. Facoltativamente, puoi specificare una o più tabelle di routing non predefinite in cui creare FSx interfacce ONTAP. Amazon `AmazonFSx` assegna un FSx tag a ogni tabella di routing associata a un file system e, se questo tag viene rimosso, può impedire ad Amazon FSx di eliminare le 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 Supporto.
```

Puoi trovare le tabelle di routing del tuo file system nella FSx console Amazon accedendo alla pagina di riepilogo del file system, nella scheda Rete e sicurezza.

Scegliendo il link alle tabelle di routing accedi alle tabelle di routing. 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 il peer diventi malsano. SVMs Se la SVM non può essere eliminata a causa di una relazione tra pari, viene visualizzato quanto segue: `LifecycleTransitionReason`

Amazon non FSx è in grado di eliminare la macchina virtuale di archiviazione perché fa parte di una relazione peer SVM o di transizione peer. 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. 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. Gestione dei file system con la ONTAP CLI

> **Note**
>
> FSx I backup di Amazon 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. 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

FSx per ONTAP SVMs crea un oggetto computer in Active Directory quando si unisce a 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. 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.

Il volume è in uno stato **MISCONFIGURED**

Esistono diverse cause potenziali per cui un volume ONTAP entra in uno `MISCONFIGURED` stato, descritte nei seguenti argomenti.

Il volume è pieno per oltre il 98%

Il file system contiene attualmente un volume pieno per oltre il 98%. Si consiglia di non superare il 95% di utilizzo del volume su base continuativa. Se non liberi spazio nel volume prima della prossima finestra di manutenzione del file system, Amazon FSx disabiliterà il blocco opportunistico sul volume, interrompendo eventuali «oplock» esistenti. Amazon FSx riattiverà gli oplock sul volume dopo il completamento del processo di patching. Per evitare ciò, riduci l'utilizzo della capacità di archiviazione del volume al di sotto del 98%. Alcuni dei modi per raggiungere questo obiettivo includono:

- Aumento delle dimensioni del volume.
- Eliminazione di dati non necessari.
- Eliminazione di istantanee non necessarie.

Per ulteriori informazioni, consultare Aggiornamento della capacità di archiviazione e Eliminazione di snapshot.

Il volume offline ha un LUN iSCSI o uno spazio dei nomi NVMe/TCP

Il file system ospita attualmente un volume che si trova in uno stato offline e tale volume contiene un LUN iSCSI, uno NVMe/TCP spazio dei nomi o entrambi. Si consiglia di mantenere i volumi online su base continuativa. Se non metti online questo volume prima della prossima finestra di manutenzione del file system, Amazon FSx lo metterà temporaneamente online per tutta la durata dell'operazione di patching. Per evitare che ciò accada, accedi online o elimina il volume.

Per riportare online un volume offline, utilizzate il comando `volume online`ONTAPCLI, come illustrato nell'esempio seguente. Se esiste solo un SVM (Vserver), non è necessario specificare il parametro. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

Il volume offline è un'origine FlexCache

Il file system contiene un volume di FlexCache origine che si trova in uno stato offline. Si consiglia di mantenere i volumi online su base continuativa. Se non metti online questo volume prima della prossima finestra di manutenzione del file system, Amazon FSx lo metterà temporaneamente online per tutta la durata dell'operazione di patching. Durante questo periodo, è possibile che i dati vengano riscritti nel volume di FlexCache origine con i dati del volume di cache. Per evitare che ciò accada, accedi online o elimina il volume.

Per riportare online un volume offline, utilizzate il comando `volume online`ONTAPCLI, come illustrato nell'esempio seguente. Se esiste solo un SVM (Vserver), non è necessario specificare il parametro. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

Il volume offline fa parte di una relazione SnapMirror

Il file system ospita attualmente un volume che si trova in uno stato offline e tale volume è un'SnapMirrororigine o una destinazione. Si consiglia di mantenere i volumi online su base continuativa. Se non metti online questo volume prima della prossima finestra di manutenzione del file system, Amazon lo FSx metterà temporaneamente online per tutta la durata dell'operazione di applicazione delle patch e metterà in pausa la SnapMirror relazione. Durante questo periodo, è possibile che i dati vengano scritti nel volume di SnapMirror destinazione con i dati del volume di SnapMirror origine. Per evitare che ciò accada, accedi online o elimina il volume.

Per riportare online un volume offline, utilizzate il comando `volume online`ONTAPCLI, come illustrato nell'esempio seguente. Se esiste solo un SVM (Vserver), non è necessario specificare il parametro. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

Il volume con restrizioni contiene un LUN iSCSI o uno spazio dei nomi NVMe/TCP

