aws

Guida per l'utente di Windows

Amazon FSx per Windows File Server

Amazon FSx per Windows File Server: Guida per l'utente di Windows

Table of Contents

Che cos'è FSx for Windows File Server?

Amazon FSx per Windows File Server fornisce server di file di Microsoft Windows completamente gestiti, supportati da un file system di Windows completamente nativo. FSx for Windows File Server offre le caratteristiche, le prestazioni e la compatibilità per trasferire e spostare facilmente le applicazioni aziendali verso. Cloud AWS

Amazon FSx supporta un'ampia gamma di carichi di lavoro Windows aziendali con archiviazione file completamente gestita basata su Microsoft Windows Server. Amazon FSx dispone del supporto nativo per le funzionalità del file system Windows e per il protocollo SMB (Server Message Block) standard del settore per accedere all'archiviazione dei file in rete. Amazon FSx è ottimizzato per le applicazioni aziendali in Cloud AWS, con compatibilità nativa di Windows, prestazioni e funzionalità aziendali e latenze costanti inferiori al millisecondo.

Grazie all'archiviazione di file su Amazon FSx, il codice, le applicazioni e gli strumenti oggi impiegati da sviluppatori e amministratori Windows possono continuare a funzionare senza alcun cambiamento. Le applicazioni e i carichi di lavoro Windows ideali per Amazon FSx includono applicazioni aziendali, home directory, web serving, gestione dei contenuti, analisi dei dati, configurazioni di build software e carichi di lavoro di elaborazione multimediale.

Come servizio completamente gestito, FSx for Windows File Server elimina il sovraccarico di attività amministrative di configurazione e provisioning di file server e volumi di archiviazione. Inoltre, Amazon FSx mantiene aggiornato il software Windows, rileva e risolve i guasti hardware ed esegue i backup. Fornisce inoltre una ricca integrazione con altri AWS servizi come AWS IAM AWS Directory Service for Microsoft Active Directory WorkSpacesAWS Key Management Service, Amazon e AWS CloudTrail.

Risorse FSx for Windows File Server: file system, backup e condivisioni di file

Le risorse principali di Amazon FSx sono file system e backup. Un file system è il luogo in cui archivi e accedi a file e cartelle. Un file system è costituito da uno o più file server e volumi di archiviazione Windows. Quando si crea un file system, si specifica una quantità di capacità di archiviazione (in GiB), IOPS SSD e capacità di throughput (in MB/s). È possibile modificare queste proprietà in base alle diverse esigenze dopo la creazione del file system. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione, Gestione degli IOPS SSD e Gestione della capacità di throughput.

I backup di FSx for Windows File Server file-system-consistent sono altamente durevoli e incrementali. Per garantire la coerenza del file system, Amazon FSx utilizza il Volume Shadow Copy Service (VSS) in Microsoft Windows. I backup giornalieri automatici sono attivati per impostazione predefinita quando crei un file system e puoi anche eseguire backup manuali aggiuntivi in qualsiasi momento. Per ulteriori informazioni, consulta Utilizzo dei backup.

Una condivisione di file Windows è una cartella specifica (e le relative sottocartelle) all'interno del file system che rendi accessibile alle istanze di calcolo con SMB. Il file system è già dotato di una condivisione di file Windows predefinita denominata. `\share` È possibile creare e gestire tutte le altre condivisioni di file Windows desiderate utilizzando lo strumento di interfaccia grafica utente (GUI) delle cartelle condivise su Windows. Per ulteriori informazioni, consulta Utilizzo delle condivisioni di file di Microsoft Windows.

È possibile accedere alle condivisioni di file utilizzando il nome DNS del file system o gli alias DNS associati al file system. Per ulteriori informazioni, consulta Gestione degli alias DNS.

Accesso alle condivisioni di file

Amazon FSx è accessibile da istanze di calcolo con il protocollo SMB (supporta le versioni da 2.0 a 3.1.1). Puoi accedere alle tue condivisioni da tutte le versioni di Windows a partire da Windows Server 2008 e Windows 7, e anche dalle versioni correnti di Linux. Puoi mappare le tue condivisioni di file Amazon FSx su istanze Amazon Elastic Compute Cloud (Amazon EC2) e su istanze, istanze Amazon 2.0 e VMware Cloud on WorkSpaces VM. AppStream AWS

Puoi accedere alle tue condivisioni di file da istanze di calcolo locali utilizzando o. AWS Direct Connect AWS VPN Oltre ad accedere alle condivisioni di file che si trovano nello stesso VPC, AWS account e AWS regione del file system, puoi anche accedere alle tue condivisioni su istanze di calcolo che si trovano in un altro Amazon VPC, account o regione. Puoi farlo utilizzando il peering VPC o i gateway di transito. Per ulteriori informazioni, consulta Metodi di accesso supportati.

Sicurezza e protezione dei dati

Amazon FSx offre diversi livelli di sicurezza e conformità per garantire la protezione dei dati. Crittografa automaticamente i dati inattivi (sia per i file system che per i backup) utilizzando le chiavi gestite in AWS Key Management Service ().AWS KMS I dati in transito vengono inoltre crittografati automaticamente utilizzando le chiavi di sessione Kerberos SMB. È stato valutato conforme alle certificazioni ISO, PCI-DSS e SOC ed è idoneo all'HIPAA.

Amazon FSx fornisce il controllo degli accessi a livello di file e cartella con gli elenchi di controllo degli accessi (ACL) di Windows. Fornisce il controllo degli accessi a livello di file system utilizzando i gruppi di sicurezza Amazon Virtual Private Cloud (Amazon VPC). Inoltre, fornisce il controllo degli accessi a livello di API utilizzando policy di accesso AWS Identity and Access Management (IAM). Gli utenti che accedono ai file system vengono autenticati con Microsoft Active Directory. Amazon FSx si integra AWS CloudTrail per monitorare e registrare le chiamate API, consentendoti di visualizzare le azioni intraprese dagli utenti sulle tue risorse Amazon FSx.

Inoltre, protegge i dati eseguendo automaticamente backup estremamente durevoli del file system su base giornaliera e consente di eseguire backup aggiuntivi in qualsiasi momento. Per ulteriori informazioni, consulta Sicurezza in Amazon FSx.

Disponibilità e durabilità

FSx for Windows File Server offre file system con due livelli di disponibilità e durabilità. I file Single-AZ garantiscono un'elevata disponibilità all'interno di un'unica zona di disponibilità (AZ) rilevando e risolvendo automaticamente i guasti dei componenti. Inoltre, i file system Multi-AZ forniscono elevata disponibilità e supporto di failover su più zone di disponibilità mediante il provisioning e la manutenzione di un file server di standby in una zona di disponibilità separata all'interno di una regione. AWS Per ulteriori informazioni sulle implementazioni di file system Single-AZ e Multi-AZ, consulta. Disponibilità e durabilità: file system Single-AZ e Multi-AZ

Gestione dei file system

È possibile amministrare i file system FSx for Windows File Server utilizzando comandi di PowerShell gestione remota personalizzati o utilizzando la GUI nativa di Windows in alcuni casi. Per ulteriori informazioni sulla gestione dei file system Amazon FSx, consulta. Amministrazione dei file system

Flessibilità in termini di prezzi e prestazioni

FSx for Windows File Server offre la flessibilità in termini di prezzo e prestazioni offrendo tipi di storage sia su unità a stato solido (SSD) che su unità disco rigido (HDD). Lo storage su HDD è progettato per un ampio spettro di carichi di lavoro, tra cui home directory, condivisioni di utenti e dipartimenti e sistemi di gestione dei contenuti. Lo storage SSD è progettato per i carichi di lavoro con le prestazioni più elevate e la maggior parte dei carichi di lavoro sensibili alla latenza, inclusi database, carichi di lavoro di elaborazione multimediale e applicazioni di analisi dei dati.

Con FSx for Windows File Server, è possibile effettuare il provisioning dello storage del file system, degli IOPS SSD e della velocità effettiva in modo indipendente per ottenere il giusto mix di costi e prestazioni. È possibile modificare le capacità di storage, gli IOPS SSD e il throughput del file system per soddisfare le mutevoli esigenze dei carichi di lavoro, in modo da pagare solo per ciò di cui si ha bisogno. Per ulteriori informazioni, consulta Ottimizzazione dei costi con Amazon FSx.

Prezzi per Amazon FSx

Con Amazon FSx, non ci sono costi hardware o software iniziali. Paghi solo per le risorse utilizzate, senza impegni minimi, costi di configurazione o costi aggiuntivi. Per informazioni sui prezzi e le tariffe associati al servizio, consulta i prezzi di Amazon FSx for Windows File Server.

Presupposti

Per utilizzare Amazon FSx, è necessario un AWS account con un'istanza Amazon EC2, un'istanza WorkSpaces , un'istanza AppStream 2.0 o una macchina virtuale in esecuzione in VMware Cloud su AWS ambienti del tipo supportato.

In questa guida, facciamo i seguenti presupposti:

- Se utilizzi Amazon EC2, supponiamo che tu abbia familiarità con Amazon EC2. Per ulteriori informazioni su come usare Amazon EC2, consulta la documentazione di Amazon Elastic Compute Cloud.
- Se lo utilizzi WorkSpaces, supponiamo che tu conosca. WorkSpaces Per ulteriori informazioni sull'uso WorkSpaces, consulta Amazon WorkSpaces User Guide.
- Se utilizzi VMware Cloud on AWS, supponiamo che tu lo conosca. Per ulteriori informazioni, consulta VMware Cloud on. AWS
- Partiamo dal presupposto che tu abbia familiarità con i concetti di Microsoft Active Directory.

Prerequisiti

Per creare un file system Amazon FSx, è necessario quanto segue:

- Un AWS account con le autorizzazioni necessarie per creare un file system Amazon FSx e un'istanza Amazon EC2. Per ulteriori informazioni, consulta Configurare il Account AWS.

- Un'istanza Amazon EC2 che esegue Microsoft Windows Server nel cloud privato virtuale (VPC) basata sul servizio Amazon VPC che desideri associare al tuo file system Amazon FSx. Per informazioni su come crearne una, consulta Getting Started with Amazon EC2 Windows Instances nella Amazon EC2 User Guide.
- Amazon FSx funziona con Microsoft Active Directory per eseguire l'autenticazione degli utenti e il controllo degli accessi. Unisci il tuo file system Amazon FSx a Microsoft Active Directory durante la creazione. Per ulteriori informazioni, consulta Utilizzo di Microsoft Active Directory in FSx for Windows File Server.
- Questa guida presuppone che tu non abbia modificato le regole sul gruppo di sicurezza predefinito per il tuo VPC basato sul servizio Amazon VPC. In caso affermativo, devi assicurarti di aggiungere le regole necessarie per consentire il traffico di rete dall'istanza Amazon EC2 al file system Amazon FSx. Per ulteriori dettagli, consulta Sicurezza in Amazon FSx.
- Installa e configura AWS Command Line Interface ()AWS CLI. Le versioni supportate sono 1.9.12 e successive. Per ulteriori informazioni, vedere Installazione, aggiornamento e disinstallazione di AWS CLI nella Guida per l'utente.AWS Command Line Interface

> **Note**
>
> Puoi controllare la versione del file AWS CLI che stai utilizzando con il `aws --version` comando.

Forum di Amazon FSx per Windows File Server

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

Sei un utente alle prime armi di Amazon FSx?

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

1. Se sei pronto a creare il tuo primo file system Amazon FSx, prova il. Guida introduttiva ad Amazon FSx for Windows File Server
2. Per informazioni sulle prestazioni, consultare Prestazioni di FSx for Windows File Server.
3. Per i dettagli sulla sicurezza di Amazon FSx, consulta. Sicurezza in Amazon FSx
4. Per informazioni sull'API Amazon FSx, consulta Amazon FSx API Reference.

Procedure consigliate per FSx for Windows File Server

Ti consigliamo di seguire queste best practice quando lavori con Amazon FSx for Windows File Server. Segui i link sottostanti per saperne di più sugli argomenti trattati.

Argomenti

Best practice generali

Verifica dei carichi di lavoro prima di passare alla produzione

Ti consigliamo di utilizzare un ambiente di staging con la stessa configurazione dell'ambiente di produzione per testare i carichi di lavoro. Ad esempio, utilizza le stesse configurazioni di Active Directory (AD) e di rete, le stesse dimensioni e configurazione del file system e le stesse funzionalità di Windows, come la deduplicazione dei dati e le copie shadow. L'esecuzione di carichi di lavoro di test in un ambiente di staging che simula il traffico di produzione desiderato contribuisce a garantire il corretto svolgimento del processo.

Consigliamo inoltre di esaminare il modello di disponibilità del file system e di garantire che il carico di lavoro sia resiliente al comportamento di ripristino previsto per il tipo di file system in uso durante eventi quali la manutenzione del file system, le modifiche della capacità di throughput e le interruzioni non pianificate del servizio. Per ulteriori informazioni, consulta Disponibilità e durabilità: file system Single-AZ e Multi-AZ.

Creazione di un piano di monitoraggio

È possibile utilizzare le metriche del file system per monitorare l'utilizzo dello storage e delle prestazioni, comprendere i modelli di utilizzo e attivare notifiche quando l'utilizzo si avvicina ai limiti di storage o di prestazioni del file system. Il monitoraggio dei file system Amazon FSx insieme al resto dell'ambiente applicativo consente di eseguire rapidamente il debug di eventuali problemi che potrebbero influire sulle prestazioni.

Garantire che i file system dispongano di risorse sufficienti

La mancanza di risorse può comportare un aumento della latenza e dell'accodamento per le richieste di I/O, il che potrebbe apparire come un'indisponibilità totale o parziale del file system. Per ulteriori informazioni sul monitoraggio delle prestazioni e sull'accesso agli avvisi e ai consigli sulle prestazioni, vedere. Monitoraggio di FSx per Windows File Server

Eseguire regolarmente il backup dei file system

I backup regolari consentono di soddisfare le esigenze di conservazione dei dati, aziendali e di conformità. Ti consigliamo di utilizzare i backup giornalieri automatici abilitati per impostazione predefinita per il tuo file system e di utilizzarli AWS Backup per una soluzione di backup centralizzata in tutto. Servizi AWS AWS Backup consente di configurare piani di backup aggiuntivi con frequenze diverse (ad esempio, più volte al giorno, giornalmente o settimanalmente) e periodi di conservazione.

Best practice di sicurezza

Ti consigliamo di seguire queste best practice per amministrare la sicurezza e i controlli di accesso del file system. Per informazioni più dettagliate sulla configurazione di Amazon FSx per soddisfare i tuoi obiettivi di sicurezza e conformità, consulta. Sicurezza in Amazon FSx

Sicurezza di rete

Non modificare o eliminare l'ENI associato al tuo file system

L'accesso al file system Amazon FSx avviene tramite un'interfaccia di rete elastica (ENI) che risiede nel cloud privato virtuale (VPC) associato 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.

Utilizzo dei gruppi di sicurezza e delle liste di controllo degli accessi di rete

È possibile utilizzare gruppi di sicurezza e elenchi di controllo degli accessi alla rete (ACL) per limitare l'accesso ai file system. Per i gruppi di sicurezza VPC, il gruppo di sicurezza predefinito è già stato aggiunto al file system nella console. Assicurati che il gruppo di sicurezza e gli ACL di rete per le sottoreti in cui crei il file system consentano il traffico sulle porte. Per ulteriori informazioni, consulta Gruppi di sicurezza Amazon VPC.

Active Directory

Quando crei un file system Amazon FSx, puoi aggiungerlo al tuo dominio Microsoft AD per fornire l'autenticazione degli utenti e l'autorizzazione al controllo degli accessi a livello di condivisione, file e cartella. I tuoi utenti possono utilizzare i loro account AD esistenti per connettersi alle condivisioni di file e accedere a file e cartelle al loro interno. Inoltre, puoi migrare la configurazione ACL di sicurezza esistente su Amazon FSx senza alcuna modifica. Amazon FSx offre due opzioni per Active Directory: AWS Microsoft AD gestito o Microsoft AD autogestito.

Se utilizzi un Microsoft AD AWS gestito, ti consigliamo di lasciare le impostazioni predefinite del tuo gruppo di sicurezza AD. Se modifichi queste impostazioni, assicurati di mantenere una configurazione di rete che soddisfi i requisiti di rete. Per ulteriori informazioni, consulta Prerequisiti di rete.

Se utilizzi un Microsoft AD autogestito, hai a disposizione opzioni aggiuntive per la configurazione del file system. Consigliamo le seguenti best practice per la configurazione iniziale quando si utilizza Amazon FSx con Microsoft AD autogestito:

- Assegna sottoreti a un singolo sito AD: se il tuo ambiente AD ha un gran numero di controller di dominio, utilizza Siti e servizi di Active Directory per assegnare le sottoreti utilizzate dai tuoi file system Amazon FSx a un singolo sito AD con la massima disponibilità e affidabilità. Assicurati che il gruppo di sicurezza VPC, l'ACL di rete VPC, le regole del firewall di Windows sui tuoi DC e qualsiasi altro controllo di routing di rete presente nell'infrastruttura AD consentano la comunicazione da Amazon FSx sulle porte richieste. Ciò consente a Windows di tornare ad altri DC se non può utilizzare il sito AD assegnato. Per ulteriori informazioni, consulta Controllo degli accessi ai file system con Amazon VPC.
- Usa un'unità organizzativa (OU) separata: utilizza un'unità organizzativa per i tuoi file system Amazon FSx separata da qualsiasi altra unità organizzativa che potresti avere.
- Configura il tuo account di servizio con i privilegi minimi richiesti: configura o delega l'account di servizio che fornisci ad Amazon FSx con i privilegi minimi richiesti. Per ulteriori informazioni, consulta Prerequisiti per l'utilizzo di un Microsoft Active Directory autogestito e Delega dei privilegi al tuo account di servizio Amazon FSx .
- Verifica continua la tua configurazione AD: esegui lo strumento di convalida Amazon FSx Active Directory sulla tua configurazione AD prima di creare il file system Amazon FSx per verificare che la configurazione sia valida per l'uso con Amazon FSx e per scoprire eventuali avvisi ed errori che lo strumento potrebbe esporre.

Evita la perdita di disponibilità a causa di una configurazione errata di AD

Quando si utilizza Amazon FSx con Microsoft AD autogestito, è importante disporre di una configurazione AD valida non solo durante la creazione del file system, ma anche per le operazioni e la disponibilità continue. Durante gli eventi di ripristino in caso di guasto, gli eventi di manutenzione ordinaria e le azioni di aggiornamento della capacità di throughput, Amazon FSx ricongiunge le risorse del file server all'Active Directory. Se la configurazione AD non è valida durante un evento, il file system passa allo stato Non configurato correttamente e rischia di non essere più disponibile. Ecco alcuni modi per evitare di perdere la disponibilità:

- Mantieni aggiornata la tua configurazione AD con Amazon FSx: se apporti modifiche, come la reimpostazione della password del tuo account di servizio, assicurati di aggiornare la configurazione per tutti i file system che utilizzano questo account di servizio.
- Monitora eventuali errori di configurazione AD: imposta automaticamente le notifiche sullo stato di configurazione errata in modo da poter ripristinare la configurazione AD del file system, se necessario. Per un esempio che utilizza una soluzione basata su Lambda per raggiungere questo obiettivo, consulta Monitoraggio dello stato dei file system Amazon FSx utilizzando Amazon e. EventBridge AWS Lambda
- Convalida regolarmente la tua configurazione AD: se desideri rilevare in modo proattivo le configurazioni errate di AD, ti consigliamo di eseguire lo strumento di convalida di Active Directory sulla tua configurazione AD su base continuativa. Se ricevi avvisi o errori durante l'esecuzione dello strumento di convalida, significa che il file system rischia di essere configurato in modo errato.
- Non spostare o modificare oggetti informatici creati da FSx: Amazon FSx crea e gestisce oggetti informatici nel tuo AD, utilizzando l'account di servizio e le autorizzazioni che fornisci. Lo spostamento o la modifica di questi oggetti informatici può comportare una configurazione errata del file system.

ACL di Windows

Con Amazon FSx, utilizzi elenchi di controllo degli accessi (ACL) standard di Windows per un controllo granulare degli accessi a livello di condivisione, file e cartella. I file system Amazon FSx verificano automaticamente le credenziali degli utenti che accedono ai dati del file system per applicare questi ACL di Windows.

- Non modificare le autorizzazioni NTFS ACL per l'utente SYSTEM: Amazon FSx richiede che l'utente SYSTEM disponga del pieno controllo delle autorizzazioni NTFS ACL su tutte le cartelle all'interno del file system. La modifica delle autorizzazioni ACL NTFS per l'utente SYSTEM

può rendere il file system inaccessibile e i futuri backup del file system potrebbero diventare inutilizzabili.

Configurazione e dimensionamento corretto del file system

Selezione di un tipo di distribuzione

Amazon FSx offre due opzioni di implementazione: Single-AZ e Multi-AZ. Consigliamo di utilizzare file system Multi-AZ per la maggior parte dei carichi di lavoro di produzione che richiedono un'elevata disponibilità di dati di file Windows condivisi. Per ulteriori informazioni, consulta Disponibilità e durabilità: file system Single-AZ e Multi-AZ.

Selezione di un tipo di archiviazione

Lo storage SSD è appropriato per la maggior parte dei carichi di lavoro di produzione che presentano requisiti di prestazioni elevati e sensibilità alla latenza. Esempi di questi carichi di lavoro includono database, analisi dei dati, elaborazione multimediale e applicazioni aziendali. Consigliamo l'SSD anche per casi d'uso che coinvolgono un gran numero di utenti finali, alti livelli di I/O o set di dati con un gran numero di file di piccole dimensioni. Infine, ti consigliamo di utilizzare l'archiviazione SSD se prevedi di abilitare le copie shadow. È possibile configurare e scalare gli IOPS SSD per i file system con storage SSD, ma non per lo storage su HDD.

Se decidi di utilizzare lo storage su HDD, verifica il tuo file system per assicurarti che sia in grado di soddisfare i tuoi requisiti prestazionali. Lo storage su HDD ha un costo inferiore rispetto allo storage SSD, ma con latenze più elevate e livelli inferiori di throughput del disco e IOPS del disco per unità di storage. Potrebbe essere adatto per condivisioni utente generiche e home directory con requisiti di I/O ridotti, sistemi di gestione dei contenuti (CMS) di grandi dimensioni in cui i dati vengono recuperati raramente o set di dati con un numero limitato di file di grandi dimensioni. Per ulteriori informazioni, consulta Configurazione e prestazioni dello storage.

Puoi aggiornare il tuo tipo di storage da HDD a SSD in qualsiasi momento utilizzando la console Amazon FSx o l'API Amazon FSx. Per ulteriori informazioni, consulta Gestione del tipo di storage.

Selezione di una capacità di throughput

Configura il file system con una capacità di throughput sufficiente a soddisfare non solo il traffico previsto del carico di lavoro, ma anche le risorse prestazionali aggiuntive necessarie per supportare le funzionalità che desideri abilitare sul file system. Ad esempio, se si esegue la deduplicazione

dei dati, la capacità di throughput selezionata deve fornire memoria sufficiente per eseguire la deduplicazione in base allo storage di cui si dispone. Se utilizzi copie shadow, aumenta la capacità di throughput a un valore almeno tre volte il valore che dovrebbe essere determinato dal carico di lavoro per evitare che Windows Server elimini le tue copie shadow. Per ulteriori informazioni, consulta Impatto della capacità di throughput sulle prestazioni.

Aumento della capacità di archiviazione e della capacità di throughput

Aumenta la capacità di storage del tuo file system quando lo spazio di archiviazione disponibile sta per esaurirsi o quando prevedi che i tuoi requisiti di storage superino l'attuale limite di archiviazione. Ti consigliamo di mantenere sempre almeno il 10% della capacità di archiviazione gratuita sul tuo file system. Si consiglia inoltre di aumentare la capacità di storage di almeno il 20% prima della scalabilità dello storage, poiché non sarà possibile aumentarla mentre il processo è in corso. Puoi utilizzare la CloudWatch metrica della FreeStoragecapacità per monitorare la quantità di spazio di archiviazione gratuito disponibile e comprenderne l'andamento. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione.

È inoltre necessario aumentare la capacità di throughput del file system se il carico di lavoro è limitato dagli attuali limiti di prestazioni. È possibile utilizzare la pagina Monitoraggio e prestazioni sulla console FSx per vedere quando le richieste del carico di lavoro hanno raggiunto o superato i limiti di prestazioni per determinare se il file system è sottodimensionato per il carico di lavoro.

Per ridurre al minimo la durata del ridimensionamento dello storage ed evitare una riduzione delle prestazioni di scrittura, si consiglia di aumentare la capacità di throughput del file system prima di aumentare la capacità di storage e quindi di ridimensionare la capacità di throughput al termine dell'aumento della capacità di storage. La maggior parte dei carichi di lavoro ha un impatto minimo sulle prestazioni durante la scalabilità dello storage, ma le applicazioni che richiedono molta scrittura e con set di dati attivi di grandi dimensioni possono temporaneamente subire una riduzione fino alla metà delle prestazioni di scrittura.

Modifica della capacità di throughput durante i periodi di inattività

L'aggiornamento della capacità di throughput interrompe la disponibilità per alcuni minuti per i file system Single-AZ e causa il failover e il failback per i file system Multi-AZ. Per i file system Multi-AZ, se il traffico è continuo durante il failover e il failback, tutte le modifiche ai dati apportate durante questo periodo dovranno essere sincronizzate tra i file server. Il processo di sincronizzazione dei dati può richiedere fino a diverse ore per carichi di lavoro con elevati livelli di scrittura e IOPS. Sebbene il file system continui a essere disponibile durante questo periodo, consigliamo di pianificare le finestre

di manutenzione e di eseguire aggiornamenti della capacità di trasmissione durante i periodi di inattività, quando il carico sul file system è minimo, per ridurre la durata della sincronizzazione dei dati. Per ulteriori informazioni, consulta Gestione della capacità di throughput.

Guida introduttiva ad Amazon FSx for Windows File Server

Di seguito, è possibile scoprire come iniziare a utilizzare FSx for Windows File Server. Questo esercizio introduttivo include i seguenti passaggi.

1. Registrati Account AWS e crea un utente amministrativo nell'account.
2. Creare un Microsoft AD Active Directory AWS gestito utilizzando AWS Directory Service. Unirai il tuo file system e l'istanza di calcolo ad Active Directory.
3. Crea un'istanza di calcolo Amazon Elastic Compute Cloud con Microsoft Windows Server. Utilizzerai questa istanza per accedere al tuo file system.
4. Crea un file system Amazon FSx for Windows File Server utilizzando la console Amazon FSx.
5. Mappa il tuo file system sulla tua istanza EC2
6. Scrivi dati sul tuo file system.
7. Eseguite il backup del file system.
8. Eliminare tutte le risorse create.

Argomenti

Configurare il Account AWS

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

Registrati per un Account AWS

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

Per iscriverti a un Account AWS

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

   Nel corso della procedura di registrazione riceverai una telefonata, durante la quale sarà necessario inserire un codice di verifica attraverso la tastiera del telefono.

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come procedura consigliata in materia di sicurezza, assegnate l'accesso amministrativo a un utente e utilizzate solo l'utente root per eseguire attività che richiedono l'accesso da parte dell'utente root.

AWS ti invia un'e-mail di conferma dopo il completamento della procedura di registrazione. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

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

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

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

Crea un utente con accesso amministrativo

1. Abilita Centro identità IAM.

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

2. In IAM Identity Center, concedi l'accesso amministrativo a un utente.

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

Accedi come utente con accesso amministrativo

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

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

Assegna l'accesso ad altri utenti

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

   Per istruzioni, consulta Creare un set di autorizzazioni nella Guida per l'utente.AWS IAM Identity Center

2. Assegna gli utenti a un gruppo, quindi assegna l'accesso Single Sign-On al gruppo.

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

Crea il tuo file system

Per creare il tuo file system Amazon FSx, devi creare l'istanza Windows Amazon Elastic Compute Cloud (Amazon EC2) e la directory. AWS Directory Service Se non l'hai già configurata, consulta. Procedura guidata 1: Prerequisiti per iniziare

Per creare il tuo file system (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di controllo, scegli Crea file system per avviare la procedura guidata di creazione del file system.
3. Sulla pagina Seleziona tipo di file system, seleziona FSx for Windows File Server, quindi seleziona Successivo. Viene visualizzata la pagina Crea file system.
4. Per il metodo di creazione scegli Standard create.