Il file system ospita attualmente un volume con restrizioni e tale volume contiene un LUN iSCSI, uno NVMe/TCP spazio dei nomi o entrambi. Si consiglia di mantenere i volumi online su base continuativa. Se non disponi online di questo volume prima della prossima finestra di manutenzione del file system, Amazon FSx lo metterà temporaneamente online per tutta la durata dell'operazione di patching. Per evitare che ciò accada, accedi online o elimina il volume.

Per riportare online un volume offline, utilizzate il comando `volume online`ONTAPCLI, come illustrato nell'esempio seguente. Se esiste solo un SVM (Vserver), non è necessario specificare il parametro. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

Il volume limitato è un'origine FlexCache

Il file system contiene un volume di FlexCache origine con restrizioni. Si consiglia di mantenere i volumi online su base continuativa. Se non disponi online di questo volume prima della prossima

finestra di manutenzione del file system, Amazon FSx lo metterà temporaneamente online per tutta la durata dell'operazione di patching. Durante questo periodo, è possibile che i dati vengano riscritti nel volume di FlexCache origine con i dati del volume di cache. Per evitare che ciò accada, accedi online o elimina il volume.

Per riportare online un volume offline, utilizzate il comando `volume online`ONTAPCLI, come illustrato nell'esempio seguente. Se esiste solo un SVM (Vserver), non è necessario specificare il parametro. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

Il volume limitato fa parte di una relazione SnapMirror

Il file system ospita attualmente un volume con restrizioni e tale volume è un'SnapMirrororigine o una destinazione. Si consiglia di mantenere i volumi online su base continuativa. Se non metti online questo volume prima della prossima finestra di manutenzione del file system, Amazon lo FSx metterà temporaneamente online per tutta la durata dell'operazione di applicazione delle patch e metterà in pausa la SnapMirror relazione. Durante questo periodo, è possibile che i dati vengano scritti nel volume di SnapMirror destinazione con i dati del volume di SnapMirror origine. Per evitare che ciò accada, accedi online o elimina il volume.

Per riportare online un volume offline, utilizzate il comando `volume online`ONTAPCLI, come illustrato nell'esempio seguente. Se esiste solo un SVM (Vserver), non è necessario specificare il parametro. `-vserver`

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

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

La capacità di archiviazione del volume è insufficiente

Se lo spazio sui volumi si sta esaurendo, è possibile utilizzare le procedure illustrate di seguito 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 FSx console Amazon e AWS CLI l' FSx API Amazon. Per ulteriori informazioni sull'aggiornamento di un volume con una capacità maggiore, consultaAggiornamento dei volumi.

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 FSx per ONTAP, utilizzando il comando `volume autosize` NetApp ONTAP CLI. Per ulteriori informazioni, consulta Abilitazione del dimensionamento automatico.

Lo storage principale del file system è pieno

Se lo storage principale del file system FSx for ONTAP è pieno, non puoi aggiungere altri dati ai volumi del file system, anche se un volume dimostra di avere una capacità di archiviazione

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 FSx console Amazon. Per ulteriori informazioni, consulta 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.

Quando si elimina un'istantanea, non si recupera una quantità di spazio di archiviazione pari alla dimensione dell'istantanea che si sta eliminando. È possibile visualizzare la quantità di storage che è possibile recuperare quando si elimina un'istantanea utilizzando il comando CLI volume snapshot compute-reclaimable -vserver, utilizzando i ONTAP dati per sostituire e. *svm_name vol_name snapshot_name*

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

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 del 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. Monitoraggio 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).

I backup non riescono a causa di una capacità di volume insufficiente

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

Recupero dei volumi FSx eliminati per ONTAP

Quando un volume FSx for ONTAP viene eliminato, viene inserito nella coda di ONTAP's ripristino. Sebbene sia possibile ripristinare un volume direttamente da questa coda utilizzando la ONTAP

CLI, il volume recuperato non riapparirà nella AWS console o nell'API FSx Amazon e AWS tutti i tag precedentemente applicati al volume andranno persi definitivamente. Per ripristinare correttamente un volume FSx for ONTAP preservando al contempo AWS l'integrazione e le politiche di sicurezza basate su tag, puoi ripristinare un backup su un nuovo volume o replicare i dati del volume su un nuovo volume utilizzando. SnapMirror Per ulteriori informazioni sulla coda di ONTAP's ripristino, consulta la documentazione. NetApp's

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 CLI: NetApp ONTAP

- 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 ONTAP CLI del tuo file system, segui i passaggi documentati nella sezione della Guida per Utilizzo della CLI NetApp ONTAP l'utente di FSx Amazon NetApp for ONTAP.

   ```
   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:

   - Sostituisci *node_name* con il nome del nodo (ad esempio,`FsxId01234567890abcdef-01`).
   - Sostituire *svm_name* con il nome della macchina virtuale di archiviazione (ad esempio,`fsx`).
   - Sostituire *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'`e0e`interfaccia e nello spazio `Default` IP. In FSx ONTAP, tutto il traffico di rete utilizza l'`e0e`interfaccia.

Quando usi il tracciamento dei pacchetti, tieni 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: _ _ .trc *node-name port-name yyyymmdd_hhmmss*
- 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. Torna 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, vedi Come usare il debug di rete dump in ONTAP 9.10+ nel. NetApp Knowledge Base

Risoluzione degli I/O errori e degli errori di recupero del blocco NFS

Questa sezione descrive i problemi relativi agli I/O errori e agli errori di recupero del blocco NFS durante gli eventi di failover sui file system ONTAP e le risoluzioni FSx per ciascuno di essi.

Si verificano errori durante gli eventi di failover I/O

Durante i failover sui FSx file system ONTAP Single-AZ, i client NFS possono riscontrare errori transitori o pause prolungate. I/O Per i client NFSv4 +, è possibile che vengano visualizzati messaggi di log del kernel come:

```
NFS: __nfs4_reclaim_open_state: Lock reclaim failed!
```

Questi messaggi indicano che il client non è riuscito a recuperare con successo i blocchi NFS durante la finestra di failover.

Per ridurre gli errori durante gli eventi di failover I/O

Su Linux, è possibile configurare le impostazioni di rete sui client per ridurre il tempo di rilevamento del failover da 55-60 secondi a 15-20 secondi.

> **Important**
>
> Verifica sempre prima queste configurazioni in un ambiente non di produzione. Queste impostazioni aumentano il traffico ARP (Address Resolution Protocol), che viene utilizzato per mappare gli indirizzi IP su indirizzi fisici (MAC) su una rete locale e potrebbe non essere adatto per ambienti con vincoli di rete.

Per configurare impostazioni di rete ottimizzate per i client NFS

1. Crea un file di configurazione sysctl su ogni client NFS. L'esempio seguente utilizza `default` per applicare le impostazioni a tutte le interfacce di rete. Se l'istanza dispone di più interfacce di rete, è possibile sostituirla `default` con il nome dell'interfaccia specifica (ad esempio, `eth0` `oens5`) utilizzato per connettersi al file system FSx for ONTAP Single-AZ:

```
$ sudo tee /etc/sysctl.d/99-fsx-failover.conf > /dev/null << 'EOF'
# NFS client optimizations for faster failover detection
# Replace 'default' with your interface name (e.g., eth0, ens5) to target a
 specific interface
net.ipv4.neigh.default.base_reachable_time_ms=5000
net.ipv4.neigh.default.delay_first_probe_time=1
net.ipv4.neigh.default.ucast_solicit=0
net.ipv4.tcp_syn_retries=3
EOF
```

2. Applica immediatamente le impostazioni:

```
$ sudo sysctl -p /etc/sysctl.d/99-fsx-failover.conf
```

3. Verifica che la configurazione sia attiva. Se lo hai usato`default`, puoi verificare con i seguenti comandi. Se hai specificato un'interfaccia specifica, `default` sostituiscila con il nome dell'interfaccia (ad esempio, `eth0` `oens5`):

```
$ sysctl net.ipv4.neigh.default.base_reachable_time_ms
$ sysctl net.ipv4.neigh.default.delay_first_probe_time
$ sysctl net.ipv4.neigh.default.ucast_solicit
$ sysctl net.ipv4.tcp_syn_retries
```

Assicurati che queste impostazioni vengano applicate in modo uniforme su tutti i client NFS che si connettono al file system FSx for ONTAP all'interno della stessa zona di disponibilità. Quando utilizzi queste ottimizzazioni di rete, tieni presente quanto segue:

- base_reachable_time_ms=5000 — Riduce la validità di accesso alla cache ARP da 30 secondi a 5 secondi, consentendo ai client di rilevare più rapidamente le modifiche alla proprietà IP durante un evento di failover.
- delay_first_probe_time=1 — Riduce il ritardo prima di esaminare una voce di rete obsoleta da 5 secondi a 1 secondo.