Dettagli del file system

1. Nella sezione Dettagli file system, specifica 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 caratteri speciali + - =. _:/
2. Per il tipo di implementazione scegli Multi-AZ o Single-AZ.

   - Scegliete Multi-AZ per implementare un file system tollerante all'indisponibilità della zona di disponibilità. Questa opzione supporta l'archiviazione su SSD e HDD.
   - Scegli Single-AZ per implementare un file system distribuito in un'unica zona di disponibilità. Single-AZ 2 è l'ultima generazione di file system a zona di disponibilità singola e supporta l'archiviazione SSD e HDD.

   Per ulteriori informazioni, consulta Disponibilità e durabilità: file system Single-AZ e Multi-AZ.
3. Per il tipo di archiviazione, puoi scegliere SSD o HDD.

   FSx for Windows File Server offre tipi di storage su unità a stato solido (SSD) e unità disco rigido (HDD). Lo storage SSD è progettato per i carichi di lavoro con le prestazioni più elevate e la maggior parte dei carichi di lavoro sensibili alla latenza, inclusi database, carichi di lavoro di elaborazione multimediale e applicazioni di analisi dei dati. Lo storage su HDD è progettato per un ampio spettro di carichi di lavoro, tra cui home directory, condivisioni di file tra utenti e dipartimenti e sistemi di gestione dei contenuti. Per ulteriori informazioni, consulta Ottimizzazione dei costi utilizzando i tipi di storage.
4. Per Provisioned SSD IOPS, puoi scegliere la modalità Automatica o User-provisioned.

   Se si sceglie la modalità Automatica, FSx for Windows File Server ridimensiona automaticamente gli IOPS SSD per mantenere 3 IOPS SSD per GiB di capacità di storage. Se

scegliete la modalità User-provisioned, inserite un numero intero compreso tra 96 e 400.000. La scalabilità degli IOPS SSD superiori a 80.000 è disponibile negli Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti orientali (Ohio), Europa (Irlanda), Asia Pacifico (Tokyo) e Asia Pacifico (Singapore). Per ulteriori informazioni, consulta Gestione degli IOPS SSD.

5. Per Capacità di archiviazione, immettere la capacità di archiviazione del file system, in GiB. Se utilizzi l'archiviazione SSD, inserisci un numero intero compreso tra 32 e 65.536. Se utilizzi l'archiviazione su HDD, inserisci un numero intero compreso tra 2.000 e 65.536. 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.
6. Mantieni Capacità di velocità effettiva sul valore di default. La capacità di throughput è la velocità sostenuta alla quale il file server che ospita il file system può fornire i dati. L'impostazione della capacità di throughput consigliata si basa sulla quantità di capacità di archiviazione scelta. Se hai bisogno di una capacità di throughput superiore a quella consigliata, scegli Specificare la capacità di throughput, quindi scegli un valore. Per ulteriori informazioni, consulta Prestazioni di FSx for Windows File Server.

   > **Note**
   >
   > Se intendi abilitare il controllo dell'accesso ai file, devi scegliere una capacità di trasmissione di 32 MB/s o superiore. Per ulteriori informazioni, consulta Controllo dell'accesso ai file.

   È possibile modificare la capacità di trasmissione in base alle esigenze in qualsiasi momento dopo la creazione del file system. Per ulteriori informazioni, consulta Gestione della capacità di throughput.

Rete e sicurezza

1. Nella sezione Rete e sicurezza, scegli l'Amazon VPC che desideri associare al tuo file system. Per questo esercizio introduttivo, scegli lo stesso Amazon VPC che hai scelto per la tua AWS Directory Service directory e la tua istanza Amazon EC2.
2. Per i gruppi di sicurezza VPC, il gruppo di sicurezza predefinito per il tuo Amazon VPC predefinito è già aggiunto al file system nella console. Se non utilizzi il gruppo di sicurezza

predefinito, assicurati che il gruppo di sicurezza scelto appartenga allo Regione AWS stesso del tuo file system. Per assicurarti di poter connettere un'istanza EC2 al tuo file system, dovrai aggiungere le seguenti regole al gruppo di sicurezza scelto:

a. Aggiungi le seguenti regole in entrata e in uscita per consentire le seguenti porte.

Regolamento	Porte
UDP	53, 88, 123, 389, 464
TCP	53, 88, 135, 389, 445, 464, 636, 3268, 3269, 5985, 9389, 49152-65535

Aggiungi da e verso gli indirizzi IP o gli ID dei gruppi di sicurezza associati alle istanze di calcolo del client da cui desideri accedere al file system.

b. Aggiungi regole in uscita per consentire tutto il traffico verso l'Active Directory a cui ti stai unendo al file system. Per ottenere ciò, procedi in uno dei seguenti modi:

- Consenti il traffico in uscita verso l'ID del gruppo di sicurezza associato alla tua directory AWS Managed AD.
- Consenti il traffico in uscita verso gli indirizzi IP associati ai controller di dominio Active Directory autogestiti.

> **Note**
>
> In alcuni casi, potresti aver modificato le regole del tuo gruppo di AWS Managed Microsoft AD sicurezza rispetto alle impostazioni predefinite. In tal caso, assicurati che questo gruppo di sicurezza disponga delle regole in entrata necessarie per consentire il traffico proveniente dal tuo file system Amazon FSx. Per ulteriori informazioni sulle regole in entrata richieste, consulta AWS Managed Microsoft AD Prerequisiti nella Guida all'amministrazione.AWS Directory Service

Per ulteriori informazioni, consulta Controllo degli accessi ai file system con Amazon VPC.

3. I file system Multi-AZ dispongono di un file server primario e uno di standby, ciascuno nella propria zona di disponibilità e nella propria sottorete. Se state creando un file system Multi-AZ

(vedere il passaggio 5), scegliete un valore di sottorete preferito per il file server primario e un valore di sottorete Standby per il file server di standby.

Se state creando un file system Single-AZ, scegliete la sottorete per il vostro file system.

Autenticazione Windows

- Per l'autenticazione Windows, sono disponibili le seguenti opzioni:

  Scegli AWS Gestito Microsoft Active Directory se desideri aggiungere il tuo file system a un dominio Microsoft Active Directory gestito da AWS, quindi scegli la tua AWS Directory Service directory dall'elenco. Per ulteriori informazioni, consulta Utilizzo di Microsoft Active Directory in FSx for Windows File Server.

  Scegli Microsoft Active Directory autogestito se desideri aggiungere il tuo file system a un dominio Microsoft Active Directory autogestito e fornire i seguenti dettagli per Active Directory. Per ulteriori informazioni, consulta Utilizzo di Amazon FSx con Microsoft Active Directory autogestito.

  - Il nome di dominio completo del tuo Active Directory.

    > **Important**
    >
    > Per Single-AZ 2 e tutti i file system Multi-AZ, il nome di dominio Active Directory non può superare i 47 caratteri. Questa limitazione si applica a entrambi i nomi di dominio AWS Directory Service Active Directory autogestiti.
    > Amazon FSx richiede una connessione diretta per il traffico interno al tuo indirizzo IP DNS. La connessione tramite un gateway Internet non è supportata. Utilizza invece il AWS Virtual Private Network peering o l'associazione VPC. AWS Direct Connect AWS Transit Gateway

  - Indirizzi IP dei server DNS: gli indirizzi IPv4 dei server DNS per il tuo dominio

    > **Note**
    >
    > Il server DNS deve avere l'EDNS (Extension Mechanisms for DNS) abilitato. Se l'EDNS è disabilitato, la creazione del file system potrebbe non riuscire.

- Nome utente dell'account di servizio: il nome utente dell'account di servizio nell'Active Directory esistente. Non includere un prefisso o un suffisso di dominio.
- Password dell'account di servizio: la password per l'account di servizio.
- (Facoltativo) Unità organizzativa (OU): il nome del percorso distinto dell'unità organizzativa in cui si desidera entrare a far parte del file system.
- (Facoltativo) Gruppo di amministratori del file system delegati: il nome del gruppo in Active Directory che può amministrare il file system. Il gruppo predefinito è «Domain Admins». Per ulteriori informazioni, consulta Delega dei privilegi al tuo account di servizio Amazon FSx .

Crittografia, controllo e accesso (alias DNS)

1. Per la crittografia, scegli la chiave di AWS KMS key crittografia utilizzata per crittografare i dati sul file system a riposo. Puoi scegliere l'aws/fsx predefinito (predefinito) gestito da AWS KMS, una chiave esistente o una chiave gestita dal cliente specificando l'ARN per la chiave. Per ulteriori informazioni, consulta Crittografia dei dati inattivi.
2. Per il controllo: facoltativo, il controllo dell'accesso ai file è disabilitato per impostazione predefinita. Per informazioni sull'attivazione e la configurazione del controllo dell'accesso ai file, vedere. Per abilitare il controllo dell'accesso ai file durante la creazione di un file system (console)
3. Per Access, facoltativo, inserisci gli alias DNS che desideri associare al file system. Ogni nome alias deve essere formattato come nome di dominio completo (FQDN). Per ulteriori informazioni, consulta Gestione degli alias DNS.

Backup e manutenzione

Per ulteriori informazioni sui backup giornalieri automatici e sulle impostazioni di questa sezione, vedereUtilizzo dei backup.

1. Per impostazione predefinita, il backup automatico giornaliero è abilitato. Puoi disabilitare questa impostazione se non desideri che Amazon FSx esegua automaticamente i backup del tuo file system su base giornaliera.
2. Se i backup automatici sono abilitati, vengono eseguiti entro un periodo di tempo noto come finestra di backup. È possibile utilizzare la finestra predefinita o scegliere l'ora di inizio della finestra di backup automatico.

3. Per il periodo di conservazione dei backup automatici, puoi utilizzare l'impostazione predefinita di 30 giorni o impostare un valore compreso tra 1 e 90 giorni per cui Amazon FSx conserverà i backup giornalieri automatici del tuo file system. Questa impostazione non si applica ai backup avviati dall'utente o ai backup eseguiti da. AWS Backup
4. Per i tag: facoltativo, inserisci 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. Per ulteriori informazioni, consulta la pagina Tagging delle risorse Amazon FSx.

   Seleziona Next (Successivo).

Rivedi la tua configurazione e crea

1. Rivedi la configurazione del file system riportata nella pagina Crea file system. Come riferimento, puoi vedere quali impostazioni del file system puoi e non puoi modificare dopo la creazione del file system. Scegliere Create file system (Crea file system).
2. Dopo che Amazon FSx ha creato il file system, scegli l'ID del file system dall'elenco nel pannello di controllo dei file system per visualizzare i dettagli. Scegli Allega e annota il nome DNS del tuo file system nella scheda Rete e sicurezza. Ti servirà nella seguente procedura per mappare una condivisione su un'istanza EC2.

Mappa la condivisione di file su un'istanza EC2 che esegue Windows Server

Ora puoi montare il tuo file system Amazon FSx sulla tua istanza Amazon EC2 basata su Microsoft Windows unita alla tua directory. AWS Directory Service Il nome della condivisione di file non è lo stesso del file system.

Per mappare una condivisione di file su un'istanza Amazon EC2 Windows utilizzando la GUI

1. Prima di poter montare una condivisione di file su un'istanza Windows, devi avviare l'istanza EC2 e unirla a un. AWS Directory Service for Microsoft Active Directory Per eseguire questa azione, scegli una delle seguenti procedure dalla Guida all'AWS Directory Service amministrazione:

   - Aggiunta di un'istanza EC2 Windows
   - Collegamento manuale di un'istanza Windows

2. Connettiti alla tua istanza. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
3. Quando sei connesso, apri File Explorer.
4. Dal pannello di navigazione, apri il menu contestuale (fai clic con il pulsante destro del mouse) per Network e scegli Map Network Drive.
5. Scegli una lettera di unità a tua scelta per Drive.
6. Puoi mappare il tuo file system utilizzando il nome DNS predefinito assegnato da Amazon FSx o utilizzando un alias DNS di tua scelta. Questa procedura descrive la mappatura di una condivisione di file utilizzando il nome DNS predefinito. Se desideri mappare una condivisione di file utilizzando un alias DNS, consulta. Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system

   Per Cartella, inserisci il nome DNS del file system e il nome della condivisione. Viene chiamata la condivisione Amazon FSx predefinita. `\share` Puoi trovare il nome DNS nella console Amazon FSx, https://console.aws.amazon.com/fsx/, nella sezione Windows File Server > Rete e sicurezza o nella risposta CreateFileSystem di DescribeFileSystems un comando API.

   - Per un file system Single-AZ unito a un Microsoft Active Directory AWS gestito, il nome DNS è simile al seguente.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - Per un file system Single-AZ unito a un Active Directory autogestito e qualsiasi file system Multi-AZ, il nome DNS è simile al seguente.

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   Ad esempio, specifica `\\fs-0123456789abcdef0.ad-domain.com\share`.
7. Scegli se riconnettersi la condivisione di file all'accesso, quindi scegli Fine.

Scrivi dati nella tua condivisione di file

Ora che hai mappato la condivisione di file sull'istanza, puoi utilizzare la condivisione di file come qualsiasi altra directory nell'ambiente Windows.

Per scrivere dati nella condivisione di file

1. Apri l'editor di testo Notepad.
2. Scrivi del contenuto nell'editor di testo. Ad esempio: *Hello, World!*
3. Salva il file nella lettera di unità della condivisione di file.
4. Utilizzando File Explorer, accedi alla tua condivisione di file e trova il file di testo che hai appena salvato.

Esegui il backup del file system

Ora che hai avuto la possibilità di utilizzare il tuo file system Amazon FSx e le relative condivisioni di file, puoi eseguirne il backup. Per impostazione predefinita, i backup giornalieri vengono creati automaticamente durante la finestra di backup di 30 minuti del file system. Tuttavia, è possibile creare un backup avviato dall'utente in qualsiasi momento. I backup comportano costi aggiuntivi. Per ulteriori informazioni sui prezzi dei backup, consulta la sezione Prezzi.

Per creare un backup del file system dalla console

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard della console, scegli il nome del file system che hai creato per questo esercizio.
3. Dalla scheda Panoramica del file system, scegli Crea backup.
4. Nella finestra di dialogo Crea backup che si apre, fornisci un nome per il backup. Questo nome può contenere un massimo di 256 lettere Unicode e includere spazi bianchi, numeri e i seguenti caratteri speciali: + - =. _:/
5. Scegliere Create backup (Crea backup).
6. Per visualizzare tutti i backup in un elenco, in modo da poter ripristinare il file system o eliminare il backup, scegli Backup.

Quando crei un nuovo backup, il relativo stato è impostato su CREAZIONE durante la creazione. Ciò può richiedere alcuni minuti. Quando il backup è disponibile per l'uso, il suo stato cambia in AVAILABLE.

Pulizia delle risorse

Dopo aver terminato questo esercizio, è necessario seguire questi passaggi per ripulire le risorse e proteggere l' AWS account.

Per eliminare le risorse

1. Sulla console Amazon EC2, interrompi l'istanza. Per ulteriori informazioni, consulta Terminate Your Instance nella Amazon EC2 User Guide.
2. Sulla console Amazon FSx, elimina il file system. Tutti i backup automatici vengono eliminati automaticamente. Tuttavia, è comunque necessario eliminare i backup creati manualmente. I passaggi seguenti descrivono questo processo:
   a. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
   b. Dalla dashboard della console, scegli il nome del file system che hai creato per questo esercizio.
   c. In Azioni, seleziona Elimina file system.
   d. Nella finestra di dialogo Elimina il file system che si apre, decidete se desiderate creare un backup finale. In tal caso, fornite un nome per il backup finale. Vengono eliminati anche tutti i backup creati automaticamente.

      > **Important**
      >
      > È possibile creare nuovi file system a partire dai backup. Si consiglia di creare un backup finale come procedura consigliata. Se ritieni di non averne bisogno dopo un certo periodo di tempo, puoi eliminare questo e altri backup creati manualmente.

   e. Immettete l'ID del file system che desiderate eliminare nella casella ID del file system.
   f. Scegliete Elimina file system.
   g. Il file system viene ora eliminato e il suo stato nella dashboard cambia in ELIMINAZIONE. Una volta eliminato, il file system non viene più visualizzato nella dashboard.
   h. Ora puoi eliminare qualsiasi backup creato manualmente per il tuo file system. Dalla barra di navigazione a sinistra, scegli Backup.
   i. Dalla dashboard, scegli tutti i backup con lo stesso ID di file system del file system che hai eliminato e scegli Elimina backup.

j. Viene visualizzata la finestra di dialogo Elimina backup. Lascia selezionata la casella di controllo per l'ID del backup selezionato e scegli Elimina backup.

Il file system Amazon FSx e i relativi backup automatici sono ora eliminati.

3. Se hai creato una AWS Directory Service directory per questo esercizioProcedura guidata 1: Prerequisiti per iniziare, puoi eliminarla ora. Per ulteriori informazioni, consulta Eliminare la directory nella Guida all'AWS Directory Service amministrazione.

Stato del file system Amazon FSx

Puoi visualizzare lo stato di un file system Amazon FSx utilizzando la console Amazon FSx, il AWS CLI comando describe-file-systems o i sistemi operativi API. DescribeFile

Stato del file system	Descrizione
DISPONIBILE	Il file system è integro, raggiungibile e disponibile per l'uso.
CREAZIONE IN CORSO	Amazon FSx sta creando un nuovo file system.
ELIMINAZIONE IN CORSO	Amazon FSx sta eliminando un file system esistente.
AGGIORNAMENTO IN CORSO	Il file system è in fase di aggiornamento avviato dal cliente.
CONFIGURATO MALE	Lo stato del file system è compromesso a causa di una modifica dell'ambiente Active Directory. Il file system non è attualmente disponibile o rischia di perdere la disponibilità e i backup potrebbero non riuscire. Per informazioni sul ripristino della disponibilità, vedere. Il file system è in uno stato configurato in modo errato
CONFIGURATO_NON DISPONIBILE	Il file system non è attualmente disponibile a causa di una modifica dell'ambiente Active

Stato del file system	Descrizione
	Directory. Per informazioni sul ripristino della disponibilità, vedereIl file system è in uno stato configurato in modo errato.
Non riuscito	• Durante la creazione di un nuovo file system, Amazon FSx non è stato in grado di creare il nuovo file system. • Il file system non è disponibile. • Il file system è guasto e Amazon FSx non è in grado di ripristinarlo. • Amazon FSx non è in grado di creare backup.

Client, metodi di accesso e ambienti supportati per Amazon FSx for Windows File Server

Puoi accedere ai tuoi file system Amazon FSx utilizzando una varietà di client e metodi supportati da entrambiAWSe ambienti locali.

Argomenti

Client supportati

Amazon FSx supporta la connessione al file system da un'ampia varietà di istanze di calcolo e sistemi operativi. Lo fa supportando l'accesso tramite il protocollo Server Message Block (SMB), versioni da 2.0 a 3.1.1.

I seguenti fileAWSle istanze di elaborazione sono supportate per l'uso con Amazon FSx:

- Istanze Amazon Elastic Compute Cloud (Amazon EC2), tra cui istanze Microsoft Windows, Amazon Linux e Amazon Linux 2. Per ulteriori informazioni, consulta Accesso alle condivisioni di file.
- Contenitori Amazon Elastic Container Service (Amazon ECS). Per ulteriori informazioni, consulta la paginaVolumi FSx for Windows File ServernelAmazon Elastic Container Service.
- WorkSpaces istanze — Per ulteriori informazioni, consulta laAWSpost sul blogUtilizzo di FSx for Windows File Server con Amazon WorkSpaces.
- Amazon AppStream Istanze 2.0: per ulteriori informazioni, consulta laAWSpost sul blogUtilizzo di Amazon FSx con Amazon AppStream 2.0.
- VM in esecuzione in VMware Cloud suAWSambienti — Per ulteriori informazioni, consulta laAWSpost sul blogArchiviazione e condivisione di file con FSx for Windows File Server in un cloud VMware suAWSAmbiente.

I seguenti sistemi operativi sono supportati per l'utilizzo con Amazon FSx:

- Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012, Windows Server 2012, Windows Server 2012, Windows Server 2012, Windows Server 2012, Windows Server 2012, Windows Server 2012.
- Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10 (incluse le esperienze desktop Windows 7 e Windows 10 di WorkSpaces) e Windows 11.
- Linux, utilizzando il`cifs-utils`strumento.
- macOS

Metodi di accesso supportati

Puoi utilizzare i metodi e gli approcci di accesso seguenti con Amazon FSx.

Accesso ai file system utilizzando i nomi DNS predefiniti

FSx for Windows File Server fornisce un nome DNS (Domain Name System) per ogni file system. Puoi accedere al file FSx for Windows File Server mappando una lettera di unità sull'istanza di calcolo alla tua condivisione di file Amazon FSx utilizzando questo nome DNS. Per ulteriori informazioni, consultare Utilizzo delle condivisioni di file di Microsoft Windows.

> **Important**
>
> Amazon FSx registra i record DNS per un file system solo se utilizzi Microsoft DNS come DNS predefinito. Se utilizzi un DNS di terze parti, devi configurare manualmente le voci DNS per i tuoi file system Amazon FSx. Per informazioni sulla scelta degli indirizzi IP corretti da utilizzare per il file system, consulta la sezioneOttenere gli indirizzi IP corretti del file system da utilizzare per il DNS.

Per trovare il nome DNS:

- Nella console Amazon FSx scegliereFile systeme quindi sceglieretDettagli. Visualizza il nome DNS nelRete e sicurezzasezione.
- Oppure, visualizzalo nella risposta delCreateFileSystemoDescribeFileSystemsComando API.

Per tutti i file system Single-AZ uniti a unAWSMicrosoft Active Directory gestito, il nome DNS è simile al seguente:`fs-0123456789abcdef0.`*`ad-dns-domain-name`*

Per tutti i file system Single-AZ uniti a un Active Directory autogestito e qualsiasi file system Multi-AZ, il nome DNS ha il seguente aspetto:`amznfsxaa11bb22.ad-domain.com`

Utilizzo di nomi DNS con Autenticazione Kerberos

Ti consigliamo di utilizzare l'autenticazione e la crittografia basate su Kerberos in transito con Amazon FSx. Kerberos fornisce l'autenticazione più sicura per i client che accedono al file system. Per abilitare l'autenticazione e la crittografia dei dati in transito basate su Kerberos per le tue sessioni SMB, usa il nome DNS del file system fornito da Amazon FSx per accedere al tuo file system.

Se disponi di un trust esterno configurato traAWSMicrosoft Active Directory gestito e Active Directory locale, per utilizzare Amazon FSx Remote PowerShell con l'autenticazione Kerberos, è necessario configurare una politica di gruppo locale sul client per l'ordine di ricerca nella foresta. Per ulteriori informazioni, consulta la paginaConfigura l'ordine di ricerca nella foresta Kerberos (KFSO)nella documentazione Microsoft.

Accesso ai file system tramite alias DNS

FSx for Windows File Server fornisce un nome DNS per ogni file system che è possibile utilizzare per accedere alle condivisioni di file. Puoi anche abilitare l'accesso ad Amazon FSx da nomi DNS diversi dal nome DNS predefinito creato da Amazon FSx registrando gli alias per i file system FSx for Windows File Server.

Utilizzando gli alias DNS, puoi spostare i dati della tua condivisione di file Windows in Amazon FSx e continuare a utilizzare i nomi DNS esistenti per accedere ai dati su Amazon FSx. Gli alias DNS consentono inoltre di utilizzare nomi significativi che semplificano l'amministrazione di strumenti e applicazioni per la connessione ai file system Amazon FSx. Per ulteriori informazioni, consulta Gestione degli alias DNS.

Utilizzo degli alias DNS con Autenticazione Kerberos

Ti consigliamo di utilizzare l'autenticazione e la crittografia basate su Kerberos in transito con Amazon FSx. Kerberos fornisce l'autenticazione più sicura per i client che accedono al file system. Per abilitare l'autenticazione Kerberos per i client che accedono ad Amazon FSx utilizzando un alias DNS, è necessario aggiungere i nomi principali di servizio (SPN) che corrispondono all'alias DNS sull'oggetto computer Active Directory del file system Amazon FSx.

Facoltativamente, è possibile imporre ai client che accedono al file system utilizzando un alias DNS di utilizzare l'autenticazione e la crittografia Kerberos impostando i seguenti Group Policy Objects (GPO) in Active Directory:

- Limita NTLM: Traffico NTLM in uscita verso server remoti- Utilizzate questa impostazione dei criteri per negare o controllare il traffico NTLM in uscita da un computer a qualsiasi server remoto che esegue il sistema operativo Windows.
- Limita NTLM: Aggiungi eccezioni del server remoto per l'autenticazione NTLM- Utilizzare questa impostazione dei criteri per creare un elenco di eccezioni di server remoti in cui i dispositivi client possono utilizzare l'autenticazione NTLM seSicurezza della rete: Limita NTLM: Traffico NTLM in uscita verso server remotil'impostazione dei criteri è configurata.

Per ulteriori informazioni, consulta Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.

Utilizzo di file system FSx for Windows File Server e i namespace DFS

FSx for Windows File Server supporta l'uso dei namespace Microsoft Distributed File System (DFS). È possibile utilizzare i namespace DFS per organizzare le condivisioni di file su più file system in un'unica struttura di cartelle comune (uno spazio dei nomi) da utilizzare per accedere all'intero set di dati di file. Puoi utilizzare un nome nel tuo Namespace DFS per accedere al file system Amazon FSx configurando la destinazione del collegamento in modo che sia il nome DNS del file system. Per ulteriori informazioni, consulta Raggruppamento di più file system con namespace DFS.

Ambienti supportati

Puoi accedere al tuo file system da risorse che si trovano nello stesso VPC del tuo file system. Per ulteriori informazioni e istruzioni dettagliate, consulta.Procedura guidata 1: Prerequisiti per iniziare.

Puoi anche accedere ai file system creati dopo il 22 febbraio 2019 da risorse locali e da risorse che si trovano in un altro VPC,AWSaccount, oAWSRegione. La tabella seguente illustra gli ambienti dai quali Amazon FSx supporta l'accesso dai client in ciascuno degli ambienti supportati, a seconda di quando è stato creato il file system.

Clienti che si trovano in...	Accesso ai file system creati prima del 22 febbraio 2019	Accesso ai file system creati prima del 17 dicembre 2020	Accesso ai file system creati dopo il 17 dicembre 2020
Sottoreti in cui viene creato il file system	✓	✓	✓
Blocchi CIDR primari del VPC in cui è stato creato il file system	✓	✓	✓
CIDR secondari del VPC in cui è stato creato il file system Altri CIDR o reti peerate		Client con indirizzi IP in RFC 1918 intervallo di indirizzi IP privati: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Client con indirizzi IP al di fuori del seguente intervallo di blocchi CIDR: 198.19.0.0/16

> **Note**
>
> In alcuni casi, potresti voler accedere a un file system creato prima del 17 dicembre 2020 da locale utilizzando un intervallo di indirizzi IP non privato. Per fare ciò, crea un nuovo file system da un backup del file system. Per ulteriori informazioni, consulta Utilizzo dei backup.

Di seguito, puoi trovare informazioni su come accedere ai file FSx for Windows File Server da locali e da diversi VPC,AWSconti, oAWSregioni.

Accesso ai file system FSx for Windows File Server da locale

FSx for Windows File Server supporta l'utilizzo diAWS Direct ConnectoAWS VPNper accedere ai file system dalle istanze di elaborazione locali. Con supporto perAWS Direct Connect, FSx for Windows File Server consente di accedere al file system tramite una connessione di rete dedicata dall'ambiente locale. Con supporto perAWS VPN, FSx for Windows File Server consente di accedere al file system dai dispositivi locali tramite un tunnel sicuro e privato.