- ucast_solicit=0 — Ignora i probe unicast neighbor e invia immediatamente richieste ARP broadcast, accelerando la riscoperta del file server attivo.
- tcp_syn_retries=3 — Riduce la durata dei tentativi di connessione TCP da 127 secondi a 15 secondi.

Dopo aver impostato le impostazioni di rete, è necessario monitorare l'ambiente per convalidare le modifiche. È possibile testare un evento di failover modificando la capacità di throughput del file system. Per ulteriori informazioni, consulta Test del failover su un file system.

Monitoraggio dell'ambiente dopo l'applicazione delle modifiche

- Monitora i log di sistema alla ricerca di errori NFS per visualizzare i messaggi di log del kernel relativi a NFS.

```
$ sudo journalctl -f | grep -i nfs
```

  Verificate che vi siano meno ricorrenze di messaggi come. `Lock reclaim failed`
- Monitora i registri delle applicazioni per confermare un minor numero di I/O timeout, errori di connessione ed errori correlati ai tentativi durante gli eventi di failover.
- Convalida l'impatto sulla rete per garantire che l'aumento del traffico ARP non influisca negativamente sulle prestazioni di rete nell'ambiente in uso.

Approcci alternativi per gli ambienti NFSv4

In NFSv4 ambienti in cui non è possibile modificare la configurazione lato client, considerate le seguenti alternative:

- NFSv4 Estendere i timeout del leasing. Collabora con il tuo amministratore di storage per aumentare i timeout di leasing NFSv4 . L'estensione di questi timeout offre ai clienti più tempo per recuperare i blocchi durante gli eventi di failover. Per ulteriori informazioni, vedete Specificare il periodo di tolleranza del NFSv4 blocco nella documentazione. NetApp ONTAP

Cronologia dei documenti per Amazon FSx for NetApp ONTAP

- Versione API: 2018-03-01
- Ultimo aggiornamento della documentazione: 16 ottobre 2025

La tabella seguente descrive le modifiche importanti alla Amazon FSx NetApp ONTAP User Guide. Per ricevere notifiche sugli aggiornamenti della documentazione, è possibile sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Supporto aggiunto per i punti di accesso Amazon S3 per Amazon FSx for ONTAP NetApp	I punti di accesso Amazon S3 FSx per Amazon for NetApp ONTAP offrono un nuovo modo di accedere ai dati archiviati nei FSx file system ONTAP utilizzando l'API Amazon S3. Con i punti di accesso Amazon S3, puoi semplificare l'accesso ai dati per le applicazioni abilitate ad Amazon S3 senza richiedere modifiche alla configurazione del file system esistente. Per ulteriori informazioni, consulta Usare i punti di accesso Amazon S3 FSx per Amazon for NetApp ONTAP.	2 dicembre 2025
Support aggiunto per Gestione dei segreti AWS l'integrazione	Amazon FSx ora si integra con Gestione dei segreti AWS per una gestione avanzata delle credenziali di Active Directory . Per ulteriori informazioni,	5 novembre 2025

	consulta Memorizzazione delle credenziali di Active Directory utilizzando. Gestione dei segreti AWS	
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione che consente ai responsabili di elencare i segreti Gestione dei segreti AWS per la selezione delle credenziali dell'account del servizio di accesso al dominio. `secretsmanager:ListSecrets` Per ulteriori informazioni, consulta la policy AWS gestita: Amazon FSx FullAccess.	5 novembre 2025
NetApp BlueXPrinominato in NetApp Console	NetApp BlueXPè ora noto comeNetApp Console. Per ulteriori informazioni, vedere Utilizzo NetApp della console.	16 ottobre 2025
Support aggiunto per Internet Protocol versione 6 (IPv6)	FSx per i file system ONTAP ora supportano due opzioni di tipo di rete: IPv4 -only e dual-stack (per entrambi e). IPv4 IPv6 È necessario specificare una di queste opzioni durante la creazione del file system. È possibile modificare il tipo di rete di un file system FSx for ONTAP esistente in qualsiasi momento. Per ulteriori informazioni, vedere Gestione del tipo di rete.	30 settembre 2025

Regione AWS Supporto aggiuntivo aggiunto	I file system di seconda generazione (Multi-AZ 2 e Single-AZ 2) FSx per ONTAP sono ora disponibili in Asia Pacifico (Seoul), Canada (Centrale), Europa (Spagna) ed Europa (Zurigo). Per ulteriori informazioni, vedere Disponibilità di. Regione AWS	30 settembre 2025
Regione AWS Supporto aggiuntivo aggiunto	FSx i file system for ONTAP sono ora disponibili nella regione Asia Pacifico (Taipei). Per ulteriori informazioni, vedere Disponibilità entro. Regione AWS	18 agosto 2025
Support aggiunto per ridurre la capacità di archiviazione SSD	FSx for ONTAP ora consente di ridurre la capacità di archiviazione delle unità a stato solido (SSD) del file system sui file system di seconda generazione, ottimizzando i costi di archiviazione per carichi di lavoro con diverse esigenze di archiviazione ad alte prestazioni. Per ulteriori informazioni, consulta Quando ridurre la capacità di archiviazione SSD.	14 agosto 2025

Amazon FSx ha aggiornato la politica FSx ServiceRolePolicy AWS gestita da Amazon	Amazon FSx ha aggiunto le `ec2:UnassignIpv6Addresses` autorizzazioni `ec2:AssignIpv6Addresses` e ad Amazon FSxServiceRolePolicy. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	22 luglio 2025
Amazon FSx ha aggiornato la politica FSx FullAccess AWS gestita da Amazon	La policy FSx FullAccess gestita da Amazon è stata aggiornata per aggiungere le `fsx:DetachAndDeleteS3AccessPoint` autorizzazioni `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , e.	25 giugno 2025
Amazon FSx ha aggiornato la politica FSx ConsoleFullAccess AWS gestita da Amazon	La policy FSx ConsoleFullAccess gestita da Amazon è stata aggiornata per aggiungere le `fsx:DetachAndDeleteS3AccessPoint` autorizzazioni `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , e.	25 giugno 2025

FSx per ONTAP supporta Amazon Elastic Service VMware	FSx for ONTAP ora può essere utilizzato come datastore esterno per Amazon EVS. Per ulteriori informazioni, consulta Using Amazon Elastic VMware Service with FSx for ONTAP.	9 giugno 2025
Regione AWS Supporto aggiuntivo aggiunto	I file system di seconda generazione (Multi-AZ 2 e Single-AZ 2) FSx per ONTAP sono ora disponibili in Asia Pacifico (Tokyo) e Asia Pacifico (Mumbai). Per ulteriori informazioni, vedere Disponibilità di. Regione AWS	2 giugno 2025
Support aggiunto per la modalità FlexCache write-back	FSx per i volumi ONTAP ora supportano FlexCache la modalità write-back. Per ulteriori informazioni, consulta Replicazione dei dati con. FlexCache	28 maggio 2025
Regione AWS Supporto aggiuntivo aggiunto	FSx i file system for ONTAP sono ora disponibili in Asia Pacifico (Tailandia) e Messico (Centrale). Per ulteriori informazioni, vedere Disponibilità entro Regione AWS.	8 maggio 2025

La protezione antiransomware autonoma (ARP) è ora supportata	ARP, una funzionalità NetApp basata sull'intelligenza artificiale che monitora e protegge dagli attacchi di ransomware e malware, è ora supportata da for ONTAP. FSx Per ulteriori informazioni, consulta Protezione dei dati con Autonomous Ransomware Protection	7 aprile 2025
Un nuovo argomento nella Guida FSx per l'utente di for ONTAP descrive come configurare un server SMB in un gruppo di lavoro	La configurazione di un server SMB in un gruppo di lavoro descrive come configurare un server SMB in un gruppo di lavoro su una SVM in alternativa all'aggiunta di una SVM a Microsoft Active Directory.	4 marzo 2025
Amazon FSx ha aggiornato la politica FSx ConsoleReadOnlyAccess AWS gestita da Amazon	Amazon FSx ha aggiornato la FSx ConsoleReadOnlyAccess politica di Amazon per aggiungere l'`ec2:DescribeNetworkInterfaces` autorizzazione. Per ulteriori informazioni, consulta la FSx ConsoleReadOnlyAccess politica di Amazon.	25 febbraio 2025