Dopo aver collegato l'ambiente locale al VPC associato al file system Amazon FSx, puoi accedere al file system utilizzando il suo nome DNS o un alias DNS. Lo fai proprio come fai dalle istanze di calcolo all'interno del VPC. Ulteriori informazioni suAWS Direct Connect, consulta laAWS Direct ConnectGuida per l'utente di. Ulteriori informazioni sulla configurazioneAWS VPNconnessioni, consultaConnessioni VPNnelAmazon VPC User Guide.

FSx for Windows File Server supporta anche l'uso di Amazon FSx File Gateway per fornire un accesso semplice e a bassa latenza alle condivisioni di file FSx per Windows File Server nel cloud dalle istanze di elaborazione locali. Per ulteriori informazioni, consulta la paginaGuida utente di Amazon FSx File Gateway.

Accesso ai file system FSx for Windows File Server da un altro VPC, oRegione AWS

Puoi accedere al file system FSx for Windows File Server da istanze di calcolo in un VPC diversoAWSaccount, oAWSRegione di quella associata al file system. A tale scopo, puoi utilizzare i gateway di peering o di transito VPC. Quando utilizzi una connessione peering VPC o un gateway di transito per connettere i VPC, le istanze di calcolo che si trovano in un VPC possono accedere ai file system Amazon FSx in un altro VPC. Questo accesso è possibile anche se i VPC appartengono a account diversi e anche se i VPC risiedono in account diversiAWSregioni.

UNConnessione di peering di VPCè una connessione di rete tra due VPC che puoi utilizzare per instradare il traffico tra gli stessi utilizzando indirizzi IPv4 o IP versione 6 (IPv6) privati. È possibile utilizzare il peering VPC per connettere i VPC all'interno dello stessoAWSRegione o traAWSregioni. Per ulteriori informazioni sul peering VPC, consulta la paginaChe cos'è il peering VPC?nelAmazon VPC Peering Guide.

Un Transit Gateway è un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti locali. Per ulteriori informazioni sull'utilizzo dei gateway di transito VPC, consulta la paginaGuida introduttiva con gateway di transitonelAmazon VPC Transit Gateway.

Dopo aver configurato una connessione peering o gateway di transito VPC, puoi accedere al tuo file system utilizzando il suo nome DNS. Lo fai proprio come fai dalle istanze di calcolo all'interno del VPC associato.

Disponibilità e durabilità: file system Single-AZ e Multi-AZ

Amazon FSx for Windows File Server offre due tipi di implementazione di file system: Single-AZ e Multi-AZ. Le seguenti sezioni forniscono informazioni per aiutarti a scegliere il tipo di implementazione giusto per i tuoi carichi di lavoro. Per informazioni sullo SLA (Service Level Agreement) di disponibilità del servizio, consulta Amazon FSx Service Level Agreement.

I file system Single-AZ sono composti da una singola istanza di file server Windows e da un set di volumi di storage all'interno di un'unica zona di disponibilità (AZ). Con i file system Single-AZ, i dati vengono replicati automaticamente per proteggerli dal guasto di un singolo componente nella maggior parte dei casi. Amazon FSx monitora continuamente eventuali guasti hardware e ripristina automaticamente gli eventi di guasto sostituendo il componente dell'infrastruttura guasto. I file system Single-AZ sono offline, in genere per meno di 20 minuti, durante questi eventi di ripristino in caso di guasto e durante la manutenzione pianificata del file system all'interno della finestra di manutenzione configurata per il file system. Con i file system Single-AZ, l'errore del file system può essere irreversibile in rari casi, ad esempio a causa di guasti di più componenti o a causa di un errore non graduale del singolo file server che lascia il file system in uno stato incoerente, nel qual caso è possibile ripristinare il file system dal backup più recente.

I file system Multi-AZ sono composti da un cluster ad alta disponibilità di file server Windows distribuiti su due AZ (una AZ preferita e una AZ in standby), che sfruttano la tecnologia Windows Server Failover Clustering (WSFC) e un set di volumi di storage su ciascuna delle due AZ. I dati vengono replicati in modo sincrono all'interno di ogni singola AZ e tra le due AZ. Rispetto all'implementazione Single-AZ, le implementazioni Multi-AZ offrono una maggiore durabilità mediante l'ulteriore replica dei dati tra le AZ e una maggiore disponibilità durante la manutenzione pianificata del sistema e le interruzioni non pianificate del servizio mediante il failover automatico sulla zona di standby. Ciò consente di continuare ad accedere ai dati e a proteggerli dai guasti delle istanze e dalle interruzioni della fase di disponibilità.

Scelta dell'implementazione di file system Single-AZ o Multi-AZ

Consigliamo di utilizzare i file system Multi-AZ per la maggior parte dei carichi di lavoro di produzione, dato il modello ad alta disponibilità e durabilità che offre. L'implementazione Single-AZ è progettata come una soluzione conveniente per carichi di lavoro di test e sviluppo, determinati carichi di lavoro di produzione con replica integrata nel livello applicativo e che non richiedono ridondanza a livello di storage aggiuntiva e carichi di lavoro di produzione con disponibilità semplificata e esigenze di

Recovery Point Objective (RPO). I carichi di lavoro con esigenze di disponibilità ridotte possono tollerare una perdita temporanea di disponibilità per un massimo di 20 minuti in caso di manutenzione pianificata del file system o interruzione non pianificata del servizio, mentre i carichi di lavoro con esigenze RPO ridotte possono tollerare, in rari casi, la perdita degli aggiornamenti dei dati dopo il backup più recente.

Supporto delle funzionalità per tipo di implementazione

La tabella seguente riassume le funzionalità supportate dai tipi di distribuzione del file system FSx for Windows File Server:

Il tipo di distribuzione	Archiviazione SSD	Archiviazione HDD	Namespace DFS	Replica DFS	Nomi DNS personalizzati	Azioni CA
Single-AZ 1	✓		✓	✓	✓	
AZ singolo 2	✓	✓	✓		✓	✓*
Multi-AZ	✓	✓	✓		✓	✓*

> **Note**
>
> * Sebbene sia possibile creare condivisioni (CA) a disponibilità continua su file system Single-AZ 2, è necessario utilizzare le condivisioni CA su file system Multi-AZ per le implementazioni di SQL Server HA.

Processo di failover per FSx for Windows File Server

Il failover automatico dei file system Multi-AZ dal file server preferito al file server di standby si verifica in presenza di una delle seguenti condizioni:

- Si verifica un'interruzione della zona di disponibilità.
- Il file server preferito non è più disponibile.

- Il file server preferito è sottoposto a manutenzione pianificata.

Quando si esegue il failover da un file server a un altro, il nuovo file server attivo inizia automaticamente a servire tutte le richieste di lettura e scrittura del file system. Quando le risorse nella sottorete preferita sono disponibili, Amazon FSx esegue automaticamente il failback al file server preferito nella sottorete preferita. Un failover si completa in genere in meno di 30 secondi, dal rilevamento dell'errore sul file server attivo alla promozione del file server di standby allo stato attivo. Inoltre, il failback alla configurazione Multi-AZ originale viene completato in meno di 30 secondi e si verifica solo dopo il ripristino completo del file server nella sottorete preferita.

Durante il breve periodo in cui il file system è in fase di failover e failback, l'I/O potrebbe essere sospeso e i parametri di CloudWatch Amazon potrebbero essere temporaneamente non disponibili.

Per i file system Multi-AZ, se il traffico è continuo durante il failover e il failback, tutte le modifiche ai dati apportate durante questo periodo dovranno essere sincronizzate tra i file server. Questo processo può richiedere fino a diverse ore per carichi di lavoro con elevati livelli di scrittura e IOPS. Consigliamo di testare l'impatto dei failover sull'applicazione mentre il file system è sottoposto a un carico più leggero.

Esperienza di failover su client Windows

Quando si esegue il failover da un file server a un altro, il nuovo file server attivo inizia automaticamente a servire tutte le richieste di lettura e scrittura del file system. Una volta che le risorse nella sottorete preferita sono disponibili, Amazon FSx esegue automaticamente il failback sul file server preferito nella sottorete preferita. Poiché il nome DNS del file system rimane lo stesso, i failover sono trasparenti per le applicazioni Windows, che riprendono le operazioni del file system senza intervento manuale. Un failover viene in genere completato in meno di 30 secondi dal rilevamento dell'errore sul file server attivo alla promozione del file server di standby allo stato attivo. Inoltre, il failback alla configurazione Multi-AZ originale viene completato in meno di 30 secondi e si verifica solo dopo il ripristino completo del file server nella sottorete preferita.

Esperienza di failover su client Linux

I client Linux non supportano il failover automatico basato su DNS. Pertanto, non si connettono automaticamente al file server di standby durante un failover. Riprenderanno automaticamente le operazioni del file system dopo che il file system Multi-AZ avrà eseguito il failback sul file server nella sottorete preferita.

Test del failover su un file system

È possibile testare il failover del file system Multi-AZ modificandone la capacità di throughput. Quando modifichi la capacità di throughput del file system, Amazon FSx disattiva il file server del file system. I file system Multi-AZ eseguono automaticamente il failover sul server secondario, mentre Amazon FSx sostituisce per primo il file server preferito. Quindi il file system esegue automaticamente il failback sul nuovo server primario e Amazon FSx sostituisce il file server secondario.

Puoi monitorare l'avanzamento della richiesta di aggiornamento della capacità di throughput nella console Amazon FSx, nella CLI e nell'API. Una volta completato con successo l'aggiornamento, il file system viene eseguito il failover sul server secondario e il failover sul server primario. Per ulteriori informazioni sulla modifica della capacità di trasmissione del file system e sul monitoraggio dello stato di avanzamento della richiesta, consulta. Gestione della capacità di throughput

Utilizzo delle risorse del file system Single e Multi-AZ

Sottoreti

Quando crei un VPC, si estende su tutte le zone di disponibilità (AZ) della regione. Le zone di disponibilità sono sedi separate progettate per rimanere isolate dai guasti che si verificano in altre zone di disponibilità. Dopo la creazione di un VPC, puoi aggiungere una o più sottoreti in ciascuna zona di disponibilità. Il VPC predefinito ha una sottorete in ogni zona di disponibilità. Ogni sottorete deve risiedere totalmente all'interno di una zona di disponibilità e non può estendersi in altre zone. Quando crei un file system Amazon FSx Single-AZ, specifichi 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 quanto riguarda AWS le applicazioni interne, si consiglia di avviare i client nella stessa zona di disponibilità del file server preferito per ridurre al minimo la latenza.

Interfacce di rete elastiche del file system

Quando crei un file system Amazon FSx, Amazon FSx effettua il provisioning di una o più interfacce di rete elastiche nell'Amazon Virtual Private Cloud (VPC) che associ al tuo file system. L'interfaccia di

rete consente al client di comunicare con il file system FSx for Windows File Server. L'interfaccia di rete è considerata rientrante nell'ambito del servizio di Amazon FSx, nonostante faccia parte del VPC del tuo account. I file system Multi-AZ dispongono di due interfacce di rete elastiche, una per ogni file server. I file system Single-AZ dispongono di un'interfaccia di rete elastica.

> **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.

La tabella seguente riassume le risorse relative alla sottorete, all'interfaccia di rete elastica e agli indirizzi IP per i tipi di distribuzione del file system FSx for Windows File Server:

Tipo di distribuzione del file system	Numero di sottoreti	Numero di interfacce di rete elastiche	Numero di indirizzi IP
Single-AZ 2	1	1	2
AZ singolo 1	1	1	1
Multi-AZ	2	2	4

Una volta creato un file system, i suoi 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. Se un indirizzo IP elastico, che è un indirizzo IP pubblico raggiungibile da Internet, viene collegato all'interfaccia di rete elastica di un file system, Amazon FSx lo scollega automaticamente.

Ottimizzazione dei costi con Amazon FSx

FSx per Windows File Server offre diverse funzionalità che consentono di ottimizzare il costo totale di proprietà (TCO) in base alle esigenze delle applicazioni. È possibile scegliere il tipo di storage (HDD o SSD) per ottenere il giusto equilibrio tra le esigenze di costi e prestazioni della propria applicazione. Hai la flessibilità di scegliere la capacità di throughput separatamente dalla quantità di capacità di storage per ottimizzare i costi. Inoltre, è possibile utilizzare la deduplicazione dei dati per ottimizzare i costi di storage eliminando i dati ridondanti sul file system.

Argomenti

Flessibilità nella scelta dello storage e della velocità effettiva in modo indipendente

Con FSx per Windows File Server, puoi configurare lo storage, gli IOPS SSD e le capacità di throughput del tuo file system in modo indipendente. Ciò offre la flessibilità necessaria per ottenere il giusto mix di costi e prestazioni. Ad esempio, puoi scegliere di disporre di una grande quantità di storage con una capacità di throughput relativamente ridotta per carichi di lavoro freddi (generalmente inattivi) per risparmiare sui costi di throughput non necessari. Oppure, come altro esempio, è possibile scegliere di disporre di una grande capacità di throughput per una quantità relativamente piccola di capacità di archiviazione. Una maggiore capacità di throughput comporta una maggiore quantità di memoria per la memorizzazione nella cache sul file server. È possibile sfruttare la memorizzazione rapida nella cache sul file server per ottimizzare le prestazioni dei dati a cui si accede attivamente. Per ulteriori informazioni, consulta Prestazioni di FSx for Windows File Server.

È possibile aumentare la capacità di archiviazione in qualsiasi momento dopo aver creato un file system. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione. Puoi scalare gli IOPS SSD indipendentemente dalla capacità di archiviazione in qualsiasi momento dopo aver creato un file system. Per ulteriori informazioni, consulta Gestione degli IOPS SSD. È possibile aumentare o diminuire la quantità di capacità di throughput in qualsiasi momento, offrendo la flessibilità necessaria per soddisfare le mutevoli esigenze prestazionali. Per ulteriori informazioni, consulta Gestione della capacità di throughput.

Ottimizzazione dei costi di archiviazione

Puoi ottimizzare i costi di storage con Amazon FSx in diversi modi, descritti di seguito.

Ottimizzazione dei costi utilizzando i tipi di storage

FSx per Windows File Server offre due tipi di storage, unità disco rigido (HDD) e unità a stato solido (SSD), per consentire di ottimizzare costi/prestazioni per soddisfare le esigenze del carico di lavoro. Lo storage su disco rigido è progettato per un'ampia gamma di carichi di lavoro, tra cui home directory, condivisioni tra utenti e dipartimenti e sistemi di gestione dei contenuti. Lo storage SSD è progettato per i carichi di lavoro dalle prestazioni più elevate e sensibili alla latenza, inclusi database, carichi di lavoro di elaborazione multimediale e applicazioni di analisi dei dati. Per ulteriori informazioni, vedereLatenzaePrezzi di Amazon FSx per Windows File Server.

Ottimizzazione dei costi di storage mediante la deduplicazione dei dati

I set di dati di grandi dimensioni spesso contengono dati ridondanti, il che aumenta i costi di archiviazione dei dati. Ad esempio, le condivisioni di file degli utenti possono avere più copie dello stesso file, archiviate da più utenti. Le condivisioni di sviluppo software possono contenere molti file binari che rimangono invariati da una build all'altra. Puoi ridurre i costi di archiviazione dei dati attivandodeduplicazione dei datiper il tuo file system. Quando è attivata, la deduplicazione dei dati riduce o elimina automaticamente i dati ridondanti archiviando porzioni duplicate del set di dati una sola volta. Per ulteriori informazioni sulla deduplicazione dei dati e su come attivarla facilmente per il tuo file system Amazon FSx, consultaDeduplicazione dei dati.

Revisione dell'utilizzo e della fatturazione

È possibile esaminare l'utilizzo del file system, inclusa la capacità di archiviazione, la capacità di throughput, il backup e il trasferimento dei dati, utilizzandoAWS BillingDashboard oAWS Cost Explorer. Questi strumenti consentono di esaminare l'utilizzo delle risorse e di filtrare e raggruppare per tipo di utilizzo, regione e altri criteri pertinenti. Tieni presente che per visualizzare l'utilizzo di un singolo file system o di un backup di un singolo file system, dovrai abilitare i tag per quella risorsa specifica e abilitare i report di fatturazione basati su tag. Per ulteriori informazioni, vedereUsandoAWStag di allocazione dei costinelAWS Billingguida per l'utente.

Utilizzo di Microsoft Active Directory in FSx for Windows File Server

Amazon FSx funziona con Microsoft Active Directory per l'integrazione con gli ambienti Microsoft Windows esistenti. Active Directory è il servizio di directory di Microsoft utilizzato per archiviare informazioni sugli oggetti sulla rete e semplificare la ricerca e l'utilizzo di tali informazioni da parte di amministratori e utenti. Questi oggetti includono in genere risorse condivise come file server e account di utenti e computer di rete.

Quando crei un file system con Amazon FSx, lo aggiungi al tuo dominio Active Directory per fornire l'autenticazione degli utenti e il controllo degli accessi a livello di file e cartella. I tuoi utenti possono quindi utilizzare le loro identità utente esistenti in Active Directory per autenticarsi e accedere al file system Amazon FSx. Gli utenti possono anche utilizzare le identità esistenti per controllare l'accesso a singoli file e cartelle. Inoltre, puoi migrare i file e le cartelle esistenti e la configurazione della lista di controllo degli accessi di sicurezza (ACL) di questi elementi su Amazon FSx senza alcuna modifica.

Amazon FSx offre due opzioni per utilizzare il file system FSx for Windows File Server con Active Directory: e. Utilizzo di Amazon FSx con AWS Directory Service for Microsoft Active Directory Utilizzo di Amazon FSx con Microsoft Active Directory autogestito

> **Note**
>
> Amazon FSx supporta Microsoft Azure Active Directory Domain Services, a cui puoi aggiungere un Microsoft Azure Active Directory.

Dopo aver creato una configurazione Active Directory unita per un file system, puoi aggiornare solo le seguenti proprietà:

- Credenziali utente del servizio
- Indirizzi IP del server DNS

Non è possibile modificare le seguenti proprietà per l'utente iscritto a Microsoft AD dopo aver creato il file system:

- DomainName

- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

Tuttavia, è possibile creare un nuovo file system da un backup e modificare queste proprietà nella configurazione di integrazione di Microsoft Active Directory per il nuovo file system. Per ulteriori informazioni, consulta Procedura guidata 2: Creare un file system da un backup.

> **Note**
>
> Amazon FSx non supporta Active Directory Connector e Simple Active Directory.

L'FSx for Windows File Server potrebbe non essere configurato correttamente se si verifica una modifica nella configurazione di Active Directory che interrompe la connessione al file system. Per riportare il file system allo stato Available, seleziona il pulsante Attempt Recovery nella console Amazon FSx o usa il `StartMisconfiguredStateRecovery` comando nell'API o nella console Amazon FSx. Per ulteriori informazioni, consulta Il file system è in uno stato configurato in modo errato.

Argomenti

- Utilizzo di Amazon FSx con AWS Directory Service for Microsoft Active Directory
- Utilizzo di Amazon FSx con Microsoft Active Directory autogestito

Utilizzo di Amazon FSx con AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) fornisce directory Active Directory effettive, completamente gestite, ad alta disponibilità e nel cloud. È possibile utilizzare queste directory di Active Directory nella distribuzione del carico di lavoro.

Se la tua organizzazione utilizza AWS Managed Microsoft AD la gestione di identità e dispositivi, ti consigliamo di integrare il file system Amazon FSx con. AWS Managed Microsoft AD In questo modo, ottieni una soluzione chiavi in mano che utilizza Amazon AWS Managed Microsoft AD FSx con. AWS gestisce l'implementazione, il funzionamento, l'alta disponibilità, l'affidabilità, la sicurezza e la perfetta integrazione dei due servizi, consentendoti di concentrarti sulla gestione efficace del tuo carico di lavoro.

Per utilizzare Amazon FSx con la tua AWS Managed Microsoft AD configurazione, puoi utilizzare la console Amazon FSx. Quando create un nuovo file system FSx for Windows File Server nella console, AWS scegliete Managed Active Directory nella sezione Autenticazione di Windows. Scegliete anche la directory specifica che desiderate utilizzare. Per ulteriori informazioni, consulta Crea il tuo file system.

L'organizzazione potrebbe gestire identità e dispositivi su un dominio Active Directory autogestito (in locale o nel cloud). In tal caso, puoi aggiungere il tuo file system Amazon FSx direttamente al tuo dominio Active Directory esistente e autogestito. Per ulteriori informazioni, consulta Utilizzo di Amazon FSx con Microsoft Active Directory autogestito.

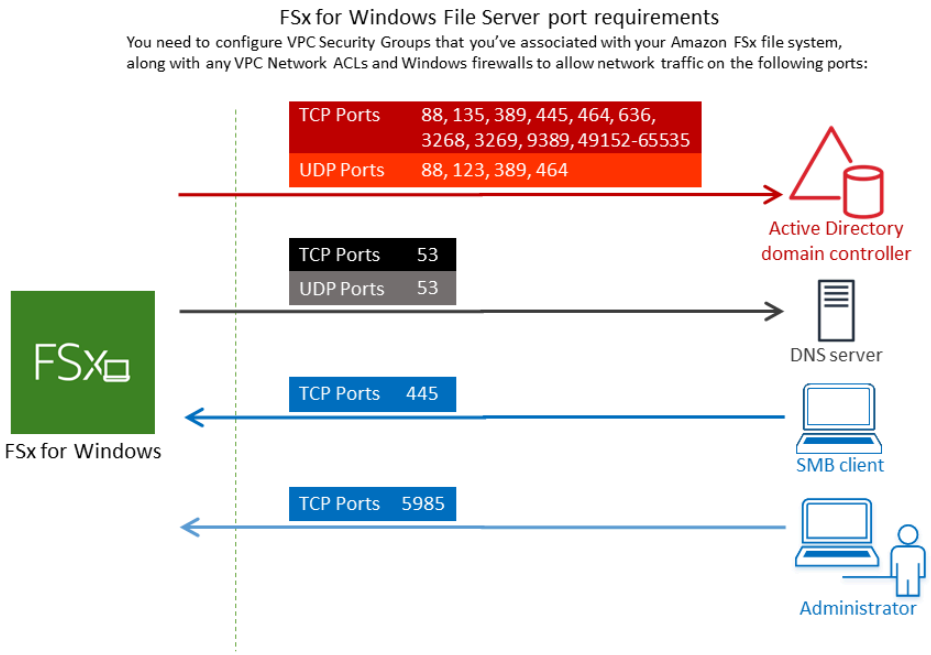
Inoltre, puoi anche configurare il tuo sistema in modo da trarre vantaggio da un modello di isolamento delle foreste di risorse. In questo modello, si isolano le risorse, inclusi i file system Amazon FSx, in una foresta Active Directory separata da quella in cui si trovano gli utenti.

> **Important**
>
> Per Single-AZ 2 e tutti i file system Multi-AZ, il nome di dominio Active Directory non può superare i 47 caratteri.

Prerequisiti di rete

Prima di creare un file system FSx for Windows File Server aggiunto al dominio AWS Microsoft Managed Active Directory, assicuratevi di aver creato e impostato le seguenti configurazioni di rete:

- Per i gruppi di sicurezza VPC, il gruppo di sicurezza predefinito per il tuo Amazon VPC predefinito è già aggiunto al file system nella console. Assicurati che il gruppo di sicurezza e gli ACL di rete VPC per le sottoreti in cui stai creando il file system FSx consentano il traffico sulle porte e nelle direzioni mostrate nel diagramma seguente.



Nella tabella seguente è indicato il ruolo di ciascuna porta.

Protocollo	Porte	Ruolo
TCP/UDP	53	Doma Name Syste (DNS)
TCP/UDP	88	Auten zione Kerbe
TCP/UDP	464	Modifi reimp zione della passw

Protocollo	Porte	Ruolo
TCP/UDP	389	Lightw ht Direct Acces Protoc
UDP	123	Netwo Time Protoc (NTP)
TCP	135	Distrib ed Comp Enviro nt/ End Point Mappe (DCE/ EPMA P)
TCP	445	Condi one di file SMB di Serviz direct

Protocollo	Porte	Ruolo
TCP	636	Lightw ht Direct Acces Protoc su TLS/ SSL (LDAP
TCP	3268	Catalo global Micros
TCP	3269	Micros Globa Catalo tramit SSL
TCP	5985	WinRI 2.0 (gesti remot di Micros Windo
TCP	9389	Serviz Web Micros AD DS, Power

Protocollo	Porte	Ruolo
TCP	49152 - 65535	Porte effime per RPC

> **Important**
>
> L'autorizzazione del traffico in uscita sulla porta TCP 9389 è necessaria per le implementazioni di file system Single-AZ 2 e Multi-AZ.

> **Note**
>
> Se utilizzi ACL di rete VPC, devi anche consentire il traffico in uscita su porte dinamiche (49152-65535) dal tuo file system FSx.

- Se stai connettendo il tuo file system Amazon FSx a un AWS Microsoft Active Directory gestito in un VPC o account diverso, assicurati la connettività tra quel VPC e l'Amazon VPC in cui desideri creare il file system. Per ulteriori informazioni, consulta Utilizzo di Amazon FSx con un AWS Managed Microsoft AD altro VPC o account.

> **Important**
>
> Mentre i gruppi di sicurezza Amazon VPC richiedono l'apertura delle porte solo nella direzione in cui viene avviato il traffico di rete, gli ACL di rete VPC richiedono che le porte siano aperte in entrambe le direzioni.

Utilizza lo strumento di convalida della rete Amazon FSx per convalidare la connettività ai controller di dominio Active Directory.

Utilizzo di un modello di isolamento delle foreste di risorse

Si unisce il file system a una AWS Managed Microsoft AD configurazione. Si stabilisce quindi una relazione di trust forestale unidirezionale tra un AWS Managed Microsoft AD dominio creato

dall'utente e il dominio Active Directory autogestito esistente. Per l'autenticazione Windows in Amazon FSx, è necessario solo un trust di foresta direzionale unidirezionale, in cui la foresta AWS gestita si fida della foresta di dominio aziendale.

Il tuo dominio aziendale assume il ruolo di dominio affidabile e il dominio AWS Directory Service gestito assume il ruolo di dominio affidabile. Le richieste di autenticazione convalidate viaggiano tra i domini in una sola direzione, consentendo agli account del dominio aziendale di autenticarsi con le risorse condivise nel dominio gestito. In questo caso, Amazon FSx interagisce solo con il dominio gestito. Il dominio gestito trasmette quindi le richieste di autenticazione al dominio aziendale.

Verifica la configurazione di Active Directory

Prima di creare il file system Amazon FSx, ti consigliamo di convalidare la connettività ai controller di dominio Active Directory utilizzando lo strumento di convalida della rete Amazon FSx. Per ulteriori informazioni, consulta Convalida della connettività ai controller di dominio Active Directory.

Le seguenti risorse correlate possono esservi utili durante l'utilizzo AWS Directory Service for Microsoft Active Directory con FSx for Windows File Server:

- Cos'è il AWS Directory Service nella Guida all'AWS Directory Service amministrazione
- Crea la tua Active Directory AWS gestita nella Guida all'AWS Directory Service amministrazione
- Quando creare una relazione di fiducia nella Guida all'AWS Directory Service amministrazione
- Procedura guidata 1: Prerequisiti per iniziare

Utilizzo di Amazon FSx con un AWS Managed Microsoft AD altro VPC o account

È possibile unire il file system FSx for Windows File Server a AWS Managed Microsoft AD una directory che si trova in un VPC diverso all'interno dello stesso account utilizzando il peering VPC. È inoltre possibile unire il file system a una AWS Managed Microsoft AD directory che si trova in un AWS account diverso utilizzando la condivisione delle directory.

> **Note**
>
> È possibile selezionarne solo uno AWS Managed Microsoft AD all'interno dello Regione AWS stesso file system. Se desideri utilizzare una configurazione di peering VPC interregionale,

devi usare una Microsoft Active Directory autogestita. Per ulteriori informazioni, consulta Utilizzo di Amazon FSx con Microsoft Active Directory autogestito.

Il flusso di lavoro per unire il file system a un AWS Managed Microsoft AD altro VPC prevede i seguenti passaggi:

1. Configura il tuo ambiente di rete.
2. Condividi la tua rubrica.
3. Unisci il tuo file system alla directory condivisa.

Per ulteriori informazioni, consulta Condividere la directory nella Guida all'AWS Directory Service amministrazione.