Ora sono supportate Harvest dashboard aggiuntive	Le Harvest dashboard aggiuntive sono ora supportate da FSx for ONTAP, incluse le dashboard che non sono abilitate per impostazione predefinita. È stato aggiunto anche un elenco di dashboard che FSx per ONTAP non sono supportati. Per ulteriori informazioni, consulta Monitoraggio dei FSx file system ONTAP con Harvest e Grafana.	18 febbraio 2025
Nuovo argomento relativo FSx alla fatturazione e ai report sull'utilizzo di ONTAP aggiunto alla FSx Guida per l'utente di ONTAP	L'argomento sui rapporti di AWS fatturazione e utilizzo per FSx for ONTAP spiega come accedere alla fatturazione e ai report di utilizzo FSx per i file system ONTAP nella console. Gestione dei costi e fatturazione AWS Fornisce inoltre tutti i tipi di utilizzo in entrambi i report specifici per ONTAP. FSx	13 febbraio 2025
Support aggiunto per gli endpoint di interfaccia VPC dual-stack per Amazon FSx	Ora puoi creare endpoint di interfaccia VPC dual-stack per FSx Amazon con indirizzi IP IPv4 IPv6 e nomi DNS. Per ulteriori informazioni, consulta ONTAP e FSx gli endpoint VPC di interfaccia.	7 febbraio 2025

Support aggiunto per endpoint API dual-stack	L'API del FSx servizio Amazon per la creazione e la gestione dei file system dispone di nuovi endpoint dual-stack. Per ulteriori informazioni, consulta gli endpoint delle API nell'Amazon FSx API Reference.	7 febbraio 2025
Amazon FSx ha aggiornato la politica FSx ConsoleFullAccess AWS gestita da Amazon	Amazon FSx ha aggiornato la FSx ConsoleFullAccess politica di Amazon per aggiungere l'`ec2:DescribeNetworkInterfaces` autorizzazione. Per ulteriori informazioni, consulta la FSx ConsoleFullAccess politica di Amazon.	7 febbraio 2025
Pubblicato un nuovo argomento, Replicazione dei dati con FlexCache	È stato pubblicato un nuovo argomento che descrive come replicare i dati in un file system ONTAP locale su un file system FSx for ONTAP utilizzato. FlexCache Per ulteriori informazioni, consulta Replicazione dei dati con. FlexCache	19 dicembre 2024

Support aggiunto per i file system di seconda generazione	È ora possibile creare file system Single-AZ e Multi-AZ di seconda generazione. Una singola coppia ad alta disponibilità (HA) ora offre fino al 6% di capacità GBps di throughput e 200.000 IOPS SSD. Per ulteriori informazioni, consulta Coppie ad alta disponibilità (HA).	9 luglio 2024
Support aggiunto per la lettura dei dati da un volume durante il ripristino da un backup	È ora possibile montare un volume con accesso in sola lettura ai dati del file durante il ripristino da un backup su file system di seconda generazione. Per ulteriori informazioni, vedere Ripristino dei backup su un nuovo volume.	9 luglio 2024
Support aggiunto per la regolazione della capacità di throughput sui file system di seconda generazione	È ora possibile regolare la capacità di throughput dei file system di seconda generazione dopo la creazione. Per ulteriori informazioni, vedere Gestione della capacità di throughput.	9 luglio 2024

Support aggiunto per l'aggiunta di coppie HA ai file system Single-AZ di seconda generazione	È ora possibile aggiungere coppie HA ai file system Single-AZ di seconda generazione dopo la creazione. È possibile avere un totale di 12 coppie HA su un file system Single-AZ di seconda generazione. Per ulteriori informazioni, vedere Aggiungere coppie ad alta disponibilità (HA).	9 luglio 2024
Support aggiunto per Non-Volatile Memory Express su protocollo TCP (/TCP) NVMe	Ora puoi utilizzare il NVMe/TCP protocollo per il trasporto dei dati su Amazon FSx per i file system NetApp ONTAP. Per ulteriori informazioni, consulta Usare i protocolli di storage a blocchi	9 luglio 2024
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, vedere Configurazione dell'autenticazione Active Directory per gli utenti. ONTAP	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 nei file system con scalabilità orizzontale. I file system con 12 coppie HA possono fornire fino al 72% di capacità GBps di throughput e 2.400.000 IOPS SSD in 12 coppie ad alta disponibilità (HA). Per ulteriori informazioni, consulta le coppie ad alta disponibilità (HA) e le prestazioni di Amazon FSx for NetApp 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 Attivazione della modalità di scrittura su cloud su un volume.	6 febbraio 2024