Per configurare il tuo ambiente di rete puoi utilizzare AWS Transit Gateway Amazon VPC e creare una connessione peering VPC. Inoltre, assicurati che il traffico di rete sia consentito tra i due VPC.

Un Transit Gateway è un hub di transito di rete che è possibile utilizzare per collegare i VPC e le reti locali. Per ulteriori informazioni sull'utilizzo di VPC Transit Gateway, consulta l'argomento relativo alle nozioni di base su Transit Gateway nella Guida di Amazon VPC Transit Gateway.

Una connessione di peering VPC è una connessione di rete tra due VPC. Questa connessione consente di instradare il traffico tra di essi utilizzando indirizzi privati del protocollo Internet versione 4 (IPv4) o del protocollo Internet versione 6 (IPv6) privati. Puoi utilizzare il peering VPC per connettere VPC all'interno della stessa AWS regione o tra regioni. AWS Per ulteriori informazioni, consulta Che cos'è il peering di VPC? nella Guida al peering di Amazon VPC.

Esiste un altro prerequisito quando si collega il file system a una AWS Managed Microsoft AD directory con un account diverso da quello del file system. È inoltre necessario condividere Microsoft Active Directory con l'altro account. A tale scopo, è possibile utilizzare la funzionalità di condivisione delle directory di AWS Managed Microsoft Active Directory. Per ulteriori informazioni, consulta Condividere la directory nella Guida all'AWS Directory Service amministrazione.

Convalida della connettività ai controller di dominio Active Directory

Prima di creare un file system FSx for Windows File Server unito ad Active Directory, utilizza lo strumento Amazon FSx Active Directory Validation per convalidare la connettività al tuo dominio Active Directory. È possibile utilizzare questo test se si utilizza FSx for Windows File Server AWS con Microsoft Active Directory gestito o con una configurazione Active Directory autogestita. Il test

Domain Controller Network Connectivity (Test-FSXADControllerConnection) non esegue la suite completa di controlli della connettività di rete su ogni controller di dominio del dominio. Utilizzate invece questo test per eseguire la convalida della connettività di rete su un set specifico di controller di dominio.

Per convalidare la connettività ai controller di dominio Active Directory

1. Avvia un'istanza Amazon EC2 Windows nella stessa sottorete e con gli stessi gruppi di sicurezza Amazon VPC che utilizzerai per il tuo file system FSx for Windows File Server. Per i tipi di implementazione Multi-AZ, utilizza la sottorete per il file server attivo preferito.
2. Unisci la tua istanza EC2 per Windows ad Active Directory. Per ulteriori informazioni, consulta Aggiungere manualmente un'istanza Windows nella Guida all'AWS Directory Service amministrazione.
3. Connettiti all'istanza EC2. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
4. Apri una PowerShell finestra Windows (utilizzando Esegui come amministratore) sull'istanza EC2.

   Per verificare se il modulo Active Directory richiesto per Windows PowerShell è installato, usa il seguente comando test.

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   Se quanto sopra restituisce un errore, installalo utilizzando il seguente comando.

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```
5. Scaricate lo strumento di convalida della rete utilizzando il seguente comando.

   ```
   PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/WindowsGuide/
   samples/AmazonFSxADValidation.zip" -OutFile "AmazonFSxADValidation.zip"
   ```
6. Espandi il file zip utilizzando il seguente comando.

   ```
   PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
   ```

7. Aggiungi il modulo AmazonFSXADValidation alla sessione corrente.

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. Imposta il valore per l'indirizzo IP del controller di dominio Active Directory ed esegui il test di connettività utilizzando i seguenti comandi:

```
$ADControllerIp = '10.0.75.243'
$Result = Test-FSxADControllerConnection -ADControllerIp $ADControllerIp
```

9. L'esempio seguente mostra il recupero dell'output del test, con i risultati di un test di connettività riuscito.

```
PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                         10.0.75.243
UdpDetails                     {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                        True


PS C:\AmazonFSxADValidation> $Result.TcpDetails

Port Result    Description
---- ------    -----------
  88 Listening Kerberos authentication
 135 Listening DCE / EPMAP (End Point Mapper)
 389 Listening Lightweight Directory Access Protocol (LDAP)
 445 Listening Directory Services SMB file sharing
 464 Listening Kerberos Change/Set password
 636 Listening Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
3268 Listening Microsoft Global Catalog
3269 Listening Microsoft Global Catalog over SSL
9389 Listening Microsoft AD DS Web Services, PowerShell
```

L'esempio seguente mostra l'esecuzione del test e l'ottenimento di un risultato negativo.

```
PS C:\AmazonFSxADValidation> $Result = Test-FSxADControllerConnection -
ADControllerIp $ADControllerIp
WARNING: TCP 9389 failed to connect. Required for Microsoft AD DS Web Services,
 PowerShell.
Verify security group and firewall settings on both client and directory
 controller.
WARNING: 1 ports failed to connect to 10.0.75.243. Check pre-requisites in
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html#self-
manage-prereqs

PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                         10.0.75.243
UdpDetails                     {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                        False
FailedTcpPorts                 {9389}


PS C:\AmazonFSxADValidation> $Result.FailedTcpPorts
9389
```

Windows socket error code mapping

https://msdn.microsoft.com/en-us/library/ms740668.aspx

Utilizzo di Amazon FSx con Microsoft Active Directory autogestito

Se la tua organizzazione gestisce identità e dispositivi su un Active Directory autogestito in locale o nel cloud, puoi aggiungere il tuo file system Amazon FSx direttamente al tuo dominio Active Directory autogestito esistente. Per usare Amazon FSx con AWS Managed Microsoft AD, puoi usare la console Amazon FSx. Quando create un nuovo file system FSx for Windows File Server nella console,

scegliete Microsoft Active Directory autogestito in Autenticazione Windows. Fornisci i seguenti dettagli per il tuo Active Directory autogestito:

- Un nome di dominio completo per la tua directory autogestita

> **Note**
>
> Il nome di dominio non deve essere nel formato SLD (Single Label Domain). Amazon FSx attualmente non supporta i domini SLD.

> **Note**
>
> Per i file system Single-AZ 2 e Multi-AZ, il nome di dominio Active Directory non può superare i 47 caratteri.

- Indirizzi IP del server DNS per il tuo dominio

  Gli indirizzi IP del server DNS, gli indirizzi IP dei controller di dominio Active Directory e la rete client devono soddisfare i seguenti requisiti:

Per i file system creati prima del 17 dicembre 2020	Per i file system creati dopo il 17 dicembre 2020
Gli indirizzi IP devono rientrare in un intervallo di indirizzi IP privati RFC 1918: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Gli indirizzi IP possono rientrare in qualsiasi intervallo, ad eccezione di: • Indirizzi IP in conflitto con gli indirizzi IP di proprietà di Amazon Web Services in quella AWS regione. Per un elenco di indirizzi IP di AWS proprietà per regione, consulta gli intervalli di indirizzi AWS IP. • Indirizzi IP nel seguente intervallo di blocchi CIDR: 198.19.0.0/16

> **Note**
>
> I controller di dominio Active Directory devono essere scrivibili.

- Nome utente e password per un account di servizio sul tuo dominio Active Directory, da utilizzare per Amazon FSx per aggiungere il file system al tuo dominio Active Directory
- (Facoltativo) L'unità organizzativa (OU) del dominio a cui desideri aggiungere il file system
- (Facoltativo) Il gruppo di dominio a cui si desidera delegare l'autorità per eseguire azioni amministrative sul file system. Ad esempio, questo gruppo di domini potrebbe gestire le condivisioni di file Windows, gestire gli Access Control List (ACL) nella cartella principale del file system, assumere 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.

> **Note**
>
> Il nome del gruppo di dominio che fornisci deve essere univoco nel tuo Active Directory. FSx for Windows File Server non creerà il gruppo di domini nelle seguenti circostanze:
>
> - Se esiste già un gruppo con il nome specificato
> - Se non specifichi un nome e un gruppo denominato «Domain Admins» esiste già in Active Directory.

Per ulteriori informazioni, consulta Unire un file system Amazon FSx a un dominio Microsoft Active Directory autogestito.

> **Important**
>
> Amazon FSx registra i record DNS per un file system solo se utilizzi Microsoft DNS come servizio DNS predefinito. Se utilizzi un DNS di terze parti, dovrai configurare manualmente le voci DNS per i tuoi file system Amazon FSx dopo averli creati.

Quando si aggiunge il file system direttamente all'Active Directory autogestito, il file server FSx for Windows risiede nella stessa foresta di Active Directory (il contenitore logico principale in una

configurazione di 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).

> **Note**
>
> Puoi isolare le tue risorse, inclusi i file system Amazon FSx, in una foresta Active Directory separata da quella in cui risiedono gli utenti. A tale scopo, unisci il tuo file system a una Active Directory AWS gestita e stabilisci una relazione di trust forestale unidirezionale tra un'Active Directory gestita da te e la tua Active Directory AWS autogestita esistente.

Argomenti

Prerequisiti per l'utilizzo di un Microsoft Active Directory autogestito

Prima di creare un file system Amazon FSx aggiunto al tuo dominio Microsoft Active Directory autogestito, esamina i seguenti prerequisiti.

Argomenti

Configurazioni locali

Assicurati di disporre di un sistema Microsoft Active Directory locale o autogestito a cui aggiungere il file system Amazon FSx. Il tuo Active Directory locale dovrebbe avere la seguente configurazione:

- Il controller di dominio Active Directory ha un livello di funzionalità del dominio pari a Windows Server 2008 R2 o superiore.
- Gli indirizzi IP del server DNS e gli indirizzi IP del controller di dominio Active Directory sono i seguenti, a seconda di quando è stato creato il file system:

Per i file system creati prima del 17 dicembre 2020	Per i file system creati dopo il 17 dicembre 2020
Gli indirizzi IP devono rientrare in un intervallo di indirizzi IP privati RFC 1918: • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	Gli indirizzi IP possono rientrare in qualsiasi intervallo, ad eccezione di: • Indirizzi IP in conflitto con gli indirizzi IP di proprietà di Amazon Web Services in quella AWS regione. Per un elenco di indirizzi IP di AWS proprietà per regione, consulta gli intervalli di indirizzi AWS IP. • Indirizzi IP nel seguente intervallo di blocchi CIDR: 198.19.0.0/16

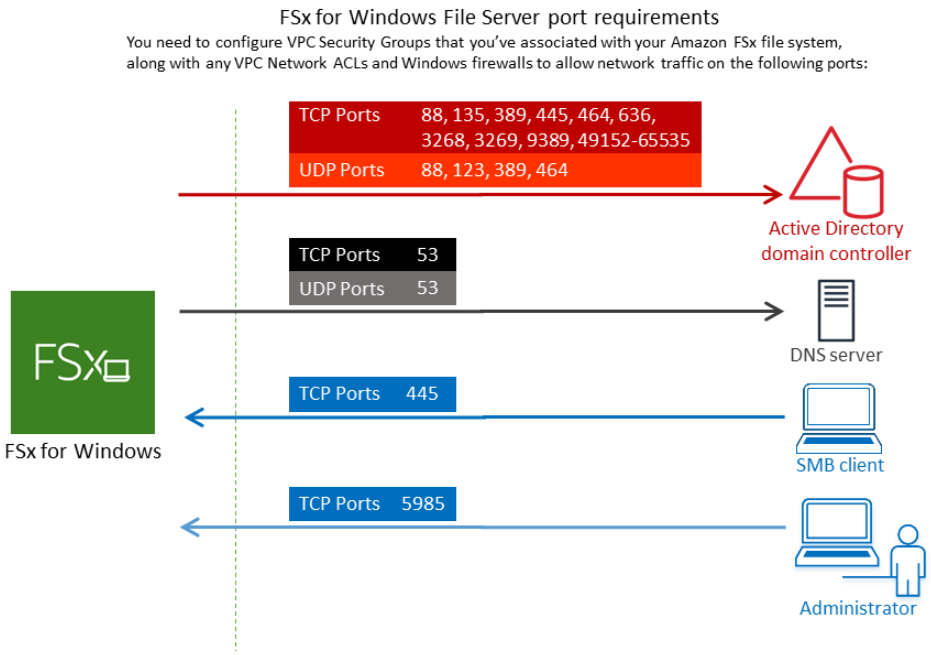
  Se è necessario accedere a un file system FSx for Windows File Server creato prima del 17 dicembre 2020 utilizzando un intervallo di indirizzi IP non privato, è possibile creare un nuovo file system ripristinando un backup del file system. Per ulteriori informazioni, consulta Utilizzo dei backup.
- Un nome di dominio che non è in formato SLD (Single Label Domain). Amazon FSx non supporta i domini SLD.
- Per Single-AZ 2 e tutti i file system Multi-AZ, il nome di dominio Active Directory non può superare i 47 caratteri.
- Se hai definito siti Active Directory, le sottoreti nel VPC associato al tuo file system Amazon FSx devono essere definite in un sito Active Directory e non devono esistere conflitti tra le sottoreti nel tuo VPC e le sottoreti negli altri siti.
- Potrebbe essere necessario aggiungere regole al firewall per consentire il traffico ICMP tra i controller di dominio Active Directory e Amazon FSx.

Configurazioni di rete

Questa sezione descrive le configurazioni di rete necessarie per aggiungere un file system all'Active Directory autogestito.

Ti consigliamo di utilizzare lo strumento di convalida Amazon FSx Active Directory per testare le impostazioni di rete prima di tentare di unire il tuo file system all'Active Directory autogestito.

- La connettività deve essere configurata tra l'Amazon VPC in cui desideri creare il file system e il tuo Active Directory autogestito. È possibile configurare questa connettività utilizzando AWS Direct Connect, AWS Virtual Private Network, il peering VPC o. AWS Transit Gateway
- Per i gruppi di sicurezza VPC, il gruppo di sicurezza predefinito per il tuo Amazon VPC predefinito deve essere aggiunto al file system nella console. Assicurati che il gruppo di sicurezza e gli ACL di rete VPC per le sottoreti in cui crei il file system FSx consentano il traffico sulle porte e nelle direzioni mostrate nel diagramma seguente.



Nella tabella seguente è indicato il ruolo di ciascuna porta.

Protocollo	Porte	Ruolo
TCP/UDP	53	Domain Name System (DNS)
TCP/UDP	88	Autenticazione Kerberos
TCP/UDP	464	Modifica/imposta la password
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)
UDP	123	Network Time Protocol (NTP)
TCP	135	Ambiente di calcolo distribuito/End Point Mapper (DCE/EPMAP)
TCP	445	Condivisione di file SMB di Servizi directory
TCP	636	Lightweight Directory Access Protocol su TLS/SSL (LDAPS)
TCP	3268	Catalogo globale Microsoft
TCP	3269	Microsoft Global Catalog tramite SSL
TCP	5985	WinRM 2.0 (gestione remota di Microsoft Windows)
TCP	9389	Servizi Web Microsoft Active Directory DS, PowerShell
TCP	49152 - 65535	Porte effimere per RPC

Assicurati che queste regole del traffico siano rispecchiate anche sui firewall che si applicano a ciascuno dei controller di dominio Active Directory, server DNS, client FSx e amministratori FSx.

> **Important**
>
> L'autorizzazione del traffico in uscita sulla porta TCP 9389 è necessaria per le implementazioni di file system Single-AZ 2 e Multi-AZ.

> **Note**
>
> Se utilizzi ACL di rete VPC, devi anche consentire il traffico in uscita su porte dinamiche (49152-65535) dal tuo file system FSx.

> **Important**
>
> Sebbene i gruppi di sicurezza Amazon VPC richiedano l'apertura delle porte solo nella direzione di avvio del traffico di rete, la maggior parte dei firewall Windows e degli ACL di rete VPC richiedono che le porte siano aperte in entrambe le direzioni.

Autorizzazioni dell'account di servizio

Assicurati di avere un account di servizio nel tuo Microsoft Active Directory autogestito con autorizzazioni delegate per aggiungere computer al dominio. Un account di servizio è un account utente in Microsoft 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 al file system:

- Possibilità di reimpostare le password
- Possibilità di impedire agli account di leggere e scrivere dati
- Capacità convalidata di scrivere sul nome host DNS
- Capacità convalidata di scrivere sul nome principale del servizio
- Capacità (può essere delegata) di creare ed eliminare oggetti informatici
- Capacità convalidata di leggere e scrivere le restrizioni relative all'account
- Possibilità di modificare le autorizzazioni

Rappresentano il set minimo di autorizzazioni necessarie per unire gli oggetti del computer ad Active Directory. Per ulteriori informazioni, vedere l'argomento della documentazione di Microsoft Windows Server Errore: accesso negato quando utenti non amministratori a cui è stato delegato il controllo tentano di aggiungere computer a un controller di dominio.

Per ulteriori informazioni sulla creazione di un account di servizio con le autorizzazioni corrette, vedere. Delega dei privilegi al tuo account di servizio Amazon FSx

Amazon FSx richiede un account di servizio valido per tutta la durata del file system Amazon FSx. Amazon FSx deve essere in grado di gestire completamente il file system ed eseguire attività che richiedono l'eliminazione e il ricongiungimento al dominio Active Directory utilizzando l'account di servizio. Queste attività includono la sostituzione di un file server guasto o l'applicazione di patch al software Windows Server. È fondamentale mantenere aggiornata la configurazione di Active Directory, incluse le credenziali dell'account di servizio, con Amazon FSx. Per ulteriori informazioni, consulta Mantenere aggiornata la configurazione di Active Directory.

Amazon FSx richiede la connettività a tutti i controller di dominio nell'ambiente Active Directory. Se disponi di più controller di dominio, assicurati che tutti soddisfino i requisiti di cui sopra e assicurati che eventuali modifiche al tuo account di servizio vengano propagate a tutti i controller di dominio.

Puoi convalidare la configurazione di Active Directory, incluso il test della connettività di più controller di dominio, utilizzando lo strumento di convalida Active Directory di Amazon FSx. Per limitare il numero di controller di dominio che richiedono connettività, puoi anche creare una relazione di fiducia tra i controller di dominio locali e. AWS Managed Microsoft AD Per ulteriori informazioni, consulta Utilizzo di un modello di isolamento delle foreste di risorse.

> **Important**
>
> Non spostare oggetti informatici creati da Amazon FSx nell'unità organizzativa dopo la creazione del file system. In questo modo il file system verrà configurato in modo errato.

Procedure consigliate per unire i file system FSx for Windows File Server a un dominio Microsoft Active Directory autogestito

Consigliamo queste best practice per unire i sistemi file Amazon FSx for Windows File Server al tuo Microsoft Active Directory autogestito.

Delega dei privilegi al tuo account di servizio Amazon FSx

Assicurati di configurare l'account di servizio che fornisci ad Amazon FSx con i privilegi minimi richiesti. Inoltre, separa l'unità organizzativa (OU) dagli altri controller di dominio.

Per aggiungere i file system Amazon FSx al tuo dominio, assicurati che l'account di servizio disponga di privilegi delegati. I membri del gruppo Domain Admins dispongono di privilegi sufficienti per eseguire questa attività. Tuttavia, è consigliabile utilizzare un account di servizio che disponga solo

dei privilegi minimi necessari per eseguire questa operazione. Le seguenti procedure mostrano come delegare solo i privilegi necessari per unire i file system Amazon FSx al tuo dominio.

È possibile utilizzare Delegate Control o Advanced Features nello snap-in MMC Active Directory User and Computers per assegnare queste autorizzazioni.

Eseguire una di queste procedure su un computer collegato ad Active Directory su cui è installato lo snap-in. Active Directory User and Computers MMC

Per assegnare le autorizzazioni a un account o a un gruppo di servizio utilizzando Delegate Control

1. Accedi al tuo sistema come amministratore di dominio per il tuo dominio Active Directory.
2. Aprire lo snap-in MMC 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 il nome del tuo account o gruppo di servizi Amazon FSx, quindi scegli Avanti.
7. Nella pagina Tasks to Delegate (Operazioni da delegare), selezionare Create a custom task to delegate (Crea un'operazione personalizzata per eseguire la delega), quindi scegliere Next (Avanti).
8. Scegli Solo i seguenti oggetti nella cartella, quindi scegli Oggetti computer.
9. Scegliete Crea oggetti selezionati in questa cartella e Elimina gli oggetti selezionati in questa cartella. Quindi scegli Successivo.
10. 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
11. Scegli Next (Avanti), quindi scegli Finish (Fine).
12. Chiudere lo snap-in MMC Utente e computer di Active Directory.

Per assegnare le autorizzazioni utilizzando le funzionalità avanzate

1. Accedi al tuo sistema come amministratore di dominio per il tuo dominio Active Directory.
2. Aprire lo snap-in MMC Utenti e computer di Active Directory.
3. Seleziona Visualizza dalla barra dei menu e assicurati che Advanced Features sia abilitata (accanto all'opzione comparirà un segno di spunta se la funzionalità è abilitata).
4. Nel riquadro attività, espandi il nodo del dominio.
5. Individua e apri (fai clic con il pulsante destro del mouse) il menu di scelta rapida dell'unità organizzativa che desideri modificare, quindi scegli Proprietà.
6. Nel riquadro Proprietà dell'unità organizzativa, selezionare la scheda Sicurezza.
7. Nella scheda Sicurezza, selezionare Avanzate. Quindi seleziona Aggiungi.
8. Nella pagina Immissione delle autorizzazioni, scegli Seleziona un principale e inserisci il nome del tuo account o gruppo di servizi Amazon FSx. Per Si applica a:, scegli gli oggetti Descendant Computer. Assicuratevi che siano selezionati i seguenti elementi:
   - Modifica le autorizzazioni
   - Crea oggetti informatici
   - Eliminare oggetti del computer
9. Seleziona Applica, quindi seleziona OK.
10. Chiudere lo snap-in MMC Utente e computer di Active Directory.

> **Important**
>
> Non spostare oggetti informatici creati da Amazon FSx nell'unità organizzativa dopo la creazione del file system. In questo modo il file system verrà configurato in modo errato. Se aggiorni il file system con un nuovo account di servizio, assicurati che il nuovo account di servizio disponga delle autorizzazioni di controllo completo per gli oggetti informatici esistenti associati al file system.

Mantenere aggiornata la configurazione di Active Directory

Per garantire la disponibilità continua e ininterrotta del file system Amazon FSx, è necessario aggiornare la configurazione di Active Directory del file system ogni volta che si apportano modifiche alla configurazione di Active Directory autogestita.

Ad esempio, se Active Directory utilizza una politica di reimpostazione della password basata sul tempo, non appena la password viene reimpostata, assicurati di aggiornare la password dell'account del servizio con Amazon FSx. 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. Per ulteriori informazioni, consulta Aggiornamento della configurazione di Active Directory autogestita.

Quando aggiorni la configurazione autogestita di Active Directory per il tuo file system Amazon FSx, lo stato del file system passa da Disponibile a Aggiornamento durante l'applicazione dell'aggiornamento. Verifica che lo stato torni a Disponibile dopo l'applicazione dell'aggiornamento: tieni presente che il completamento dell'aggiornamento può richiedere fino a diversi minuti. Per ulteriori informazioni, consulta Monitoraggio degli aggiornamenti di Active Directory gestiti autonomamente.

Se c'è un problema con la configurazione aggiornata di Active Directory autogestita, lo stato del file system passa a Configurato erroneamente. Questo stato mostra un messaggio di errore e l'azione correttiva consigliata accanto alla descrizione del file system nella console, nell'API e nella CLI. Dopo aver intrapreso l'azione correttiva consigliata, verifica che lo stato del file system passi infine a Disponibile.

Per ulteriori informazioni sulla risoluzione di possibili configurazioni errate di Active Directory autogestite, consulta. Il file system è in uno stato configurato in modo errato

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, è possibile limitare i privilegi al minimo necessario. Per fare ciò, usa le regole del gruppo di sicurezza. Per ulteriori informazioni, vedi Gruppi di sicurezza Amazon VPC.

Creazione di regole per i gruppi di sicurezza in uscita per l'interfaccia di rete del file system

Per una maggiore sicurezza, prendi in considerazione la configurazione di un gruppo di sicurezza con regole del traffico in uscita. Queste regole dovrebbero consentire il traffico in uscita solo verso i controller di domini Microsoft Active Directory autogestiti o all'interno della sottorete o del gruppo di sicurezza. Applica questo gruppo di sicurezza al VPC associato all'interfaccia di rete elastica del tuo file system Amazon FSx. Per ulteriori informazioni, consulta Controllo degli accessi ai file system con Amazon VPC.

Convalida della configurazione di Active Directory

Prima di creare un file system FSx for Windows File Server unito ad Active Directory, ti consigliamo di convalidare la configurazione di Active Directory utilizzando lo strumento di convalida Amazon FSx Active Directory. Tieni presente che la connettività Internet in uscita è necessaria per convalidare correttamente la configurazione di Active Directory.

Per convalidare la configurazione di Active Directory

1. Avvia un'istanza Amazon EC2 per Windows nella stessa sottorete e con gli stessi gruppi di sicurezza Amazon VPC utilizzati per il file system FSx for Windows File Server. Assicurati che la tua istanza EC2 disponga delle autorizzazioni IAM richieste. `AmazonEC2ReadOnlyAccess` Puoi convalidare le autorizzazioni del ruolo dell'istanza EC2 utilizzando il simulatore di policy IAM. Per ulteriori informazioni, consulta Testing IAM Policies with the IAM Policy Simulator nella IAM User Guide.
2. Unisci la tua istanza EC2 per Windows alla tua Active Directory. Per ulteriori informazioni, consulta Aggiungere manualmente un'istanza Windows nella Guida all'AWS Directory Service amministrazione.
3. Connettiti all'istanza EC2. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
4. Apri una PowerShell finestra Windows (utilizzando Esegui come amministratore) sull'istanza EC2.

   Per verificare se il modulo Active Directory richiesto per Windows PowerShell è installato, usa il seguente comando test.

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   Se quanto sopra restituisce un errore, installalo utilizzando il seguente comando.

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```
5. Scaricate lo strumento di convalida della rete utilizzando il seguente comando.

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

6. Espandi il file zip utilizzando il seguente comando.

```
PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
```

7. Aggiunge il `AmazonFSxADValidation` modulo alla sessione corrente.

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. Imposta i parametri richiesti sostituendo nel seguente comando il tuo:

   - *Nome di dominio Active Directory (DOMAINNAME.COM)*
   - Preparare l'`$Credential`oggetto per la password dell'account del servizio utilizzando una delle seguenti opzioni.
     - Per generare l'oggetto credenziale in modo interattivo, utilizzate il comando seguente.

       ```
       $Credential = Get-Credential
       ```

     - Per generare l'oggetto credenziale utilizzando una AWS Secrets Manager risorsa, utilizzate il comando seguente.

       ```
       $Secret = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
        $AdminSecret).SecretString
       $Credential = (New-Object PSCredential($Secret.UserName,(ConvertTo-SecureString
        $Secret.Password -AsPlainText -Force)))
       ```

   - *Indirizzi IP del server DNS (IP_ADDRESS_1, IP_ADDRESS_2)*
   - *ID di sottorete per le sottoreti in cui intendi creare il file system Amazon FSx (SUBNET_1, SUBNET_2, ad esempio).* subnet-04431191671ac0d19

```
PS C:\>
$FSxADValidationArgs = @{
    # DNS root of ActiveDirectory domain
    DomainDNSRoot = 'DOMAINNAME.COM'

    # IP v4 addresses of DNS servers
    DnsIpAddresses = @('IP_ADDRESS_1', 'IP_ADDRESS_2')
```

```
    # Subnet IDs for Amazon FSx file server(s)
    SubnetIds = @('SUBNET_1', 'SUBNET_2')

    Credential = $Credential
}
```

9. (Facoltativo) Imposta l'unità organizzativa, il gruppo di amministratori delegati e abilita la convalida delle autorizzazioni degli account di servizio seguendo le istruzioni nel file incluso prima di eseguire lo strumento di convalida. DomainControllersMaxCount `README.md`

> **Note**
>
> Il `Domain Admins` gruppo ha un nome diverso se il sistema operativo non è in inglese. Ad esempio, il gruppo è denominato `Administrateurs du domaine` nella versione francese del sistema operativo. Se non si specifica un valore, viene utilizzato il nome di `Domain Admins` gruppo predefinito e la creazione del file system ha esito negativo.