Support aggiunto per il backup FlexGroup dei volumi con AWS Backup	Ora puoi utilizzarlo AWS Backup per eseguire il backup e il ripristino FlexGroup dei volumi sui file system FSx for ONTAP. Per ulteriori informazioni, consulta Utilizzo AWS Backup con Amazon FSx.	11 gennaio 2024
Amazon FSx ha aggiornato le politiche FSx ServiceRolePolicy AWS gestite di Amazon FSx FullAccess FSx ConsoleFullAccess FSx ReadOnlyAccess FSxConsoleReadOnlyAccess, Amazon, Amazon e Amazon	Amazon FSx ha aggiornato le FSx ServiceRolePolicy politiche di Amazon FSx FullAccess FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon e Amazon per aggiungere l'`ec2:GetSecurityGroupsForVpc` autorizzazione. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	9 gennaio 2024
Amazon FSx ha aggiornato Amazon FSx FullAccess e le politiche FSx ConsoleFullAccess AWS gestite da Amazon	Amazon FSx ha aggiornato le FSx ConsoleFullAccess politiche di Amazon FSx FullAccess e Amazon per aggiungere l'`ManageCrossAccountDataReplication` azione. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	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 i parametri 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 i file system con scalabilità orizzontale in grado di fornire fino al 36% di capacità GBps di throughput e 1.200.000 IOPS SSD su sei coppie ad alta disponibilità (HA). Per ulteriori informazioni, consulta le coppie ad alta disponibilità (HA) e le prestazioni di Amazon FSx for NetApp ONTAP.	26 novembre 2023
Support aggiunto per i FlexGroup volumi	Amazon FSx for NetApp ONTAP ha aggiunto il supporto per i FlexGroup volumi. 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 proprietari possono gestire questa funzionalità nella FSx console Amazon, nella CLI e nell'API. Per ulteriori informazioni, consulta Creazione di file system FSx for ONTAP in sottoreti condivise	26 novembre 2023
Amazon FSx ha aggiornato Amazon FSx FullAccess e le politiche FSx ConsoleFullAccess AWS gestite da Amazon	Amazon FSx ha aggiornato le FSx ConsoleFullAccess politiche di Amazon FSx FullAccess e Amazon per aggiungere l'`fsx:CopySnapshotAndUpdateVolume` autorizzazione. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	26 novembre 2023
Amazon FSx ha aggiornato Amazon FSx FullAccess e le politiche FSx ConsoleFullAccess AWS gestite da Amazon	Amazon FSx ha aggiornato le FSx ConsoleFullAccess politiche di Amazon FSx FullAccess e Amazon per aggiungere le `fsx:UpdateSharedVPCConfiguration` autorizzazioni `fsx:DescribeSharedVPCConfiguration` e. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	14 novembre 2023

Support aggiunto per 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 ora offre metriche prestazionali aggiuntive e una dashboard di monitoraggio avanzata per una migliore visibilità dell'attività del file system. Per ulteriori informazioni, consulta Monitoraggio con. CloudWatch	17 agosto 2023
Amazon FSx ha aggiornato la politica FSx ServiceRolePolicy AWS gestita da Amazon	Amazon FSx ha aggiornato l'`cloudwatch:PutMetricData` autorizzazione in Amazon FSxServiceRolePolicy. Per ulteriori informazioni, consulta Amazon FSx updates to AWS managed policy.	24 luglio 2023
Support aggiunto per l'utilizzo diretto NetApp di System Manager	Puoi gestire i tuoi file system FSx for ONTAP utilizzando System Manager direttamente daNetApp BlueXP. Per ulteriori informazioni, vedere Utilizzo di NetApp System Manager con BlueXP.	13 luglio 2023

Support aggiunto per il monitoraggio degli eventi EMS	Puoi monitorare FSx gli eventi del file system ONTAP utilizzando la versione nativa di NetApp ONTAP. Events Management System (EMS) È possibile visualizzare gli eventi EMS utilizzando la CLI di NetApp ONTAP. Per ulteriori informazioni, consulta Monitoraggio degli eventi FSx ONTAP EMS.	13 luglio 2023
Support aggiunto per SnapLock	FSx for ONTAP ora supporta i SnapLock volumi. 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 ed Enterprise con. SnapLock Per ulteriori informazioni, consulta Lavorare con SnapLock.	13 luglio 2023