10. Eseguite lo strumento di convalida utilizzando questo comando.

```
PS C:\> $Result = Test-FSxADConfiguration @FSxADValidationArgs
```

11. Di seguito è riportato un esempio di esito positivo del test.

```
Test 1 - Validate EC2 Subnets ...
...
Test 17 - Validate 'Delete Computer Objects' permission ...

Test computer object amznfsxtestd53f deleted!
...
SUCCESS - All tests passed! Please proceed to creating an Amazon FSx file system.
 For your convenience, SelfManagedActiveDirectoryConfiguration of result can be
 used directly in CreateFileSystemWindowsConfiguration for New-FSXFileSystem
PS C:\AmazonFSxADValidation> $Result.Failures.Count
0
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

Di seguito è riportato un esempio di risultato di un test con errori.

```
Test 1 - Validate EC2 Subnets ...
```

```
...
Test 7 - Validate that provided EC2 Subnets belong to a single AD Site ...

Name          DistinguishedName
     Site
----          -----------------
     ----
10.0.0.0/19   CN=10.0.0.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local   CN=SiteB,CN=Sites,CN=Configu...
10.0.128.0/19 CN=10.0.128.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local CN=Default-First-Site-Name,C...
10.0.64.0/19  CN=10.0.64.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local  CN=SiteB,CN=Sites,CN=Configu...



Best match for EC2 subnet subnet-092f4caca69e360e7 is AD site CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=te
st-ad,DC=local
Best match for EC2 subnet subnet-04431191671ac0d19 is AD site
 CN=SiteB,CN=Sites,CN=Configuration,DC=test-ad,DC=local
WARNING: EC2 subnets subnet-092f4caca69e360e7 subnet-04431191671ac0d19 matched to
 different AD sites! Make sure they
are in a single AD site.
...
9 of 16 tests skipped.
FAILURE - Tests failed. Please see error details below:

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}



Please address all errors and warnings above prior to re-running validation to
 confirm fix.
PS C:\AmazonFSxADValidation> $Result.Failures.Count
1
PS C:\AmazonFSxADValidation> $Result.Failures

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}
```

```
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

Se ricevi avvisi o errori quando esegui lo strumento di convalida, consulta la guida alla risoluzione dei problemi inclusa nel pacchetto dello strumento di convalida () `TROUBLESHOOTING.md` e. Risoluzione dei problemi di Amazon FSx

Unire un file system Amazon FSx a un dominio Microsoft Active Directory autogestito

Quando si crea un nuovo file system FSx for Windows File Server, è possibile configurare l'integrazione con Microsoft Active Directory in modo che si aggiunga al dominio Microsoft Active Directory autogestito. A tale scopo, fornisci le seguenti informazioni per Microsoft Active Directory:

- Il nome di dominio completo della directory Microsoft Active Directory locale.

> **Note**
>
> Amazon FSx attualmente non supporta i domini Single Label Domain (SLD).

- Gli indirizzi IP dei server DNS del tuo dominio.
- Credenziali per un account di servizio nel dominio Microsoft Active Directory locale. Amazon FSx utilizza queste credenziali per accedere alla tua Active Directory autogestita.

È anche possibile specificare:

- Un'unità organizzativa (OU) specifica all'interno del dominio a cui desideri far aderire il file system Amazon FSx.
- Il nome del gruppo di dominio i cui membri dispongono dei privilegi amministrativi per il file system Amazon FSx.

> **Note**
>
> Il nome del gruppo di dominio fornito deve essere univoco in Active Directory. FSx for Windows File Server non creerà il gruppo di domini nelle seguenti circostanze:
>
> - Se esiste già un gruppo con il nome specificato

- Se non specifichi un nome e un gruppo denominato «Domain Admins» esiste già in Active Directory.

Dopo aver specificato queste informazioni, Amazon FSx aggiunge il tuo nuovo file system al tuo dominio Active Directory autogestito utilizzando l'account di servizio che hai fornito.

> **Important**
>
> Amazon FSx registra i record DNS per un file system solo se il dominio Active Directory a cui ti stai unendo utilizza Microsoft DNS come DNS predefinito. Se utilizzi un DNS di terze parti, dovrai configurare manualmente le voci DNS per i tuoi file system Amazon FSx dopo aver creato il file system. Per ulteriori informazioni sulla scelta degli indirizzi IP corretti da utilizzare per il file system, consulta. Ottenere gli indirizzi IP corretti del file system da utilizzare per il DNS

Prima di iniziare

Assicurati di aver completato i Prerequisiti per l'utilizzo di un Microsoft Active Directory autogestito dettagli inUtilizzo di Amazon FSx con Microsoft Active Directory autogestito.

Per creare un file system FSx for Windows File Server unito a un Active Directory (console) autogestito

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di controllo, scegli Crea file system per avviare la procedura guidata di creazione del file system.
3. Scegli FSx for Windows File Server, quindi scegli Avanti. Viene visualizzata la pagina Crea file system.
4. Fornisci un nome per il tuo file system. È possibile utilizzare un massimo di 256 lettere Unicode, spazi bianchi e numeri, oltre ai caratteri speciali + - =. _:/
5. Per Capacità di archiviazione, immettere la capacità di archiviazione del file system, in GiB. Se utilizzi l'archiviazione SSD, inserisci un numero intero compreso tra 32 e 65.536. Se utilizzi l'archiviazione su HDD, inserisci un numero intero compreso tra 2.000 e 65.536. 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.

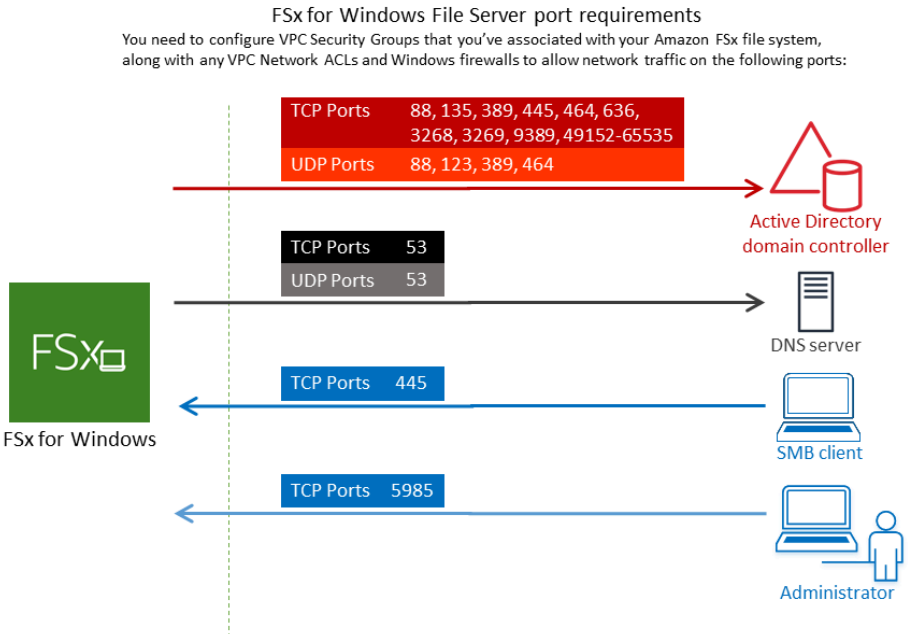
6. Mantieni Capacità di velocità effettiva sul valore di default. La capacità di throughput è la velocità sostenuta alla quale il file server che ospita il file system può fornire i dati. L'impostazione della capacità di throughput consigliata si basa sulla quantità di capacità di archiviazione scelta. Se hai bisogno di una capacità di throughput superiore a quella consigliata, scegli Specificare la capacità di throughput, quindi scegli un valore. Per ulteriori informazioni, consulta Prestazioni di FSx for Windows File Server.

   È possibile modificare la capacità di throughput in base alle esigenze in qualsiasi momento dopo aver creato il file system. Per ulteriori informazioni, consulta Gestione della capacità di throughput.

7. Scegli il VPC che desideri associare al tuo file system. Ai fini di questo esercizio introduttivo, scegli lo stesso VPC utilizzato per la AWS Directory Service directory e l'istanza Amazon EC2.

8. Scegli un valore qualsiasi per le zone di disponibilità e la sottorete.

9. Per i gruppi di sicurezza VPC, il gruppo di sicurezza predefinito per il tuo Amazon VPC predefinito è già aggiunto al file system nella console. Assicurati che il gruppo di sicurezza e gli ACL di rete VPC per le sottoreti in cui stai creando il file system FSx consentano il traffico sulle porte e nelle direzioni mostrate nel diagramma seguente.



Nella tabella seguente è indicato il ruolo di ciascuna porta.

Protocollo	Porte	Ruolo
TCP/UDP	53	Doma Name Syste (DNS)
TCP/UDP	88	Auten zione Kerbe
TCP/UDP	464	Modifi reimp zione della passw
TCP/UDP	389	Lightw ht Direct Acces Proto
UDP	123	Netwo Time Proto (NTP)

Protocollo	Porte	Ruolo
TCP	135	Distrib ed Comp Enviro nt/ End Point Mapp (DCE/ EPMA P)
TCP	445	Condi one di file SMB di Serviz direct
TCP	636	Lightw ht Direct Acces Protoc su TLS/ SSL (LDAP
TCP	3268	Catalo global Micros

Protocollo	Porte	Ruolo
TCP	3269	Micros Globa Catalo tramit SSL
TCP	5985	WinRI 2.0 (gesti remot di Micros Windo
TCP	9389	Serviz Web Micros Active Direct DS, Powe l
TCP	49152 - 65535	Porte effime per RPC

> **Important**
>
> L'autorizzazione del traffico in uscita sulla porta TCP 9389 è necessaria per le implementazioni di file system Single-AZ 2 e Multi-AZ.

> **Note**
>
> Se utilizzi ACL di rete VPC, devi anche consentire il traffico in uscita su porte dinamiche (49152-65535) dal tuo file system FSx.

- Regole in uscita per consentire tutto il traffico verso gli indirizzi IP associati ai server DNS e ai controller di dominio per il dominio Microsoft Active Directory autogestito. Per ulteriori informazioni, consulta la documentazione Microsoft sulla configurazione del firewall per le comunicazioni con Active Directory.
- Assicurati che queste regole del traffico siano rispecchiate anche sui firewall che si applicano a ciascuno dei controller di dominio Active Directory, server DNS, client FSx e amministratori FSx.

> **Note**
>
> Se hai definito siti Active Directory, devi assicurarti che le sottoreti nel VPC associato al tuo file system Amazon FSx siano definite in un sito Active Directory e che non esistano conflitti tra le sottoreti nel tuo VPC e le sottoreti negli altri siti. È possibile visualizzare e modificare queste impostazioni utilizzando lo snap-in MMC di Active Directory Sites and Services.

> **Important**
>
> Sebbene i gruppi di sicurezza Amazon VPC richiedano l'apertura delle porte solo nella direzione di avvio del traffico di rete, la maggior parte dei firewall Windows e degli ACL di rete VPC richiedono che le porte siano aperte in entrambe le direzioni.

10. Per l'autenticazione Windows, scegli Microsoft Active Directory autogestito.
11. Immettere un valore per Nome di dominio completo per la directory Microsoft Active Directory autogestita.

> **Note**
>
> Il nome di dominio non deve essere nel formato SLD (Single Label Domain). Amazon FSx attualmente non supporta i domini SLD.

> **Important**
>
> Per Single-AZ 2 e tutti i file system Multi-AZ, il nome di dominio Active Directory non può superare i 47 caratteri.

12. Immettere un valore per Unità organizzativa per la directory Microsoft Active Directory autogestita.

> **Note**
>
> Assicurati che l'account di servizio fornito disponga delle autorizzazioni delegate all'unità organizzativa specificata qui o all'unità organizzativa predefinita se non ne specifichi una.

13. Immettere almeno uno e non più di due valori per gli indirizzi IP del server DNS per la directory Microsoft Active Directory autogestita.
14. Inserisci un valore di stringa per il nome utente dell'account di servizio per l'account sul tuo dominio Active Directory autogestito, ad esempio. `ServiceAcct` Amazon FSx utilizza questo nome utente per accedere al tuo dominio Microsoft Active Directory.

> **Important**
>
> NON includere un prefisso di dominio (`corp.com\ServiceAcct`) o un suffisso di dominio (`ServiceAcct@corp.com`) quando inserisci il nome utente dell'account di servizio.
> NON utilizzate il nome distinto (DN) quando inserite il nome utente dell'account di servizio (`CN=ServiceAcct,OU=example,DC=corp,DC=com`).

15. Inserisci un valore per la password dell'account di servizio per l'account nel tuo dominio Active Directory autogestito. Amazon FSx utilizza questa password per accedere al tuo dominio Microsoft Active Directory.

16. Inserisci nuovamente la password per confermarla in Conferma password.
17. Per il gruppo di amministratori di file system delegati, specifica il `Domain Admins` gruppo o un gruppo di amministratori di file system delegati personalizzato (se ne hai creato uno). Il gruppo specificato deve avere l'autorità delegata per eseguire attività amministrative sul file system. Se non fornisci un valore, Amazon FSx utilizza il gruppo `Domain Admins` Builtin. Tieni presente che Amazon FSx non supporta la presenza di un contenitore Builtin `Delegated file system administrators group` (né il `Domain Admins` gruppo né il gruppo personalizzato specificato).

> **Important**
>
> Se non fornisci un gruppo di amministratori di file system delegati, per impostazione predefinita Amazon FSx tenta di utilizzare il gruppo Builtin nel tuo dominio Active `Domain Admins` Directory. Se il nome di questo gruppo Builtin è stato modificato o se utilizzi un gruppo diverso per l'amministrazione del dominio, devi fornire quel nome per il gruppo qui.

> **Important**
>
> NON includete un prefisso di dominio (corp.com\ FSxAdmins) o un suffisso di dominio (F SxAdmins @corp .com) quando fornite il parametro del nome del gruppo.
> NON utilizzate il nome distinto (DN) per il gruppo. Un esempio di nome distinto è CN=FSxAdmins, OU=Example, DC=corp, DC=com.

Per creare un file system FSx for Windows File Server unito a un Active Directory autogestito ()AWS CLI

L'esempio seguente crea un file system FSx for Windows File Server con `SelfManagedActiveDirectoryConfiguration` una `us-east-2` nella zona di disponibilità.

```
aws fsx --region us-east-2 \
create-file-system \
--file-system-type WINDOWS \
--storage-capacity 300 \
--security-group-ids security-group-id \
--subnet-ids subnet-id\
```

```
--windows-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAdmini
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',ThroughputCapacity=8
```

> **Important**
>
> Non spostare oggetti informatici creati da Amazon FSx nell'unità organizzativa dopo la creazione del file system. In questo modo il file system verrà configurato in modo errato.

Ottenere gli indirizzi IP corretti del file system da utilizzare per il DNS

Amazon FSx registra i record DNS per un file system solo se utilizzi Microsoft DNS come servizio DNS predefinito. Se utilizzi un DNS di terze parti, dovrai configurare manualmente le voci DNS per i tuoi file system Amazon FSx. Questa sezione descrive come ottenere gli indirizzi IP corretti del file system da utilizzare se è necessario aggiungere manualmente il file system al DNS. Tieni presente che una volta creato un file system, i relativi indirizzi IP non cambiano finché il file system non viene eliminato.

Come ottenere gli indirizzi IP del file system da utilizzare per le voci DNS A

1. In https://console.aws.amazon.com/fsx/, scegliete il file system di cui desiderate ottenere l'indirizzo IP per visualizzare la pagina dei dettagli del file system.
2. Nella scheda Rete e sicurezza, effettuate una delle seguenti operazioni:
   - Per i file system Single-AZ 1:
     - Nel pannello Subnet, scegli l'interfaccia di rete elastica mostrata in Interfaccia di rete per aprire la pagina Interfacce di rete nella console Amazon EC2.
     - L'indirizzo IP da utilizzare per il file system Single-AZ 1 è indicato nella colonna IP IPv4 privato primario.
   - Per i file system Single-AZ 2 o Multi-AZ:
     - Nel pannello Preferred subnet, scegli l'interfaccia di rete elastica mostrata in Interfaccia di rete per aprire la pagina Interfacce di rete nella console Amazon EC2.

- L'indirizzo IP della sottorete preferita da utilizzare è mostrato nella colonna IP IPv4 privato secondario.
- Nel pannello della sottorete Amazon FSx Standby, scegli l'interfaccia di rete elastica mostrata in Interfaccia di rete per aprire la pagina Interfacce di rete nella console Amazon EC2.
- L'indirizzo IP della sottorete di standby da utilizzare è mostrato nella colonna IP IPv4 privato secondario.

> **Note**
>
> Se è necessario configurare voci DNS per Windows Remote PowerShell Endpoint per file system Single-AZ 2 o Multi-AZ, è necessario utilizzare l'indirizzo IPv4 privato primario per l'interfaccia di rete elastica per la sottorete Preferred. Per ulteriori informazioni, consulta Utilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell.

Aggiornamento della configurazione di Active Directory autogestita

Puoi utilizzare l' AWS Management Console API Amazon FSx o AWS CLI aggiornare il nome utente e la password dell'account di servizio e gli indirizzi IP del server DNS della configurazione Active Directory autogestita di un file system. Puoi monitorare lo stato di avanzamento di un aggiornamento della configurazione di Active Directory autogestito in qualsiasi momento utilizzando la AWS Management Console CLI e l'API. Per ulteriori informazioni, consulta Monitoraggio degli aggiornamenti di Active Directory gestiti autonomamente.

Per aggiornare la configurazione di Active Directory autogestita (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il file system Windows per il quale desideri aggiornare la configurazione di Active Directory autogestita.
3. Nella scheda Rete e sicurezza, quindi scegli Aggiorna per gli indirizzi IP del server DNS o per il nome utente dell'account di servizio, a seconda delle proprietà di Active Directory che stai aggiornando.
4. Inserisci i nuovi indirizzi IP del server DNS o le nuove credenziali dell'account di servizio nella finestra di dialogo che appare.
5. Scegli Aggiorna per avviare l'aggiornamento della configurazione di Active Directory.

È possibile monitorare l'avanzamento dell'aggiornamento utilizzando AWS Management Console o il AWS CLI.

Per aggiornare la configurazione di Active Directory (CLI) autogestita

- Per aggiornare la configurazione di Active Directory autogestita di un file system FSx for Windows File Server, utilizzare AWS CLI il comando update-file-system. Imposta i seguenti parametri:
  - `--file-system-id`all'ID del file system che si sta aggiornando.
  - `UserName`il nuovo nome utente per l'account del servizio Active Directory autogestito.
  - `Password`la nuova password per l'account del servizio Active Directory autogestito.
  - `DnsIps`gli indirizzi IP per i server DNS di Active Directory autogestiti.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 'SelfManagedActiveDirectoryConfiguration={UserName=username,Password=password,\
     DnsIps=[192.0.2.0,192.0.2.24]}'
```

Se l'azione di aggiornamento ha esito positivo, il servizio restituisce una risposta HTTP 200. L'`AdminstrativeActions`oggetto nella risposta descrive la richiesta e il relativo stato.

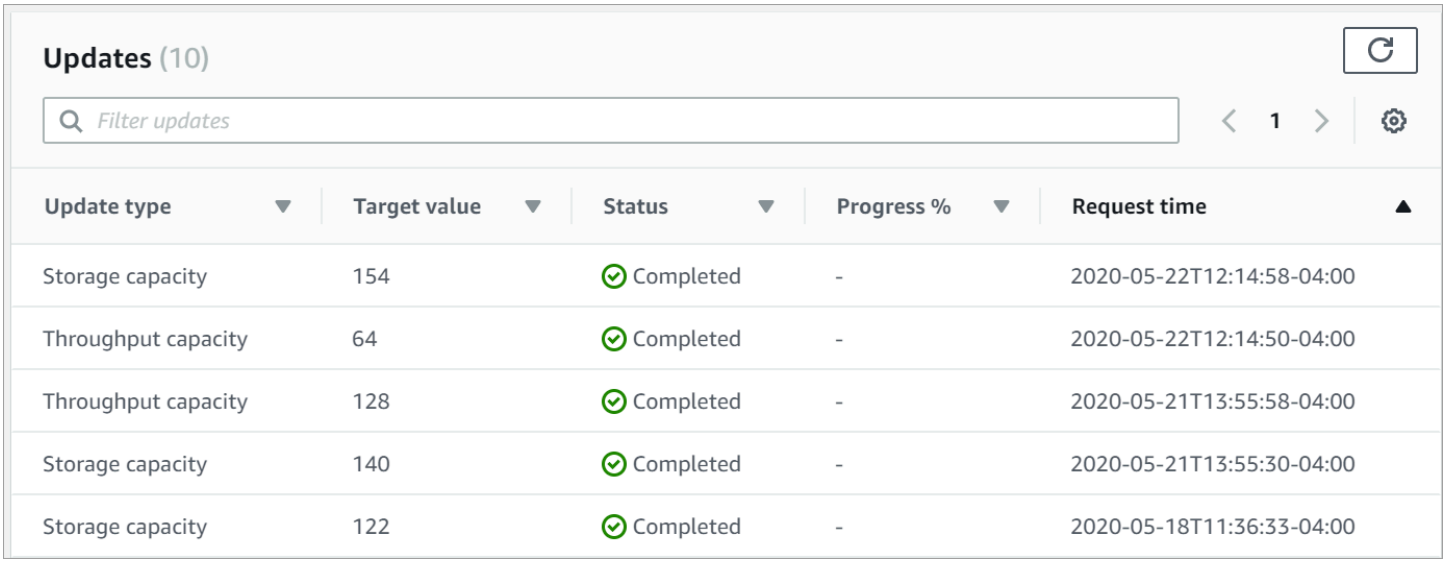
Monitoraggio degli aggiornamenti di Active Directory gestiti autonomamente

Quando si aggiorna la configurazione di Active Directory autogestita del file system, lo stato del file system passa da Disponibile a Aggiornamento durante l'applicazione dell'aggiornamento. Una volta completato l'aggiornamento, lo stato torna a Disponibile. Tieni presente che il completamento dell'aggiornamento può richiedere fino a diversi minuti.

È possibile monitorare lo stato di avanzamento di un aggiornamento della configurazione di Active Directory autogestito utilizzando l' AWS Management Console API o la AWS CLI, descritta nelle sezioni seguenti.

Monitoraggio degli aggiornamenti nella console

Nella scheda Aggiornamenti della finestra dei dettagli del file system, puoi visualizzare i 10 aggiornamenti più recenti per ogni tipo di aggiornamento.



Per gli aggiornamenti di Active Directory autogestiti, puoi visualizzare le seguenti informazioni.

Tipo di aggiornamento

I tipi supportati sono i seguenti:

- Indirizzo IP del server DNS
- Credenziali dell'account di servizio

Target value (Valore target)

Il valore desiderato a cui aggiornare la proprietà del file system. Per gli aggiornamenti delle credenziali degli account di servizio, viene visualizzato solo il nome utente, le password degli account di servizio non vengono mai incluse in questo campo.

Stato

Lo stato attuale dell'aggiornamento. Per gli aggiornamenti di Active Directory autogestiti, 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 del file system è stato completato con successo.

- Non riuscito: l'aggiornamento del file system non è riuscito. Scegli il punto interrogativo (?) per visualizzare i dettagli sull'errore.

Progresso%

Visualizza lo stato di avanzamento dell'aggiornamento del file system come percentuale di completamento.

Orario della richiesta

L'ora in cui Amazon FSx ha ricevuto la richiesta di azione di aggiornamento.

Monitoraggio degli aggiornamenti tramite l'API AWS CLI and

È possibile visualizzare e monitorare le richieste di aggiornamento del file system in corso utilizzando il AWS CLI comando describe-file-systems e l'azione Systems API. DescribeFile L'`AdministrativeActions`array elenca le 10 azioni di aggiornamento più recenti per ogni tipo di azione amministrativa.

L'esempio seguente mostra un estratto della risposta di un comando CLI che mostra due aggiornamenti del describe-file-systems file system Active Directory autogestiti.

```
{
    "OwnerId": "111122223333",
    .
    .
    .
    "StorageCapacity": 1000,
    "AdministrativeActions": [
        {
            "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
            "RequestTime": 1581694766.757,
            "Status": "PENDING",
            "TargetFileSystemValues": {
                "WindowsConfiguration": {
                    "SelfManagedActiveDirectoryConfiguration": {
                        "UserName": "serviceUser",
                    }
                }
            }
        },
        {
```

```
                "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                "RequestTime": 1619032957.759,
                "Status": "FAILED",
                "TargetFileSystemValues": {
                    "WindowsConfiguration": {
                        "SelfManagedActiveDirectoryConfiguration": {
                        "DnsIps": [
                                "10.0.138.161"
                            ]
                        }
                    }
                },
                "FailureDetails": {
                    "Message": "Failure details message."
                }
            }
        ],
    .
    .
    .
```

Utilizzo delle condivisioni di file di Microsoft Windows

Una condivisione di file di Microsoft Windows è una cartella specifica del file system. Include le sottocartelle di quella cartella, che puoi rendere accessibili alle tue istanze di calcolo con il protocollo Server Message Block (SMB). Il file system è dotato di una condivisione di file Windows predefinita, denominata. `share` È possibile creare e gestire tutte le altre condivisioni di file Windows desiderate utilizzando lo strumento di interfaccia grafica utente (GUI) di Windows denominato Cartelle condivise.

Accesso alle condivisioni di file

Per accedere alle tue condivisioni di file, utilizzi la funzionalità Windows Map Network Drive per mappare una lettera di unità sulla tua istanza di calcolo alla tua condivisione di file Amazon FSx. Il processo di mappatura di una condivisione di file su un'unità dell'istanza di calcolo è noto come montaggio di una condivisione di file in Linux. Questo processo varia a seconda del tipo di istanza di calcolo e del sistema operativo. Dopo aver mappato la condivisione di file, le applicazioni e gli utenti possono accedere ai file e alle cartelle della condivisione di file come se fossero file e cartelle locali.

Di seguito sono riportate le procedure per mappare una condivisione di file sulle diverse istanze di calcolo supportate.

Argomenti

Mappatura di una condivisione di file su un'istanza Amazon EC2 Windows

Puoi mappare una condivisione di file su un'istanza EC2 Windows utilizzando Windows File Explorer o il prompt dei comandi.

Per mappare una condivisione di file su un'istanza Amazon EC2 Windows (console)

1. Avvia l'istanza EC2 per Windows e connettila al Microsoft Active Directory a cui hai collegato il tuo file system Amazon FSx. A tale scopo, scegli una delle seguenti procedure dalla Guida all'AWS Directory Service amministrazione:

- Unisciti senza problemi a un'istanza Windows EC2
- Unisciti manualmente a un'istanza Windows

2. Connettiti all'istanza EC2 Windows. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
3. Dopo esserti connesso, apri File Explorer.
4. Nel riquadro di navigazione, apri il menu contestuale (fai clic con il pulsante destro del mouse) per Rete e scegli Map Network Drive.
5. Per Drive, scegli una lettera di unità.
6. Per Cartella, inserisci il nome DNS del file system o un alias DNS associato al file system e il nome della condivisione.

> **Important**
>
> L'utilizzo di un indirizzo IP anziché del nome DNS potrebbe causare l'indisponibilità durante il processo di failover del file system Multi-AZ. Inoltre, i nomi DNS o gli alias DNS associati sono necessari per l'autenticazione basata su Kerberos nei file system Multi-AZ e Single-AZ.

Puoi trovare il nome DNS del file system e tutti gli alias DNS associati sulla console Amazon FSx scegliendo Windows File Server, rete e sicurezza. Oppure, puoi trovarli nella risposta dell'operazione CreateFileSystem o DescribeFile Systems API. Per ulteriori informazioni sull'utilizzo degli alias DNS, consulta. Gestione degli alias DNS

- Per un file system Single-AZ unito a un Microsoft Active Directory AWS gestito, il nome DNS è simile al seguente.

```
fs-0123456789abcdef0.ad-domain.com
```

- Per un file system Single-AZ unito a un Active Directory autogestito e qualsiasi file system Multi-AZ, il nome DNS è simile al seguente.