Support aggiunto per la IPsec crittografia dei dati in transito	FSx per ONTAP ora supporta l'utilizzo della IPsec crittografia per crittografare i dati in transito tra file system e client connessi. Per ulteriori informazioni, vedere Configurazione tramite autenticazione PSK e Configurazione IPsec IPsec tramite autenticazione certificata.	13 luglio 2023
La dimensione massima del volume è aumentata	FSx for ONTAP ha aggiornato la dimensione massima di un volume da 100 TB a 300 TB. Per ulteriori informazioni, consulta Attivare il dimensionamento automatico dei volumi.	13 luglio 2023
Amazon FSx ha aggiornato la politica FSx FullAccess AWS gestita da Amazon	Amazon FSx ha aggiornato la FSx FullAccess politica di Amazon per rimuovere l'`fsx:*`autorizzazione e aggiungere `fsx` azioni specifiche. Per ulteriori informazioni, consulta la FSx FullAccess policy di Amazon.	13 luglio 2023
Amazon FSx ha aggiornato la politica FSx ConsoleFullAccess AWS gestita da Amazon	Amazon FSx ha aggiornato la FSx ConsoleFullAccess politica di Amazon per rimuovere l'`fsx:*`autorizzazione e aggiungere `fsx` azioni specifiche. Per ulteriori informazioni, consulta la FSx ConsoleFullAccess policy di Amazon.	13 luglio 2023

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 Console di gestione AWS l'API AWS CLI e. Per ulteriori informazioni, vedere Aggiungere una SVM a un Active Directory.	13 giugno 2023
Support per la cache di NVMe lettura aggiunto per i file system Single-AZ	NVMe la cache di lettura è ora supportata per i file system Single-AZ creati dopo il 28 novembre 2022 con almeno il 2% della capacità GBps 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, consulta Creazione per i file system ONTAP FSx .	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 for ONTAP esistente. FSx 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 FSx console Amazon AWS CLI o l'API 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' FSx API AWS CLI o Amazon 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 quando crei o aggiorni un volume utilizzando la FSx console Amazon o AWS CLI l' FSx API Amazon. 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 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 trasmissione sulle prestazioni.	28 novembre 2022

Support aggiunto FSx per l'utilizzo di ONTAP come datastore esterno per Cloud on VMware AWS	Puoi utilizzare ONTAP come datastore esterno FSx per VMware Cloud on AWS Software-Defined Data Center (). SDDCs Questo supporto aggiuntivo offre la flessibilità necessaria per aumentare o ridurre lo storage indipende ntemente dalle risorse di elaborazione per il cloud sui carichi di lavoro. VMware AWS Per ulteriori informazioni, consulta Using VMware Cloud with FSx for ONTAP.	30 agosto 2022
Aumenta automaticamente la capacità di archiviazione di un file system	Utilizza un CloudFormation modello personalizzabile AWS sviluppato per aumentare automaticamente la capacità di archiviazione del file system quando la quantità di capacità di archiviazione SSD utilizzat a supera una soglia specifica ta. Per ulteriori informazi oni, 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 FSx file system oltre a utilizzare i FSx backup nativi di Amazon. Per ulteriori informazioni, consulta Utilizzo AWS Backup con Amazon FSx.	18 maggio 2022

Support aggiunto per le implementazioni di file system ONTAP in una singola zona di disponibilità	È possibile creare file system Single-AZ FSx for 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' FSx API Amazon dal tuo VPC senza inviare traffico su Internet. Per ulteriori informazioni, consulta Amazon FSx e interfaccia gli endpoint VPC.	5 aprile 2022
Support aggiunto per la modifica della capacità di throughput per i file system ONTAP esistenti	È ora possibile modificare 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 assegnare IOPS per i file system esistenti FSx for ONTAP man mano che i requisiti di storage e IOPS evolvono. Per ulteriori informazioni, consulta 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 di ONTAP in metriche leggibili quasi in tempo reale. FSx 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 128 MBps e 256 MBps opzioni per la velocità effettiva del file system. Per ulteriori informazioni, vedere 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 APIs i NetApp file system familiari 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.