```
amznfsxaa11bb22.ad-domain.com
```

Ad esempio, per utilizzare il nome DNS di un file system Single-AZ, inserisci quanto segue per Cartella.

```
\\fs-0123456789abcdef0.ad-domain.com\share
```

Per utilizzare il nome DNS di un file system Multi-AZ, immettete quanto segue in Folder.

```
\\famznfsxaa11bb22.ad-domain.com\share
```

Per utilizzare un alias DNS associato al file system, immettete quanto segue in Folder.

```
\\fqdn-dns-alias\share
```

7. Scegli un'opzione per Riconnettiti all'accesso, che indica se la condivisione di file deve riconnettersi all'accesso, quindi scegli Fine.

Per mappare una condivisione di file su un'istanza Amazon EC2 Windows (prompt dei comandi)

1. Avvia l'istanza EC2 per Windows e connettila al Microsoft Active Directory a cui hai collegato il tuo file system Amazon FSx. A tale scopo, scegli una delle seguenti procedure dalla Guida all'AWS Directory Service amministrazione:
   - Unisciti senza problemi a un'istanza Windows EC2
   - Unisciti manualmente a un'istanza Windows
2. Connect alla tua istanza EC2 Windows come utente nella tua AWS Managed Microsoft AD directory. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
3. Dopo la connessione, apri una finestra del prompt dei comandi.
4. Installa la condivisione di file utilizzando una lettera di unità a tua scelta, il nome DNS del file system e il nome della condivisione. Puoi trovare il nome DNS utilizzando la console Amazon FSx scegliendo Windows File Server, rete e sicurezza. Oppure, puoi trovarli nella risposta dell'operazione `CreateFileSystem` o `DescribeFileSystems` API.
   - Per un file system Single-AZ unito a un Microsoft Active Directory AWS gestito, il nome DNS è simile al seguente.

```
fs-0123456789abcdef0.ad-domain.com
```

- Per un file system Single-AZ unito a un Active Directory autogestito e qualsiasi file system Multi-AZ, il nome DNS è simile al seguente.

```
amznfsxaa11bb22.ad-domain.com
```

Di seguito è riportato un comando di esempio per montare la condivisione di file.

```
$ net use H: \\amzfsxaa11bb22.ad-domain.com\share /persistent:yes
```

Al posto del `net use` comando, puoi anche utilizzare qualsiasi PowerShell comando supportato per montare una condivisione di file.

Montaggio di una condivisione di file su un'istanza Amazon EC2 per Mac

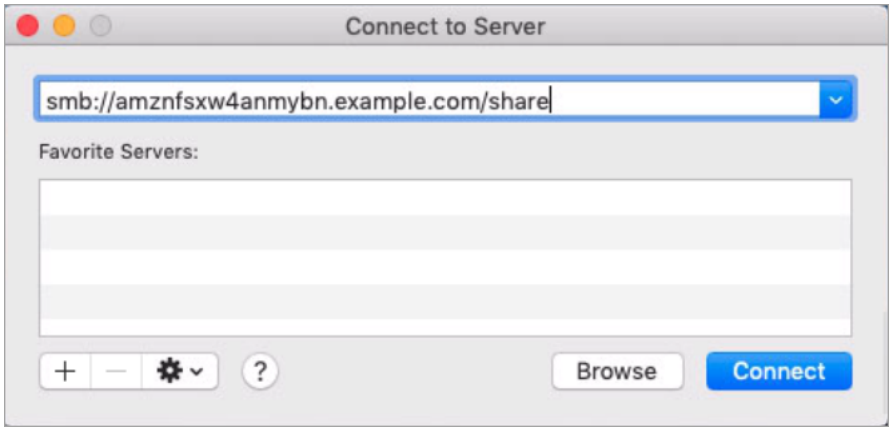
Puoi montare una condivisione di file su un'istanza Mac di Amazon EC2 che sia unita o meno alla tua Active Directory. Se l'istanza non è aggiunta al tuo Active Directory, assicurati di aggiornare le opzioni DHCP impostate per Amazon Virtual Private Cloud (Amazon VPC) in cui risiede l'istanza per includere i name server DNS per il tuo dominio Active Directory. Quindi riavvia l'istanza.

Per montare una condivisione di file su un'istanza Mac (GUI) di Amazon EC2

1. Avvia l'istanza EC2 per Mac. A tale scopo, scegli una delle seguenti procedure dalla Guida per l'utente di Amazon EC2:
   - Avvia un'istanza Mac utilizzando la console
   - Avvia un'istanza Mac utilizzando AWS CLI
2. Connect alla tua istanza EC2 per Mac utilizzando Virtual Network Computing (VNC). Per ulteriori informazioni, consulta Connect to your instance using VNC nella Amazon EC2 User Guide.
3. Sulla tua istanza EC2 per Mac, connettiti alla condivisione di file Amazon FSx, come segue:
   a. Apri Finder, scegli Vai, quindi scegli Connect to Server.

b. Nella finestra di dialogo Connect to Server, immettete il nome DNS del file system o un alias DNS associato al file system e il nome della condivisione. Quindi scegliere Connetti.

   Puoi trovare il nome DNS del file system e tutti gli alias DNS associati sulla console Amazon FSx scegliendo Windows File Server, rete e sicurezza. Oppure, puoi trovarli nella risposta dell'operazione CreateFileSystem o DescribeFile Systems API. Per ulteriori informazioni sull'utilizzo degli alias DNS, consulta. Gestione degli alias DNS



c. Nella schermata successiva, scegli Connect per continuare.

d. Inserisci le tue credenziali Microsoft Active Directory (AD) per l'account del servizio Amazon FSx, come mostrato nell'esempio seguente. Quindi scegliere Connetti.

e. Se la connessione è riuscita, puoi vedere la condivisione Amazon FSx in Locations nella finestra del Finder.

Per montare una condivisione di file su un'istanza Mac di Amazon EC2 (riga di comando)

1. Avvia l'istanza EC2 per Mac. A tale scopo, scegli una delle seguenti procedure dalla Guida per l'utente di Amazon EC2:

   - Avvia un'istanza Mac utilizzando la console
   - Avvia un'istanza Mac utilizzando AWS CLI

2. Connect alla tua istanza EC2 per Mac utilizzando Virtual Network Computing (VNC). Per ulteriori informazioni, consulta Connect to your instance using VNC nella Amazon EC2 User Guide.

3. Monta la condivisione di file con il seguente comando.

   ```
   mount_smbfs //file_system_dns_name/file_share mount_point
   ```

   Puoi trovare il nome DNS sulla console Amazon FSx scegliendo Windows File Server, rete e sicurezza. Oppure, puoi trovarli nella risposta dell'operazione `CreateFileSystem` o `DescribeFileSystems` API.

   - Per un file system Single-AZ unito a un Microsoft Active Directory AWS gestito, il nome DNS è simile al seguente.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - Per un file system Single-AZ unito a un Active Directory autogestito e qualsiasi file system Multi-AZ, il nome DNS è simile al seguente.

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   Il comando mount utilizzato in questa procedura esegue le seguenti operazioni nei punti indicati:

   - *//file_system_dns_name/file_share*— specifica il nome DNS e la condivisione del file system da montare.
   - *mount_point* — La directory sull'istanza EC2 su cui state montando il file system.

Montaggio di una condivisione di file su un'istanza Amazon EC2 Linux

Puoi montare una condivisione di file FSx for Windows File Server su un'istanza Amazon EC2 Linux che fa parte o non fa parte del tuo Active Directory.

> **Note**
>
> - I comandi seguenti specificano parametri come il protocollo SMB, la memorizzazione nella cache e la dimensione del buffer di lettura e scrittura solo a titolo esemplificativo. Le scelte dei parametri per il `cifs` comando Linux, così come la versione del kernel Linux utilizzata, possono influire sulla velocità effettiva e sulla latenza per le operazioni di rete tra il client e il file system Amazon FSx. Per ulteriori informazioni, consulta `cifs` la documentazione relativa all'ambiente Linux che stai utilizzando.
> - I client Linux non supportano il failover automatico basato su DNS. Per ulteriori informazioni, consulta Esperienza di failover su client Linux.

Per montare una condivisione di file su un'istanza Amazon EC2 Linux unita al tuo Active Directory

1. Se non hai già un'istanza EC2 Linux in esecuzione aggiunta a Microsoft Active Directory, consulta Aggiungere manualmente un'istanza Linux nella Guida all'AWS Directory Service amministrazione per le istruzioni in merito.
2. Connect alla tua istanza EC2 Linux. Per ulteriori informazioni, consulta Connect to your Linux istance nella Amazon EC2 User Guide.
3. Per installare il pacchetto `cifs-utils`, esegui il comando seguente. Questo pacchetto viene utilizzato per montare file system di rete come Amazon FSx su Linux.

   ```
   $ sudo yum install cifs-utils
   ```

4. Crea la directory **`/mnt/fsx`** dei punti di montaggio. È qui che installerai il file system Amazon FSx.

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

5. Effettua l'autenticazione con kerberos utilizzando il seguente comando.

   ```
   $ kinit
   ```

6. Monta la condivisione di file con il seguente comando.

```
$ sudo mount -t cifs //file_system_dns_name/file_share mount_point --verbose -o
 vers=SMB_version,sec=krb5,cruid=ad_user,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=no
file-server-Ip
```

Puoi trovare il nome DNS sulla console Amazon FSx scegliendo Windows File Server, rete e sicurezza. In alternativa, puoi trovarli nella risposta della nostra operazione `CreateFileSystem` `DescribeFileSystems` API.

- Per un file system Single-AZ unito a un Microsoft Active Directory AWS gestito, il nome DNS è simile al seguente.

```
fs-0123456789abcdef0.ad-domain.com
```

- Per un file system Single-AZ unito a un Active Directory autogestito e qualsiasi file system Multi-AZ, il nome DNS è simile al seguente.

```
amznfsxaa11bb22.ad-domain.com
```

*CIFSMaxBufSize*Sostituiscilo con il valore massimo consentito dal kernel. Eseguite il comando seguente per ottenere questo valore.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

L'output mostra che la dimensione massima del buffer è 130048.

7. Verificate che il file system sia montato eseguendo il comando seguente, che restituisce solo i file system del tipo CIFS (Common Internet File System).

```
$ mount -l -t cifs
//fs-0123456789abcdef0/share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=krb5,cache=cache_mode,username=user1@CORP.NETWORK.COM,ui
```

Il comando mount utilizzato in questa procedura esegue le seguenti operazioni nei punti indicati:

- *//file_system_dns_name/file_share*— specifica il nome DNS e la condivisione del file system da montare.
- *mount_point* — La directory sull'istanza EC2 su cui state montando il file system.
- `-t cifs vers=`*SMB_version*— Speciifica il tipo di file system come CIFS e la versione del protocollo SMB. Amazon FSx for Windows File Server supporta le versioni SMB dalla 2.0 alla 3.1.1.
- `sec=krb5`— Specifica di utilizzare Kerberos versione 5 per l'autenticazione.
- `cache=`*cache_mode*— Imposta la modalità cache. Questa opzione per la cache CIFS può influire sulle prestazioni, pertanto è necessario verificare quali impostazioni funzionano meglio (e consultare la documentazione di Linux) per il kernel e il carico di lavoro. Le opzioni `strict` e none sono consigliate, perché `loose` possono causare incoerenze nei dati a causa della semantica del protocollo più flessibile.
- `cruid=`*ad_user*— Imposta l'uid del proprietario della cache delle credenziali all'amministratore della directory AD.
- */mnt/fsx*— Speciifica il punto di montaggio per la condivisione di file Amazon FSx sull'istanza EC2.
- `rsize=`*CIFSMaxBufSize*`,wsize=`*CIFSMaxBufSize*— Speciifica la dimensione massima del buffer di lettura e scrittura consentita dal protocollo CIFS. Sostituisci *CIFSMaxBufSize* con il valore massimo consentito dal kernel. Determina il `CIFSMaxBufSize` eseguendo il comando seguente.

  ```
  $ modinfo cifs | grep CIFSMaxBufSize
  parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
   16384 Range: 8192 to 130048 (uint)
  ```

  L'output mostra che la dimensione massima del buffer è 130048.
- `ip=`*preferred-file-server-Ip*— Imposta l'indirizzo IP di destinazione su quello del file server preferito del file system.

  È possibile recuperare l'indirizzo IP del file server preferito del file system nel modo seguente:

  - Utilizzando la console Amazon FSx, nella scheda Rete e sicurezza della pagina dei dettagli del file system.
  - Nella risposta del comando `describe-file-systems` CLI o del comando DescribeFileSystems API equivalente.

Per montare una condivisione di file su un'istanza Amazon EC2 Linux non aggiunta ad Active Directory

La procedura seguente monta una condivisione di file Amazon FSx su un'istanza Amazon EC2 Linux che non è unita al tuo Active Directory (AD). Per un'istanza Linux EC2 che non è aggiunta al tuo AD, puoi montare una condivisione di file FSx for Windows File Server solo utilizzando il relativo indirizzo IP privato. Puoi ottenere l'indirizzo IP privato del file system utilizzando la console Amazon FSx, nella scheda Rete e sicurezza, in Indirizzo IP del file server preferito.

Questo esempio utilizza l'autenticazione NTLM. A tale scopo, si monta il file system come utente membro del dominio Microsoft Active Directory a cui è unito il file system FSx for Windows File Server. Le credenziali per l'account utente vengono fornite in un file di testo creato sull'istanza EC2,. `creds.txt` Questo file contiene il nome utente, la password e il dominio dell'utente.

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

Per avviare e configurare l'istanza Amazon Linux EC2

1. Avvia un'istanza Amazon Linux EC2 utilizzando la console Amazon EC2. Per ulteriori informazioni, consulta Launch an instance nella Amazon EC2 User Guide.
2. Connettiti alla tua istanza Amazon Linux EC2. Per ulteriori informazioni, consulta Connect to your Linux istance nella Amazon EC2 User Guide.
3. Per installare il pacchetto `cifs-utils`, esegui il comando seguente. Questo pacchetto viene utilizzato per montare file system di rete come Amazon FSx su Linux.

   ```
   $ sudo yum install cifs-utils
   ```

4. Crea il punto di montaggio **`/mnt/fsxx`** in cui intendi montare il file system Amazon FSx.

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

5. Crea il file `creds.txt` delle credenziali nella `/home/ec2-user` directory, utilizzando il formato mostrato in precedenza.
6. Imposta i permessi del `creds.txt` file in modo che solo tu (il proprietario) possa leggere e scrivere sul file eseguendo il comando seguente.

```
$ chmod 700 creds.txt
```

Per montare il file system

1. È possibile montare una condivisione di file non unita ad Active Directory utilizzando il relativo indirizzo IP privato. Puoi ottenere l'indirizzo IP privato del file system utilizzando la console Amazon FSx, nella scheda Rete e sicurezza, nell'indirizzo IP del file server preferito.
2. Installa il file system usando il seguente comando:

   ```
   $ sudo mount -t cifs //file-system-IP-address/file_share /mnt/fsx
    --verbose -o vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
   creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
   ```

   Sostituisci *CIFSMaxBufSize* con il valore massimo consentito dal tuo kernel. Eseguite il comando seguente per ottenere questo valore.

   ```
   $ modinfo cifs | grep CIFSMaxBufSize
   parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
    16384 Range: 8192 to 130048 (uint)
   ```

   L'output mostra che la dimensione massima del buffer è 130048.
3. Verificate che il file system sia montato eseguendo il comando seguente, che restituisce solo i file system CIFS.

   ```
   $ mount -l -t cifs
   //file-system-IP-address/file_share on /mnt/fsx type cifs
    (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_mode,username=user1,domain=CORP.EXA
   ```

Il comando mount utilizzato in questa procedura esegue le seguenti operazioni nei punti indicati:

- *//file-system-IP-address/file_share*— Specificate l'indirizzo IP e la condivisione del file system che state montando.
- `-t cifs vers=`*SMB_version*— Speciifica il tipo di file system come CIFS e la versione del protocollo SMB. Amazon FSx for Windows File Server supporta le versioni SMB dalla 2.0 alla 3.1.1.

- `sec=ntlmsspi`— specifica di utilizzare NT LAN Manager Security Support Provider Interface (NTLMSSPI) per l'autenticazione.
- `cache=`*`cache_mode`*— Imposta la modalità cache. Questa opzione per la cache CIFS può influire sulle prestazioni, pertanto è necessario verificare quali impostazioni funzionano meglio (e consultare la documentazione di Linux) per il kernel e il carico di lavoro. Le opzioni `strict` e `none` sono consigliate, perché `loose` possono causare incoerenze nei dati a causa della semantica del protocollo più flessibile.
- `cred=/home/ec2-user/creds.txt`— Speciifica dove ottenere le credenziali dell'utente.
- */mnt/fsx*— Speciifica il punto di montaggio per la condivisione di file Amazon FSx sull'istanza EC2.
- `rsize=`*`CIFSMaxBufSize`*`,wsize=`*`CIFSMaxBufSize`*— Speciifica la dimensione massima del buffer di lettura e scrittura consentita dal protocollo CIFS. Sostituisci *`CIFSMaxBufSize`* con il valore massimo consentito dal kernel. Determina il `CIFSMaxBufSize` eseguendo il comando seguente.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

Montaggio automatico di condivisioni di file su un'istanza Amazon Linux EC2 non aggiunta a Active Directory

Puoi montare automaticamente la condivisione di file FSx for Windows File Server ogni volta che l'istanza Amazon EC2 Linux su cui è montata si riavvia. A tale scopo, aggiungi una voce al `/etc/fstab` file sull'istanza EC2. Il file `/etc/fstab` contiene informazioni sui file system. Il comandomount -a, che viene eseguito durante l'avvio dell'istanza, monta i file system elencati nel `/etc/fstab` file.

Per un'istanza Amazon EC2 Linux che non fa parte di Active Directory, puoi montare una condivisione di file FSx for Windows File Server solo utilizzando il relativo indirizzo IP privato. Puoi ottenere l'indirizzo IP privato del file system utilizzando la console Amazon FSx, nella scheda Rete e sicurezza, in Indirizzo IP del file server preferito.

La procedura seguente utilizza l'autenticazione Microsoft NTLM. Il file system viene montato come utente membro del dominio Microsoft Active Directory a cui viene aggiunto il file system FSx for Windows File Server. Le credenziali per l'account utente sono fornite nel file di testo. `creds.txt` Questo file contiene il nome utente, la password e il dominio dell'utente.

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

Per montare automaticamente una condivisione di file su un'istanza Amazon Linux EC2 non aggiunta al tuo Active Directory

Per avviare e configurare l'istanza Amazon Linux EC2

1. Avvia un'istanza Amazon Linux EC2 utilizzando la console Amazon EC2. Per ulteriori informazioni, consulta Launch an instance nella Amazon EC2 User Guide.
2. Connettiti alla tua istanza. Per ulteriori informazioni, consulta Connect to your Linux istance nella Amazon EC2 User Guide.
3. Per installare il pacchetto `cifs-utils`, esegui il comando seguente. Questo pacchetto viene utilizzato per montare file system di rete come Amazon FSx su Linux.

   ```
   $ sudo yum install cifs-utils
   ```

4. Creazione della directory `/mnt/fsx`. È qui che installerai il file system Amazon FSx.

   ```
   $ sudo mkdir /mnt/fsx
   ```

5. Crea il file `creds.txt` delle credenziali nella `/home/ec2-user` directory.
6. Imposta i permessi del file in modo che solo tu (il proprietario) possa leggere il file eseguendo il comando seguente.

   ```
   $ sudo chmod 700 creds.txt
   ```

Per montare automaticamente il file system

1. Si monta automaticamente una condivisione di file non aggiunta ad Active Directory utilizzando il relativo indirizzo IP privato. Puoi ottenere l'indirizzo IP privato del file system utilizzando la console Amazon FSx, nella scheda Rete e sicurezza, in Indirizzo IP del file server preferito.
2. Per montare automaticamente la condivisione di file utilizzando il relativo indirizzo IP privato, aggiungi la riga seguente al `/etc/fstab` file.

```
//file-system-IP-address/file_share /mnt/fsx cifs
 vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

   Sostituisci *CIFSMaxBufSize* con il valore massimo consentito dal tuo kernel. Eseguite il comando seguente per ottenere questo valore.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

   L'output mostra che la dimensione massima del buffer è 130048.
3. Verifica la `fstab` voce utilizzando il `mount` comando con l'opzione 'fake' insieme alle opzioni 'all' e 'verbose'.

```
$ sudo mount -fav
home/ec2-user/fsx      : successfully mounted
```

4. Per montare la condivisione di file, riavvia l'istanza Amazon EC2.
5. Quando l'istanza è nuovamente disponibile, verifica che il file system sia montato eseguendo il comando seguente.

```
$ sudo mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_code,username=user1,domain=CORP.EXA
```

   La riga aggiunta al `/etc/fstab` file in questa procedura esegue le seguenti operazioni nei punti indicati:

- `//file-system-IP-address/file_share`: specifica l'indirizzo IP e la condivisione del file system Amazon FSx che stai montando.
- `/mnt/fsx`: specifica il punto di montaggio per il file system Amazon FSx sull'istanza EC2.
- `cifs vers=SMB_version`— Speciifica il tipo di file system come CIFS e la versione del protocollo SMB. Amazon FSx for Windows File Server supporta le versioni SMB dalla 2.0 alla 3.1.1.
- `sec=ntlmsspi`— specifica l'utilizzo dell'interfaccia NT LAN Manager Security Support Provider per facilitare l'autenticazione NTLM challenge-response.
- `cache=cache_mode`— Imposta la modalità cache. Questa opzione per la cache CIFS può influire sulle prestazioni, pertanto è necessario verificare quali impostazioni funzionano meglio (e consultare la documentazione di Linux) per il kernel e il carico di lavoro. Le opzioni `strict` e `none` sono consigliate, perché `loose` possono causare incoerenze nei dati a causa della semantica del protocollo più flessibile.
- `cred=/home/ec2-user/creds.txt`— Speciifica dove ottenere le credenziali dell'utente.
- `_netdev`— Indica al sistema operativo che il file system risiede su un dispositivo che richiede l'accesso alla rete. L'utilizzo di questa opzione impedisce all'istanza di montare il file system finché il servizio di rete non viene abilitato sul client.
- `0`— Indica che il file system deve essere sottoposto a backup da`dump`, se è un valore diverso da zero. Per Amazon FSx, questo valore dovrebbe essere. `0`
- `0`— Speciifica l'ordine in cui `fsck` controlla i file system all'avvio. Per i file system Amazon FSx, questo valore dovrebbe `0` indicare che `fsck` non deve essere eseguito all'avvio.

Migrazione dello storage di file esistente su Amazon FSx

FSx for Windows File Server offre le caratteristiche, le prestazioni e la compatibilità per aiutarti a trasferire e spostare facilmente le applicazioni aziendali su Amazon Web Services Cloud. Il processo di migrazione a FSx for Windows File Server prevede i seguenti passaggi:

1. Esegui la migrazione dei file su FSx for Windows File Server. Per ulteriori informazioni, consulta Migrazione dello storage di file esistente su FSx for Windows File Server.
2. Esegui la migrazione della configurazione della condivisione di file su FSx for Windows File Server. Per ulteriori informazioni, consulta Migrazione delle configurazioni di condivisione di file su Amazon FSx.
3. Associa il tuo nome DNS esistente come alias DNS per il tuo file system Amazon FSx. Per ulteriori informazioni, consulta Associare un alias DNS ad Amazon FSx.
4. Passare a FSx for Windows File Server. Per ulteriori informazioni, consulta Passaggio ad Amazon FSx.

I dettagli di ogni fase del processo sono disponibili nelle seguenti sezioni.

Argomenti

Migrazione dello storage di file esistente su FSx for Windows File Server

Per migrare i file esistenti sui file system FSx for Windows File Server, si consiglia di AWS DataSync utilizzare un servizio di trasferimento dati online progettato per semplificare, automatizzare e accelerare la copia di grandi quantità di dati da e verso i servizi di storage. AWS DataSync copia i dati su Internet o. AWS Direct Connect Essendo un servizio completamente gestito, DataSync elimina gran parte della necessità di modificare applicazioni, sviluppare script o gestire l'infrastruttura. Per ulteriori informazioni, consulta Migrazione di file esistenti su FSx for Windows File Server utilizzando AWS DataSync.

Come soluzione alternativa, è possibile utilizzare Robust File Copy o Robocopy, che è una directory da riga di comando e un set di comandi per la replica dei file per Microsoft Windows. Per procedure dettagliate su come utilizzare Robocopy per migrare lo storage di file su FSx for Windows File Server, vedere. Migrazione di file esistenti su FSx for Windows File Server utilizzando Robocopy

Procedure consigliate per la migrazione dello storage di file esistente su FSx for Windows File Server

Per migrare grandi quantità di dati su FSx for Windows File Server il più rapidamente possibile, utilizza i file system Amazon FSx configurati con storage su unità a stato solido (SSD). Una volta completata la migrazione, puoi spostare i dati su file system Amazon FSx utilizzando lo storage su disco rigido (HDD) se questa è la soluzione migliore per la tua applicazione.

Per spostare i dati da un file system Amazon FSx utilizzando lo storage SDD allo storage HDD, puoi eseguire le seguenti operazioni. (Tieni presente che i file system HDD hanno una capacità di storage minima di 2 TB e non puoi modificare la capacità di archiviazione durante il ripristino da un backup.)

1. Effettua un backup del file system SSD. Per ulteriori informazioni, consulta Creazione di backup avviati dall'utente.
2. Ripristina il backup su un file system utilizzando l'archiviazione su HDD. Per ulteriori informazioni, consulta Ripristino dei backup.

Migrazione di file esistenti su FSx for Windows File Server utilizzando AWS DataSync

Si consiglia di AWS DataSync utilizzarlo per trasferire dati tra file system FSx for Windows File Server. DataSync è un servizio di trasferimento dati che semplifica, automatizza e accelera lo spostamento e la replica dei dati tra sistemi di storage locali e altri AWS servizi di archiviazione su Internet o. AWS Direct Connect DataSync può trasferire i dati e i metadati del file system, come proprietà, timestamp e autorizzazioni di accesso.

DataSync supporta la copia delle liste di controllo degli accessi (ACL) NTFS e supporta anche la copia delle informazioni sul controllo di controllo dei file, note anche come liste di controllo degli accessi di sistema NTFS (SACL), utilizzate dagli amministratori per controllare la registrazione di controllo dei tentativi degli utenti di accedere ai file.

È possibile utilizzare DataSync per trasferire file tra due file system FSx for Windows File Server e anche per spostare i dati su un file system con un account AWS o Regione AWS diverso. È

possibile utilizzare DataSync i file system FSx for Windows File Server per altre attività. Ad esempio, è possibile eseguire migrazioni di dati una tantum, importare periodicamente dati per carichi di lavoro distribuiti e pianificare la replica per la protezione e il ripristino dei dati.

In AWS DataSync, una posizione per FSx for Windows File Server è un endpoint per un FSx for Windows File Server. È possibile trasferire file tra una posizione per FSx for Windows File Server e una posizione per altri file system. Per informazioni, vedere Lavorare con le posizioni nella Guida per l'AWS DataSync utente.

DataSync accede al file server FSx for Windows utilizzando il protocollo Server Message Block (SMB). Si autentica con il nome utente e la password configurati nella console o. AWS DataSync AWS CLI

Prerequisiti

Per migrare i dati nella configurazione di Amazon FSx for Windows File Server, 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.

Se stai eseguendo una migrazione di dati di grandi dimensioni o una migrazione che coinvolge molti file di piccole dimensioni, ti consigliamo di utilizzare un file system Amazon FSx con tipo di storage SSD. Questo perché DataSync le attività comportano scansioni dei metadati dei file che possono esaurire i limiti IOPS del disco dei file system HDD, con conseguenti migrazioni di lunga durata e un impatto sulle prestazioni del file system. Per ulteriori informazioni, consulta Procedure consigliate per la migrazione dello storage di file esistente su FSx for Windows File Server.

Se il set di dati è composto principalmente da file di piccole dimensioni, i file sono milioni o se la larghezza di banda di rete disponibile è superiore a quella utilizzata per una singola DataSync attività, puoi anche accelerare i trasferimenti di dati con un'architettura scalabile. Per ulteriori informazioni, consulta: Come accelerare i trasferimenti di dati con architetture AWS DataSync scalabili orizzontalmente.

È possibile monitorare l'utilizzo dell'I/O su disco del file system utilizzando le metriche delle prestazioni FSx.

Passaggi di base per la migrazione dei file utilizzando DataSync

Per trasferire file da una posizione di origine a una posizione di destinazione utilizzando DataSync, procedi nel seguente modo di base:

- Scaricare e distribuire un agente nell'ambiente e attivarlo.
- Creare e configurare una posizione di origine e di destinazione.
- Creare e configurare un'attività.
- Eseguire l'attività per trasferire i file dall'origine alla destinazione.

Per informazioni su come trasferire file da un file system locale esistente a FSx for Windows File Server, consulta Trasferimento dati tra storage autogestito e, Creazione di una posizione per SMB AWS e Creazione di una posizione per Amazon FSx for Windows File Server nella Guida per l'utente.AWS DataSync

Per informazioni su come trasferire file da un file system esistente nel cloud al file server FSx for Windows, consulta Distribuisci il tuo agente come istanza Amazon EC2 nella Guida per l'utente.AWS DataSync

Migrazione tra due file system Amazon FSx

Puoi utilizzarlo DataSync per migrare i dati tra due file system Amazon FSx. Questo può essere utile se devi spostare il carico di lavoro da un file system esistente a un nuovo file system con una configurazione diversa, ad esempio da una configurazione Single-AZ a una Multi-AZ. È inoltre possibile utilizzarlo DataSync per suddividere il carico di lavoro tra due file system.

Ecco un esempio di panoramica del processo di migrazione:

1. Crea DataSync posizioni per i file system di origine e di destinazione. Tieni presente che l'origine e la destinazione devono appartenere allo stesso dominio Active Directory (AD) o avere una relazione di trust AD tra i rispettivi domini.
2. Crea e configura un' DataSync attività per trasferire dati dall'origine alla destinazione. È possibile eseguire l'attività come istanza singola o impostarla in modo che venga eseguita automaticamente in base a una pianificazione configurata dall'utente.
3. Una volta completata correttamente l'operazione, i dati nel file system di destinazione sono una copia esatta dell'origine. Tieni presente che dovrai sospendere temporaneamente qualsiasi attività di scrittura o aggiornamento dei file sul file system di origine per completare l'operazione. È quindi possibile passare al file system di destinazione ed eliminare il file system di origine.

Prima di eseguire la migrazione dal file system di produzione, è possibile testare il processo di migrazione su un file system ripristinato da un backup recente. Ciò consente di stimare la durata del processo di trasferimento dei dati e di risolvere DataSync gli errori in anticipo.

Per ridurre al minimo i tempi di cutover, è possibile eseguire DataSync le attività in anticipo, spostando la maggior parte dei dati dal file system di origine al file system di destinazione. Dopo aver interrotto il traffico verso il file system di origine, puoi eseguire un'ultima operazione di trasferimento per sincronizzare tutti i dati appena aggiornati dopo l'interruzione del traffico e trasferirli al file system di destinazione.

È possibile configurare DataSync le attività in modo che vengano eseguite solo in determinate directory o per includere o escludere determinati percorsi. Questo può essere utile se esegui più attività in parallelo o se desideri migrare un sottoinsieme di dati.

È possibile creare un alias DNS sul file system di destinazione che sia uguale al nome DNS del file system di origine. Ciò consente agli utenti finali e alle applicazioni di continuare ad accedere ai dati dei file utilizzando il nome DNS del file system di origine. Per ulteriori informazioni su come configurare un alias DNS, vedere:. Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system

Quando si esegue questo tipo di migrazione, si consiglia quanto segue:

- Pianifica la migrazione per evitare backup del file system, finestre di manutenzione settimanali e `Data Deduplication` lavori. In particolare, consigliamo di disabilitare il `Data Deduplication GarbageCollection` processo se coincide con la migrazione pianificata.
- Utilizza un tipo di archiviazione SSD per i file system di origine e di destinazione. Puoi passare da un tipo di storage HDD a uno SSD eseguendo il ripristino dal backup. Per ulteriori informazioni, vedere:. Migrazione dello storage di file esistente su FSx for Windows File Server
- Configura i tuoi file system di origine e destinazione con una capacità di trasmissione sufficiente per la quantità di dati che devi trasferire. Durante i DataSync processi operativi, monitorate l'utilizzo delle prestazioni sia del file system di origine che di quello di destinazione. Per ulteriori informazioni, consulta Monitoraggio delle metriche con Amazon CloudWatch.
- Imposta il DataSync monitoraggio per aiutarti a comprendere lo stato di avanzamento delle attività in corso. Puoi anche inviare DataSync log al gruppo Amazon CloudWatch Logs per aiutarti a eseguire il debug delle tue attività in caso di errori.

Migrazione di file esistenti su FSx for Windows File Server utilizzando Robocopy

Basato su Microsoft Windows Server, Amazon FSx for Windows File Server ti consente di migrare completamente i set di dati esistenti nei file system Amazon FSx. Puoi migrare i dati per ogni file.

È inoltre possibile migrare tutti i metadati pertinenti dei file, inclusi attributi, timestamp, elenchi di controllo degli accessi (ACL), informazioni sui proprietari e informazioni di controllo. Con questo supporto totale per la migrazione, Amazon FSx consente di spostare carichi di lavoro e applicazioni basati su Windows basandosi su questi set di dati di file su Amazon Web Services Cloud.

Utilizza i seguenti argomenti come guida nel processo di copia dei dati dei file esistenti. Quando esegui questa copia, conservi tutti i metadati dei file dai tuoi data center locali o dai tuoi file server autogestiti su Amazon EC2.

Prerequisiti

Prima di iniziare, assicurati di fare quanto segue:

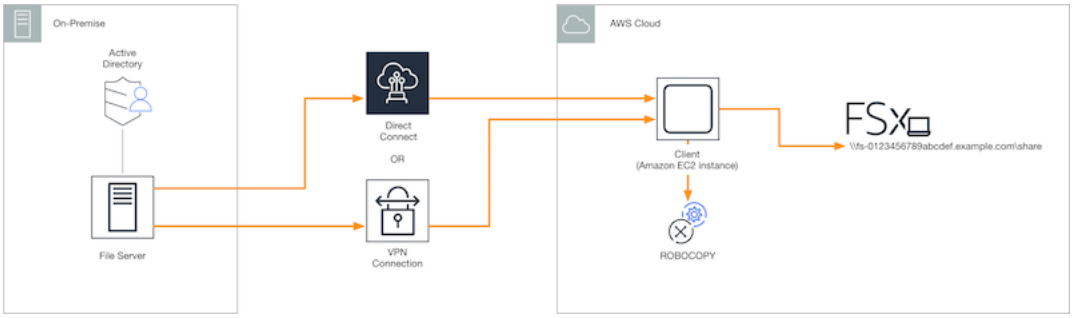
- Stabilisci la connettività di rete (utilizzando AWS Direct Connect o VPN) tra il tuo Active Directory locale e il VPC in cui desideri creare il file system Amazon FSx.
- Crea un account di servizio su Active Directory con autorizzazioni delegate per aggiungere computer al dominio. Per ulteriori informazioni, consulta Delegare i privilegi all'account di servizio nella Guida all'amministrazione.AWS Directory Service
- Crea un file system Amazon FSx, aggiunto alla tua directory Microsoft AD autogestita (locale).
- Nota la posizione (ad esempio`\\Source\Share`) della condivisione di file (locale o interna AWS) che contiene i file esistenti che desideri trasferire su Amazon FSx.
- Nota la posizione (ad esempio`\\Target\Share`) della condivisione di file sul file system Amazon FSx a cui desideri trasferire i file esistenti.

La tabella seguente riassume i requisiti di accessibilità del file system di origine e di destinazione per tre modelli di accesso utente di migrazione.

Modello di accesso utente per la migrazione	Requisiti di accessibilità del file system di origine	Requisiti di accessibilità del file server FSx di destinazione
Modello di autorizzazioni di lettura/scrittura dirette	L'utente deve disporre almeno delle autorizzazioni di lettura (ACL NTFS) per i file e le cartelle da migrare.	L'utente deve disporre almeno delle autorizzazioni di scrittura (ACL NTFS) per i file e le cartelle da migrare.

Modello di accesso utente per la migrazione	Requisiti di accessibilità del file system di origine	Requisiti di accessibilità del file server FSx di destinazione
Modello di privilegi di backup/ripristino per sovrascrivere le autorizzazioni di accesso	L'utente deve essere membro del gruppo Backup Operators di Active Directory locale e utilizzar e il flag /b con. RoboCopy	L'utente deve essere membro del gruppo di amministratori del file system Amazon FSx* e utilizzar e il flag /b con. RoboCopy
Modello di privilegi di amministratore di dominio (completo) per ignorare le autorizzazioni di accesso	L'utente deve essere membro del gruppo Domain Admins di Active Directory locale.	L'utente deve essere membro del gruppo di amministratori del file system Amazon FSx* e utilizzar e il flag /b con RoboCopy

> **Note**
>
> * Per i file system uniti a un AWS Managed Microsoft AD, il gruppo di amministratori di file system Amazon FSx è Delegated AWS FSx Administrators. Nel tuo Microsoft AD autogestito, il gruppo di amministratori del file system Amazon FSx è Domain Admins o il gruppo personalizzato che hai specificato per l'amministrazione al momento della creazione del file system.



Come migrare i file esistenti su Amazon FSx utilizzando Robocopy

Puoi migrare i file esistenti su Amazon FSx utilizzando la seguente procedura.

Per migrare i file esistenti su Amazon FSx

1. Avvia un'istanza Amazon EC2 per Windows Server 2016 nello stesso Amazon VPC del file system Amazon FSx.
2. Esegui la connessione all'istanza Amazon EC2. Per ulteriori informazioni, consulta Connessione a un'istanza Windows nella Guida per l'utente di Amazon EC2 per le istanze Windows.
3. *Apri il **prompt dei comandi** e mappa la condivisione di file di origine sul file server esistente (locale o interno AWS) a una lettera di unità (ad esempio, Y:) come segue.* A tale scopo, fornisci le credenziali per un membro del gruppo Domain Administrators di Active Directory locale.

   ```
   C:\>net use Y: \\fileserver1.mydata.com\localdata /user:mydata.com\Administrator
   Enter the password for 'fileserver1.mydata.com': _

   Drive Y: is now connected to \\fileserver1.mydata.com\localdata.

   The command completed successfully.
   ```

4. Mappa la condivisione di file di destinazione sul tuo file system Amazon FSx su una lettera di unità diversa (ad esempio, *Z*:) sull'istanza Amazon EC2 come segue. A tale scopo, fornisci le credenziali per un account utente che fa parte del tuo gruppo di amministratori di dominio di Active Directory locale e del gruppo di amministratori del tuo file system Amazon FSx. Per i file system uniti a un AWS Managed Microsoft AD, quel gruppo è **`AWS Delegated FSx Administrators`**. In Microsoft AD autogestito, tale gruppo è **`Domain Admins`** o il gruppo personalizzato specificato per l'amministrazione al momento della creazione del file system.

   Per ulteriori informazioni, consulta la tabella dei requisiti di accessibilità dei file system di origine e destinazione nel. Prerequisiti

   ```
   C:\>net use Z: \\amznfsxabcdef1.mydata.com\share /user:mydata.com\Administrator
   Enter the password for 'amznfsxabcdef1.mydata.com': _

   Drive Z: is now connected to \\amznfsxabcdef1.mydata.com\share.

   The command completed successfully.
   ```

5. Scegliete Esegui come amministratore dal menu contestuale. Apri il prompt dei comandi o Windows PowerShell come amministratore ed esegui il seguente comando Robocopy per copiare i file dalla condivisione di origine a quella di destinazione.

Il ROBOCOPY comando è un'utilità flessibile per il trasferimento di file con diverse opzioni per controllare il processo di trasferimento dei dati. Grazie a questo processo di ROBOCOPY comando, tutti i file e le directory della condivisione di origine vengono copiati nella condivisione di destinazione Amazon FSx. La copia conserva gli ACL NTFS di file e cartelle, gli attributi, i timestamp, le informazioni sul proprietario e le informazioni di controllo.

```
robocopy Y:\ Z:\ /copy:DATSOU /secfix /e /b /MT:8
```

Il comando di esempio precedente utilizza gli elementi e le opzioni seguenti:

- Y: fa riferimento alla condivisione di origine situata nella foresta di Active Directory locale mydata.com.
- Z: si riferisce alla condivisione di destinazione\\ amznfsxabcdef1.mydata.com\ share su Amazon FSx.
- /copy: specifica le seguenti proprietà del file da copiare:
  - D — dati
  - A — attributi
  - T — timestamp
  - S — ACL NTFS
  - O — informazioni sul proprietario
  - U — informazioni di controllo.
- /secfix — Risolve la sicurezza dei file su tutti i file, anche quelli ignorati.
- /e — Copia le sottodirectory, incluse quelle vuote.
- /b — Utilizza il privilegio di backup e ripristino di Windows per copiare i file anche se i relativi ACL NTFS negano le autorizzazioni all'utente corrente.
- /MT:8 — Speciifica quanti thread utilizzare per eseguire copie multithread.

> **Note**
>
> Se si stanno copiando file di grandi dimensioni tramite una connessione lenta o inaffidabile, è possibile abilitare la modalità di riavvio utilizzando l'opzione al posto dell'opzione. /zb robocopy /b Con la modalità di riavvio, se il trasferimento di un file di grandi dimensioni viene interrotto, un'operazione Robocopy successiva può riprendere a metà del trasferimento

anziché dover copiare nuovamente l'intero file dall'inizio. L'attivazione della modalità di riavvio può ridurre la velocità di trasferimento dei dati.

Migrazione delle configurazioni di condivisione di file su Amazon FSx

Puoi migrare una configurazione di condivisione di file esistente su Amazon FSx utilizzando la seguente procedura. In questa procedura, il file server di origine è il file server di cui desideri migrare la configurazione di condivisione file su Amazon FSx.

> **Note**
>
> Esegui innanzitutto la migrazione dei file su Amazon FSx prima di migrare la configurazione di condivisione dei file. Per ulteriori informazioni, consulta Migrazione dello storage di file esistente su FSx for Windows File Server.

Per migrare le condivisioni di file esistenti su FSx for Windows File Server

1. Sul file server di origine, scegliete Esegui come amministratore dal menu contestuale. Apri Windows PowerShell come amministratore.
2. Esporta le condivisioni di file del file server di origine in un file denominato `SmbShares.xml` eseguendo i seguenti comandi in PowerShell. Sostituisci F: in questo esempio con la lettera di unità sul file server da cui stai esportando le condivisioni di file.

   ```
   $shareFolder = Get-SmbShare -Special $false | ? { $_.Path -like “F:\*” }
   $shareFolder | Export-Clixml -Path F:\SmbShares.xml
   ```

3. Modifica il `SmbShares.xml` file, sostituendo tutti i riferimenti a F: (la tua lettera di unità) in D:\share poiché i file system Amazon FSx risiedono su D:\share.
4. Importa la configurazione di condivisione di file esistente in FSx for Windows File Server. Su un client che ha accesso al file system Amazon FSx di destinazione e al file server di origine, copia la configurazione della condivisione di file salvata. Quindi importalo in una variabile utilizzando il seguente comando.

   ```
   $shares = Import-Clixml -Path F:\SmbShares.xml
   ```

5. Preparate l'oggetto credenziale necessario per creare le condivisioni di file sul file server FSx for Windows File Server utilizzando una delle seguenti opzioni.

   Per generare l'oggetto credenziale in modo interattivo, utilizzate il comando seguente.

   ```
   $credential = Get-Credential
   ```

   Per generare l'oggetto credenziale utilizzando una AWS Secrets Manager risorsa, utilizzate il comando seguente.

   ```
   $credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
    $AdminSecret).SecretString
   $FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
   SecureString $credential.Password -AsPlainText -Force)))
   ```

6. Esegui la migrazione della configurazione della condivisione di file sul tuo file server Amazon FSx utilizzando lo script seguente.

   ```
   $FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",
    "ConcurrentUserLimit", "CATimeout", "FolderEnumerationMode", "CachingMode",
    "FullAccess", "ChangeAccess", "ReadAccess", "NoAccess", "SecurityDescriptor",
    "Path", "Name", "EncryptData")
   ForEach ($item in $shares) {
       $param = @{};
       Foreach ($property in $item.psObject.properties) {
           if ($property.Name -In $FSxAcceptedParameters) {
               $param[$property.Name] = $property.Value
           }
       }
       Invoke-Command -ConfigurationName FSxRemoteAdmin -ComputerName
    amznfsxxxxxxxxx.corp.com -ErrorVariable errmsg -ScriptBlock { New-FSxSmbShare -
   Credential $Using:credential @Using:param }
   }
   ```

Migrazione della configurazione DNS per utilizzare Amazon FSx

FSx for Windows File Server fornisce un nome DNS (Domain Name System) predefinito per ogni file system che è possibile utilizzare per accedere ai dati sul file system. Puoi anche accedere ai tuoi file

system utilizzando qualsiasi nome DNS di tua scelta configurando il nome DNS alternativo come alias DNS per il tuo file system Amazon FSx.

Con gli alias DNS, puoi continuare a utilizzare i nomi DNS esistenti per accedere ai dati archiviati su Amazon FSx durante la migrazione dello storage del file system da locale ad Amazon FSx. Questo aiuta a eliminare la necessità di aggiornare strumenti o applicazioni che utilizzano i nomi DNS durante la migrazione ad Amazon FSx. È possibile associare gli alias DNS ai file system FSx for Windows File Server esistenti, quando si creano nuovi file system e quando si crea un nuovo file system da un backup. È possibile associare fino a 50 alias DNS a un file system contemporaneamente. Per ulteriori informazioni, consulta Gestione degli alias DNS.

Un nome alias DNS deve soddisfare i seguenti requisiti:

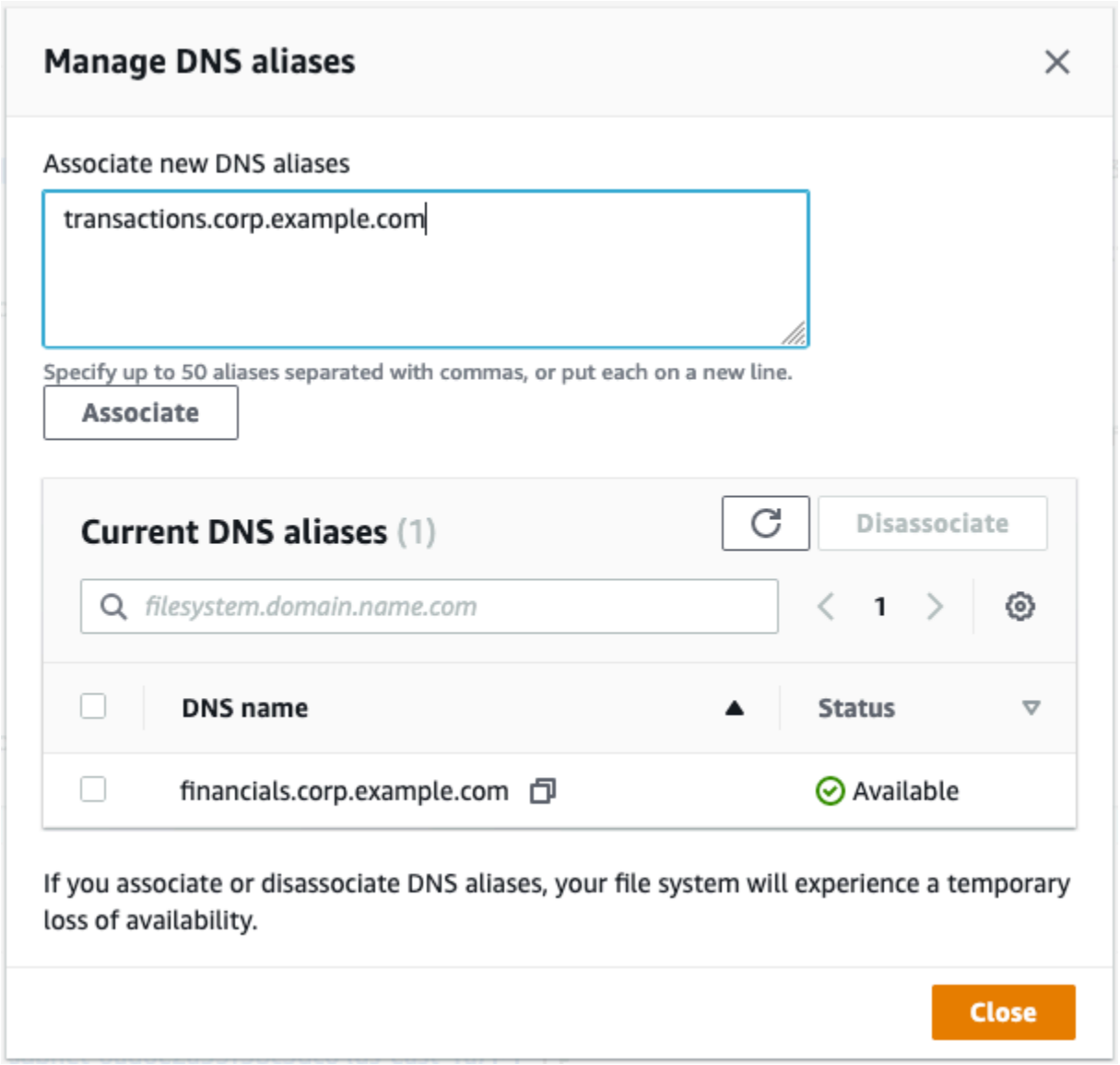
- Deve essere formattato come nome di dominio completo (FQDN), ad esempio. `accounting.example.com`
- Può contenere caratteri alfanumerici e il trattino (-).
- Non può iniziare o terminare con un trattino (-).
- Può iniziare con un numerico.

Per i nomi alias DNS, Amazon FSx archivia i caratteri alfabetici come lettere minuscole (a-z), indipendentemente dal modo in cui li specifichi: come lettere maiuscole, minuscole o lettere corrispondenti in codici di escape.

Le seguenti procedure descrivono come associare gli alias DNS ai file system FSx for Windows File Server esistenti utilizzando la console, l'interfaccia a riga di comando e l'API di Amazon FSx. Per ulteriori informazioni sull'associazione degli alias DNS durante la creazione di nuovi file system, inclusi nuovi file system da un backup, consulta. Associazione degli alias DNS ai file system

Per associare gli alias DNS a un file system esistente (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il file system Windows a cui desideri associare i tuoi alias DNS.
3. Nella scheda Rete e sicurezza, scegliete Gestisci alias DNS per aprire la finestra di dialogo Gestisci alias DNS.



4. Nella casella Associa nuovi alias, inserisci gli alias DNS che desideri associare.
5. Scegliete Associa per aggiungere gli alias al file system.

   È possibile monitorare lo stato degli alias appena associati nell'elenco degli alias correnti. Quando lo stato è Available, l'alias viene associato al file system (un processo che può richiedere fino a 2,5 minuti).

Per associare alias DNS a un file system (CLI) esistente

- Utilizzate il comando `associate-file-system-aliases` CLI o l'operazione AssociateFileSystemAliasesAPI per associare gli alias DNS a un file system esistente.

La seguente richiesta CLI associa due alias al file system specificato.

```
aws fsx associate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com transfers.corp.example.com
```

La risposta mostra lo stato degli alias che Amazon FSx associa al file system.

```
{
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": CREATING
          },
          {
              "Name": "transfers.corp.example.com",
              "Lifecycle": CREATING
          }
      ]
  }
```

Per monitorare lo stato degli alias che state associando, utilizzate il comando `describe-file-system-aliases` CLI (DescribeFileSystemAliasesè l'operazione API equivalente). Se `Lifecycle` per un alias è impostato il valore AVAILABLE, puoi utilizzarlo per accedere al file system (un processo che può richiedere fino a 2,5 minuti).

Passaggio ad Amazon FSx

Per eseguire il trasferimento al file system FSx for Windows File Server, effettuate le seguenti operazioni:

- Preparatevi per il taglio.
  - Disconnettere temporaneamente i client SMB dal file system originale.
  - Esegui una sincronizzazione finale della configurazione del file e della condivisione di file.
- Configura i nomi principali di servizio (SPN) per il tuo file system Amazon FSx.
- Aggiorna i record DNS CNAME in modo che puntino al tuo file system Amazon FSx.

Le procedure per eseguire ciascuno di questi passaggi sono fornite nelle sezioni seguenti.

Argomenti

Preparazione per il passaggio ad Amazon FSx

Per prepararti al cutover del tuo file system Amazon FSx, devi fare quanto segue:

- Disconnetti tutti i client che scrivono sul file system originale.
- Esegui una sincronizzazione finale dei file utilizzando AWS DataSync o Robocopy. Per ulteriori informazioni, consulta Migrazione dello storage di file esistente su FSx for Windows File Server.
- Esegui una sincronizzazione finale della configurazione della condivisione di file. Per ulteriori informazioni, consulta Migrazione delle configurazioni di condivisione di file su Amazon FSx.

Configura gli SPN per l'autenticazione Kerberos

Ti consigliamo di utilizzare l'autenticazione e la crittografia basate su Kerberos in transito con Amazon FSx. Kerberos fornisce l'autenticazione più sicura per i client che accedono al file system. Per abilitare l'autenticazione Kerberos per i client che accedono ad Amazon FSx utilizzando un alias DNS, devi aggiungere nomi principali di servizio (SPN) che corrispondono all'alias DNS sull'oggetto computer Active Directory del tuo file system Amazon FSx.

Sono necessari due SPN per l'autenticazione Kerberos.

```
HOST/alias
HOST/alias.domain
```

Ad esempio, se l'alias è`finance.domain.com`, i due SPN richiesti sono i seguenti.

```
HOST/finance
HOST/finance.domain.com
```

Un SPN può essere associato solo a un singolo oggetto computer Active Directory alla volta. Se esistono SPN esistenti per il nome DNS configurato per l'oggetto computer Active Directory del file system originale, è necessario eliminarli prima di creare SPN per il file system Amazon FSx.

Le seguenti procedure descrivono come trovare eventuali SPN esistenti, eliminarli e creare nuovi SPN per l'oggetto informatico Active Directory del tuo file system Amazon FSx.

Per installare il modulo Active Directory richiesto PowerShell

1. Accedi a un'istanza Windows aggiunta all'Active Directory a cui è collegato il tuo file system Amazon FSx.
2. Apri PowerShell come amministratore.
3. Installa il modulo PowerShell Active Directory utilizzando il seguente comando.

```
Install-WindowsFeature RSAT-AD-PowerShell
```

Per trovare ed eliminare gli alias DNS esistenti, SPN sull'oggetto computer Active Directory del file system originale

1. Trova tutti gli SPN esistenti utilizzando i seguenti comandi. Sostituiscilo *alias_fqdn* con l'alias DNS che hai associato al file system in. Migrazione della configurazione DNS per utilizzare Amazon FSx

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. Eliminare gli SPN HOST esistenti restituiti nel passaggio precedente utilizzando lo script di esempio seguente.

   - Sostituiscilo *alias_fqdn* con l'alias DNS completo in cui hai associato il file system. Migrazione della configurazione DNS per utilizzare Amazon FSx
   - Sostituisci *file_system_DNS_name* con il nome DNS del file system originale.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
```

```
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. Ripeti questi passaggi per ogni alias DNS associato al file system in. Migrazione della configurazione DNS per utilizzare Amazon FSx

Per impostare gli SPN sull'oggetto computer Active Directory del tuo file system Amazon FSx

1. Imposta nuovi SPN per il tuo file system Amazon FSx eseguendo i seguenti comandi.

   - Sostituisci *file_system_DNS_name* con il nome DNS assegnato da Amazon FSx al file system.

     Per trovare il nome DNS del tuo file system sulla console Amazon FSx, scegli File system e scegli il tuo file system. Scegli il pannello Rete e sicurezza della pagina dei dettagli del file system. Puoi anche ottenere il nome DNS nella risposta dell'operazione DescribeFileSystems API.

   - Sostituiscilo *alias_fqdn* con l'alias DNS completo in cui hai associato il file system. Migrazione della configurazione DNS per utilizzare Amazon FSx

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> L'impostazione di un SPN per il file system Amazon FSx avrà esito negativo se nell'AD per l'oggetto computer del file system originale esiste un SPN per l'alias DNS. Per informazioni su come trovare ed eliminare gli SPN esistenti, consulta. Per trovare ed eliminare gli alias DNS esistenti, SPN sull'oggetto computer Active Directory del file system originale

2. Verifica che i nuovi SPN siano configurati per l'alias DNS utilizzando lo script di esempio seguente. Assicurati che la risposta includa due HOST SPN e. `HOST/alias` `HOST/alias_fqdn`

   Sostituisci *`file_system_DNS_name`* con il nome DNS assegnato da Amazon FSx al tuo file system. Per trovare il nome DNS del tuo file system sulla console Amazon FSx, scegli File system, scegli il tuo file system, quindi scegli il pannello Rete e sicurezza nella pagina dei dettagli del file system.

   Puoi anche ottenere il nome DNS nella risposta dell'operazione DescribeFileSystems API.

   ```
   ## Verify SPNs on FSx file system AD computer object
   $FileSystemDnsName = "file_system_dns_name"
   $FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
   [0].Name.Split(".")[0]
   $FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
   SetSpn /L ${FSxAdComputer}.Name
   ```

3. Ripeti i passaggi precedenti per ogni alias DNS associato al file system in. Migrazione della configurazione DNS per utilizzare Amazon FSx

> **Note**
>
> Puoi applicare l'autenticazione e la crittografia Kerberos in transito con i client che si connettono al file system utilizzando alias DNS impostando i seguenti Group Policy Object (GPO) in Active Directory:
>
> - Limita NTLM: traffico NTLM in uscita verso server remoti
> - Limita NTLM: aggiungi eccezioni del server remoto per l'autenticazione NTLM

Per ulteriori informazioni, consulta Applicazione dell'autenticazione Kerberos tramite GPO la procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.

Aggiornamento dei record DNS CNAME per il file system Amazon FSx

Dopo aver configurato correttamente gli SPN per il tuo file system, puoi passare ad Amazon FSx sostituendo ogni record DNS risolto nel file system originale con un record DNS che si risolve nel nome DNS predefinito del file system Amazon FSx.

PowerShell Per installare i cmdlet richiesti

1. Accedi a un'istanza Windows aggiunta ad Active Directory a cui fa parte il tuo file system Amazon FSx come utente membro di un gruppo con autorizzazioni di amministrazione DNS (AWS Delegated Domain Name System Administrators in Managed AWS Microsoft Active Directory e Domain Admins o un altro gruppo a cui hai delegato le autorizzazioni di amministrazione DNS nel tuo Active Directory autogestito)

   Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
2. Apri PowerShell come amministratore.
3. Il modulo server PowerShell DNS è necessario per eseguire le istruzioni di questa procedura. Installarlo utilizzando il comando seguente.

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

Per aggiornare un record DNS CNAME esistente

1. Lo script seguente aggiorna tutti i record DNS CNAME esistenti *alias_fqdn* per l'oggetto computer del file system Amazon FSx. Se non ne viene trovato nessuno, crea un nuovo record DNS CNAME per l'alias DNS *alias_fqdn* che si risolve nel nome DNS predefinito per il file system Amazon FSx.

   Per eseguire lo script:

   - Sostituiscilo *alias_fqdn* con l'alias DNS associato al file system.

- Sostituisci *file_system_DNS_name* con il nome DNS predefinito che Amazon FSx ha assegnato al file system.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name)[0]

Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

2. Ripeti il passaggio precedente per ogni alias DNS associato al file system. Migrazione della configurazione DNS per utilizzare Amazon FSx

Utilizzo di FSx for Windows File Server con Microsoft SQL Server

Microsoft SQL Server ad alta disponibilità (HA) viene in genere distribuito su più nodi di database in un Windows Server Failover Cluster (WSFC), con ogni nodo che ha accesso all'archiviazione condivisa dei file. È possibile utilizzare FSx for Windows File Server come archiviazione condivisa per le distribuzioni di Microsoft SQL Server ad alta disponibilità (HA) in due modi: come archiviazione per file di dati attivi e come testimone di condivisione di file SMB.

> **Note**
>
> Attualmente, Amazon FSx non supporta la funzionalità IFI (Instant File Initialization) di Microsoft SQL Server.

L'archiviazione SSD è consigliata per SQL Server. Lo storage SSD è progettato per i carichi di lavoro con le prestazioni più elevate e più sensibili alla latenza, inclusi i database.

Per informazioni sull'utilizzo di Amazon FSx per ridurre la complessità e i costi delle implementazioni di SQL Server ad alta disponibilità, consulta i seguenti post sul blog sulloAWS storage:

- Semplifica le implementazioni ad alta disponibilità di Microsoft SQL Server utilizzando Amazon FSx for Windows File Server
- Ottimizzazione dei costi per le implementazioni di SQL Server ad alta disponibilità suAWS
- Semplifica le implementazioni di SQL Server Always On conAWS Launch Wizard e Amazon FSx

Utilizzo di Amazon FSx per i file di dati di SQL Server attivi

Microsoft SQL Server può essere distribuito con una condivisione di file SMB come opzione di archiviazione per i file di dati attivi. Amazon FSx è ottimizzato per fornire storage condiviso per database SQL Server supportando le condivisioni di file CA (Continuous Available). Queste condivisioni di file sono progettate per applicazioni come SQL Server che richiedono l'accesso ininterrotto ai dati dei file condivisi. Sebbene sia possibile creare condivisioni CA su file system Single-AZ 2, è necessario utilizzare le condivisioni CA sui file system Multi-AZ per tutte le distribuzioni di SQL Server, che abbiano o meno.

Crea una condivisione disponibile in modo continuo

Puoi creare condivisioni CA utilizzando l'interfaccia a riga di comando di Amazon FSx per la gestione remota su PowerShell. Per specificare che la condivisione è una condivisione disponibile in modo continuo, utilizzare l'opzione`New-FSxSmbShare` con l'`-ContinuouslyAvailable`opzione impostata su`$True`. Per ulteriori informazioni sulla creazione di una nuova condivisione FCA, consultaCreazione di una condivisione a disponibilità continua (CA).

Configurazione delle impostazioni di timeout SMB

Come descritto inProcesso di failover per FSx for Windows File Server, il failover e il failback per Multi-AZ possono causare pause di I/O che in genere si completano in meno di 30 secondi. L'applicazione SQL Server può avere una sensibilità diversa alle impostazioni di timeout a seconda di come è configurata.

È possibile ottimizzare il timeout della sessione di configurazione del client SMB per assicurarsi che l'applicazione sia resiliente ai failover del file system Multi-AZ. È possibile testare il comportamento dell'applicazione durante i failover aggiornando la capacità di throughput del file system, che avvia un failover e un failback automatici.

Utilizzo di Amazon FSx come testimone di condivisione di file SMB

Le distribuzioni di cluster Windows Server Failover in genere implementano un testimone di condivisione di file SMB per mantenere il quorum delle risorse del cluster. Le condivisioni di file Witness richiedono solo una piccola quantità di spazio di archiviazione per le informazioni sul quorum. I file system Amazon FSx possono essere utilizzati come testimoni di condivisione di file SMB per le implementazioni di cluster di failover di Windows Server.

Utilizzo di FSx for Windows File Server con Amazon Kendra

Amazon Kendra è un servizio di ricerca estremamente accurato e intelligente. I file system FSx for Windows File Server possono essere utilizzati come origini dati per Amazon Kendra, consentendo di indicizzare e cercare in modo intelligente le informazioni contenute nei documenti archiviati nel file system.

- Per ulteriori informazioni su Amazon Kendra, consultaChe cos'è Amazon KendranellaGuida per sviluppatori di Amazon Kendra.
- Per ulteriori informazioni su come aggiungere il file system come origine dati Amazon Kendra, consultaCome iniziare a utilizzare un'origine dati Amazon FSx (console)nellaGuida per sviluppatori di Amazon Kendra.
- Per informazioni generali su Amazon Kendra, consulta laSito web Amazon Kendra.
- Per una panoramica su come effettuare ricerche nel file system utilizzando Amazon Kendra, consultaCerca in modo sicuro i dati non strutturati sui file system Windows con il connettore Amazon Kendra per Amazon FSx for Windows File ServersulAWSBlog Machine Learning.

Prestazioni del file system

Quando aggiungi un file system FSx for Windows File Server come origine dati, Amazon Kendra esegue la scansione dei file e delle cartelle del file system su una frequenza di sincronizzazione regolare per creare e mantenere l'indice di ricerca. (È possibile selezionare la frequenza di sincronizzazione quando si stabilisce l'integrazione.) Questa attività di accesso ai file di Amazon Kendra consumerà risorse del file system, in modo simile alle attività dei tuoi carichi di lavoro che accedono al file system.

Assicurati che il file system sia configurato con risorse sufficienti in modo che le prestazioni del carico di lavoro non siano influenzate. In particolare, se si prevede di indicizzare un numero elevato di file, si consiglia di utilizzare un file system con tipo di storage SSD, che fornisce un throughput massimo più elevato e livelli IOPS per le richieste che devono accedere ai volumi di storage.

Per ulteriori informazioni sul modello di prestazioni Amazon FSx, consultaPrestazioni di FSx for Windows File Server.

Protezione dei dati con backup, copie shadow e repliche pianificate

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

- I backup nativi di Amazon FSx supportano le esigenze di conservazione e conformità dei backup all'interno di Amazon FSx.
- AWS Backup i backup dei tuoi file system Amazon FSx fanno parte di una soluzione di backup centralizzata e automatizzata per AWS tutti i servizi nel cloud e in locale.
- Le copie shadow di Windows consentono agli utenti di annullare facilmente le modifiche ai file e confrontare le versioni dei file ripristinando i file nelle versioni precedenti.
- AWS DataSync la replica pianificata del file system Amazon FSx su un secondo file system fornisce protezione e ripristino dei dati.

Argomenti

Utilizzo dei backup

Con Amazon FSx, i backup sono file-system-consistent altamente durevoli e incrementali. Ogni backup contiene tutte le informazioni necessarie per creare un nuovo file system, ripristinando efficacemente un' point-in-time istantanea del file system. Per garantire la coerenza del file system, Amazon FSx utilizza il Volume Shadow Copy Service (VSS) in Microsoft Windows. Per garantire un'elevata durabilità, Amazon FSx archivia i backup in Amazon Simple Storage Service (Amazon S3).

I backup di Amazon FSx sono incrementali, indipendentemente dal fatto che vengano generati utilizzando il backup giornaliero automatico o la funzionalità di backup avviato dall'utente. Ciò significa che vengono salvati solo i dati sul file system che sono stati modificati dopo il backup più recente. Ciò riduce al minimo il tempo necessario per creare il backup e consente di risparmiare sui costi di archiviazione evitando la duplicazione dei dati.

Ad un certo punto del processo di backup, l'I/O dello storage può essere sospeso brevemente, in genere per alcuni secondi. Poiché il servizio VSS deve svuotare tutte le scritture memorizzate nella cache su disco prima di riprendere l'I/O, la durata della pausa può essere più lunga se il carico di lavoro prevede una grande quantità di operazioni di scrittura al secondo (). `DataWriteOperations` La maggior parte degli utenti finali e delle applicazioni sperimenterà questa sospensione dell'I/O come una breve pausa di I/O. Le applicazioni possono avere una sensibilità diversa alle impostazioni di timeout a seconda di come sono configurate.

La creazione di backup regolari per il tuo file system è una best practice che completa la replica che Amazon FSx for Windows File Server esegue per il tuo file system. I backup Amazon FSx aiutano a supportare le esigenze di conservazione e conformità dei backup. Lavorare con i backup di Amazon FSx è semplice, che si tratti di creare backup, copiare un backup, ripristinare un file system da un backup o eliminare un backup. Tieni presente che per visualizzare l'utilizzo di un singolo backup del file system, dovrai abilitare i tag per quel backup specifico e abilitare i report di fatturazione basati su tag.

Argomenti

Utilizzo di backup giornalieri automatici

Per impostazione predefinita, Amazon FSx esegue un backup giornaliero automatico del file system. Questi backup giornalieri automatici vengono eseguiti durante la finestra di backup giornaliera stabilita al momento della creazione del file system. Quando scegli la finestra di backup giornaliera, ti consigliamo di scegliere un momento della giornata conveniente. Questo orario è idealmente al di fuori del normale orario di funzionamento delle applicazioni che utilizzano il file system.

I backup giornalieri automatici vengono conservati per un determinato periodo di tempo, noto come periodo di conservazione. Quando crei un file system nella console Amazon FSx, il periodo di conservazione del backup giornaliero automatico predefinito è di 30 giorni. Il periodo

di conservazione predefinito è diverso nell'API e nella CLI di Amazon FSx. Puoi impostare il periodo di conservazione in modo che sia compreso tra 0 e 90 giorni. L'impostazione del periodo di conservazione su 0 (zero) giorni disattiva i backup giornalieri automatici. I backup giornalieri automatici vengono eliminati quando il file system viene eliminato.

> **Note**
>
> L'impostazione del periodo di conservazione su 0 giorni significa che il backup del file system non viene mai eseguito automaticamente. Si consiglia vivamente di utilizzare backup giornalieri automatici per file system a cui sono associati qualsiasi livello di funzionalità critiche.

Puoi utilizzare l'SDK AWS CLI o uno degli AWS SDK per modificare la finestra di backup e il periodo di conservazione dei backup per i tuoi file system. Utilizza l'operazione `UpdateFileSystem`API o il comando `update-file-system`CLI. Per ulteriori informazioni, consulta Procedura passo per passo Aggiornare un file system esistente.

Utilizzo dei backup avviati dall'utente

Con Amazon FSx, puoi eseguire manualmente il backup dei tuoi file system in qualsiasi momento. Puoi farlo utilizzando la console Amazon FSx, l'API o AWS Command Line Interface ()AWS CLI. I backup avviati dall'utente dei file system Amazon FSx non scadono mai e sono disponibili per tutto il tempo che desideri conservarli. I backup avviati dall'utente vengono conservati anche dopo l'eliminazione del file system di cui era stato eseguito il backup. Puoi eliminare i backup avviati dall'utente solo utilizzando la console Amazon FSx, l'API o la CLI. Non vengono mai eliminati automaticamente da Amazon FSx. Per ulteriori informazioni, consulta Eliminazione di backup.

Se un backup viene avviato mentre il file system viene modificato (ad esempio durante un aggiornamento della capacità di throughput o durante la manutenzione del file system), la richiesta di backup viene messa in coda e riprenderà al termine dell'attività.

Creazione di backup avviati dall'utente

La procedura seguente illustra come creare un backup avviato dall'utente nella console Amazon FSx per un file system esistente.

Per creare un backup del file system avviato dall'utente

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

2. Dalla dashboard della console, scegli il nome del file system di cui desideri eseguire il backup.
3. Da Azioni, scegli Crea backup.
4. Nella finestra di dialogo Crea backup che si apre, fornisci un nome per il backup. I nomi di Backup possono contenere un massimo di 256 caratteri Unicode, inclusi lettere, spazi bianchi, numeri e caratteri speciali. + - = _:/
5. Scegliere Create backup (Crea backup).

A questo punto è stato creato il backup del file system. Puoi trovare una tabella di tutti i tuoi backup nella console Amazon FSx 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.

Utilizzo AWS Backup con Amazon FSx

AWS Backup è un modo semplice ed economico per proteggere i dati eseguendo il backup dei file system Amazon FSx. AWS Backup è un servizio di backup unificato progettato per semplificare la creazione, la copia, il ripristino e l'eliminazione dei backup, fornendo al contempo report e controlli migliorati. AWS Backup semplifica lo sviluppo di una strategia di backup centralizzata per la conformità legale, normativa e professionale. AWS Backup semplifica inoltre la protezione dei volumi di AWS storage, dei database e dei file system fornendo una posizione centrale in cui è possibile eseguire le seguenti operazioni:

- Configura e controlla le AWS risorse di cui desideri eseguire il backup.
- Automatizzare la pianificazione dei backup.
- Impostare le policy di conservazione.
- Copia i backup tra AWS regioni e tra AWS account.
- Monitora tutte le attività recenti di backup, copia e ripristino.

AWS Backup utilizza la funzionalità di backup integrata di Amazon FSx. I backup eseguiti dalla AWS Backup console hanno lo stesso livello di coerenza e prestazioni del file system e le stesse opzioni di ripristino dei backup eseguiti tramite la console Amazon FSx. I backup AWS Backup prelevati sono incrementali rispetto a qualsiasi altro backup Amazon FSx che esegui, avviati dall'utente o automatici.

Se gestisci questi backup, ottieni funzionalità aggiuntive, come opzioni di conservazione illimitate e la possibilità di creare backup pianificati con una frequenza ogni ora. AWS Backup Inoltre, AWS Backup conserva i backup immutabili anche dopo l'eliminazione del file system di origine. Ciò protegge dall'eliminazione accidentale o dannosa.

I backup eseguiti da AWS Backup sono considerati backup avviati dall'utente e vengono conteggiati ai fini della quota di backup avviata dall'utente per Amazon FSx. Puoi visualizzare e ripristinare i backup eseguiti AWS Backup nella console Amazon FSx, nella CLI e nell'API. Tuttavia, non puoi eliminare i backup eseguiti nella console, AWS Backup nella CLI o nell'API di Amazon FSx. Per ulteriori informazioni su come eseguire il backup dei file system Amazon FSx, consulta Working with Amazon FSx File System nella Developer Guide. AWS Backup AWS Backup

Copia di backup

Puoi utilizzare Amazon FSx per copiare manualmente i backup all'interno dello stesso AWS account in un'altra AWS regione (copie tra regioni) o all'interno della stessa regione (copie interne alla AWS regione). È possibile effettuare copie tra regioni solo all'interno della stessa partizione. AWS Puoi creare copie di backup avviate dall'utente utilizzando la console o l'API Amazon FSx. AWS CLI Quando crei una copia di backup avviata dall'utente, ha il seguente tipo. `USER_INITIATED`

È inoltre possibile utilizzare AWS Backup per copiare i backup tra AWS regioni e tra account. AWS AWS Backup è un servizio di gestione dei backup completamente gestito che fornisce un'interfaccia centrale per piani di backup basati su policy. Grazie alla sua gestione tra account, è possibile utilizzare automaticamente le policy di backup per applicare piani di backup a tutti gli account dell'organizzazione.

Le copie di backup in più regioni sono particolarmente utili per il disaster recovery in più regioni. I backup vengono eseguiti e copiati in un'altra AWS regione in modo che, in caso di emergenza nella AWS regione principale, sia possibile eseguire il ripristino dal backup e ripristinare rapidamente la disponibilità nell'altra regione. AWS È inoltre possibile utilizzare copie di backup per clonare il set di dati dei file in un'altra AWS regione o all'interno della stessa regione. AWS Puoi creare copie di backup all'interno dello stesso AWS account (interregionale o regionale) utilizzando la console Amazon FSx o l'API AWS CLI Amazon FSx. Puoi anche utilizzarla AWS Backupper eseguire copie di backup, su richiesta o basate su policy.

Le copie di backup su più account sono utili per soddisfare i requisiti di conformità normativa relativi alla copia dei backup su un account isolato. Forniscono inoltre un ulteriore livello di protezione dei dati per aiutare a prevenire l'eliminazione accidentale o dolosa dei backup, la perdita di credenziali o la compromissione delle chiavi. AWS KMS I backup su più account supportano il fan-in (copia dei

backup da più account primari su un account di copia di backup isolato) e il fan-out (copia i backup da un account principale a più account di copia di backup isolati).

È possibile creare copie di backup su più account utilizzando with support. AWS Backup AWS Organizations I limiti degli account per le copie su più account sono definiti dalle AWS Organizations politiche. Per ulteriori informazioni sull'utilizzo per AWS Backup creare copie di backup su più account, consulta Creazione di copie di backup Account AWS nella Guida per gli AWS Backup sviluppatori.

Limitazioni relative alla copia di backup

Di seguito sono riportate alcune limitazioni relative alla copia dei backup:

- Le copie di backup interregionali sono supportate solo tra due AWS regioni commerciali qualsiasi, tra le regioni Cina (Pechino) e Cina (Ningxia) e tra le regioni AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali), ma non tra questi set di regioni.
- Le copie di backup interregionali non sono supportate nelle regioni che hanno scelto di aderire.
- È possibile creare copie di backup all'interno di qualsiasi regione. AWS
- Il backup di origine deve avere lo stato di `AVAILABLE` prima di poterlo copiare.
- Non è possibile eliminare un backup di origine se viene copiato. Potrebbe verificarsi un breve ritardo tra il momento in cui il backup di destinazione diventa disponibile e il momento in cui è consentito eliminare il backup di origine. È necessario tenere presente questo ritardo se si tenta di eliminare nuovamente un backup di origine.
- Puoi avere fino a cinque richieste di copie di backup in corso in un'unica AWS regione di destinazione per account.

Autorizzazioni per le copie di backup in più regioni

Si utilizza una dichiarazione di policy IAM per concedere le autorizzazioni per eseguire un'operazione di copia di backup. Per comunicare con la AWS regione di origine e richiedere una copia di backup su più regioni, il richiedente (ruolo IAM o utente IAM) deve avere accesso al backup di origine e alla regione di origine. AWS

La policy viene utilizzata per concedere le autorizzazioni all'`CopyBackup`azione per l'operazione di copia di backup. Si specifica l'azione nel `Action` campo della politica e si specifica il valore della risorsa nel `Resource` campo della politica, come nell'esempio seguente.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111111111111:backup/*"
        }
    ]
}
```

Per ulteriori informazioni sulle policy IAM, consulta Policies and permissions in IAM nella IAM User Guide.

Copie complete e incrementali

Quando copi un backup su una AWS regione di destinazione o su un AWS account di destinazione diverso dal backup di origine, la prima copia è una copia di backup completa, anche se utilizzi la stessa chiave KMS per crittografare sia le copie di origine che quelle di destinazione del backup.

Dopo la prima copia di backup, tutte le copie di backup successive nella stessa regione di destinazione all'interno dello stesso AWS account sono incrementali, a condizione che non siano stati eliminati tutti i backup precedentemente copiati in quella regione e che sia stata utilizzata la stessa AWS KMS chiave. Se nessuna delle due condizioni non viene soddisfatta, l'operazione di copia genera una copia di backup completa (non incrementale).

Per copiare un backup all'interno dello stesso account (interregionale o regionale) utilizzando la console

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione, scegliere Backup.
3. Nella tabella Backup, scegli il backup che desideri copiare, quindi scegli Copia backup.
4. Nella sezione Rule settings (Impostazioni regole), procedi nel seguente modo:
    - Nell'elenco Regione di destinazione, scegli una AWS regione di destinazione in cui copiare il backup. La destinazione può trovarsi in un'altra AWS regione (copia interregionale) o all'interno della stessa AWS regione (copia interna all'area).
    - (Facoltativo) Seleziona Copia tag per copiare i tag dal backup di origine al backup di destinazione. Se selezioni Copia tag e aggiungi anche tag al passaggio 6, tutti i tag vengono uniti.

5. Per Crittografia, scegli la chiave di AWS KMS crittografia per crittografare il backup copiato.
6. Per Tag: facoltativo, inserisci una chiave e un valore per aggiungere tag per il backup copiato. Se aggiungi tag qui e hai selezionato anche Copia tag al passaggio 4, tutti i tag vengono uniti.
7. Scegli Copia backup.

Il backup viene copiato all'interno dello stesso AWS account nella regione selezionata AWS .

Per copiare un backup all'interno dello stesso account (interregionale o interregionale) utilizzando la CLI

- Utilizza il comando `copy-backup` CLI o l'operazione CopyBackupAPI per copiare un backup all'interno dello stesso AWS account, in una AWS regione o all'interno di una AWS regione.

  Il comando seguente copia un backup con un ID `backup-0abc123456789cba7` proveniente dalla `us-east-1` regione.

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  La risposta mostra la descrizione del backup copiato.

  Puoi visualizzare i tuoi backup sulla console Amazon FSx o a livello di codice utilizzando `describe-backups` il comando CLI o l'operazione API. DescribeBackups

Ripristino dei backup

È possibile utilizzare un backup disponibile per creare un nuovo file system, ripristinando in modo efficace un' point-in-time istantanea di un altro file system. Puoi ripristinare un backup utilizzando la console o uno degli AWS SDK. AWS CLI Il ripristino di un backup su un nuovo file system richiede lo stesso tempo della creazione di un nuovo file system. I dati ripristinati dal backup vengono caricati lentamente sul file system, durante il quale si verificherà una latenza leggermente superiore.

Per garantire che gli utenti possano continuare ad accedere al file system ripristinato, assicurati che il dominio Active Directory associato al file system ripristinato sia lo stesso del file system originale o che sia considerato affidabile dal dominio AD del file system originale. Per ulteriori informazioni su Active Directory, vedereUtilizzo di Microsoft Active Directory in FSx for Windows File Server.

La procedura seguente illustra come ripristinare un backup utilizzando la console per creare un nuovo file system.

> **Note**
>
> È possibile ripristinare il backup solo su un file system dello stesso tipo di distribuzione e capacità di archiviazione dell'originale. È possibile aumentare la capacità di archiviazione del file system ripristinato non appena sarà disponibile. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione.

Per ripristinare un file system da un backup

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard della console, scegli Backup dalla barra di navigazione a sinistra.
3. Scegli il backup che desideri ripristinare dalla tabella Backup, quindi scegli Ripristina backup.

   In questo modo si apre la procedura guidata per la creazione del file system. Questa procedura guidata è identica alla procedura guidata standard per la creazione del file system, tranne per il fatto che il tipo di distribuzione e la capacità di archiviazione sono già impostati e non possono essere modificati. Tuttavia, puoi modificare la capacità di throughput, il VPC associato e altre impostazioni e il tipo di archiviazione. Il tipo di archiviazione è impostato su SSD per impostazione predefinita, ma è possibile modificarlo in HDD nelle seguenti condizioni:

   - Il tipo di implementazione del file system è Multi-AZ o Single-AZ 2.
   - La capacità di storage è di almeno 2.000 GiB.
4. Completa la procedura guidata come quando crei un nuovo file system.
5. Scegliere Review and create (Rivedi e crea).
6. Controlla le impostazioni che hai scelto per il tuo file system Amazon FSx, quindi scegli Crea file system.

Hai eseguito il ripristino da un backup e ora viene creato un nuovo file system. Quando il suo stato cambia a`AVAILABLE`, è possibile utilizzare il file system normalmente.

Eliminazione di backup

L'eliminazione di un backup è un'azione permanente e irrecuperabile. Vengono eliminati anche tutti i dati contenuti in un backup eliminato. Non eliminate un backup a meno che non siate sicuri di non averne più bisogno in futuro. Non puoi eliminare i backup eseguiti da AWS Backup, che hanno il tipo AWS Backup, nella console Amazon FSx, nella CLI o nell'API.

Per eliminare un backup

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dalla dashboard della console, scegli Backup dalla barra di navigazione a sinistra.
3. Scegli il backup che desideri eliminare dalla tabella Backup, quindi scegli Elimina backup.
4. Nella finestra di dialogo Elimina backup che si apre, verifica che l'ID del backup identifichi il backup che desideri eliminare.
5. Conferma che la casella di controllo sia selezionata per il backup che desideri eliminare.
6. Scegli Elimina backup.

Il backup e tutti i dati inclusi vengono ora eliminati in modo permanente e irrecuperabile.

Dimensioni dei backup

La dimensione dei backup viene determinata utilizzando lo storage utilizzato nel file system, anziché la capacità di storage totale fornita. La dimensione dei backup dipenderà dalla capacità di archiviazione utilizzata e dalla quantità di dati generati dal file system. A seconda di come i dati vengono distribuiti tra i volumi di storage del file system e della frequenza con cui vengono modificati, l'utilizzo totale del backup può essere superiore o inferiore alla capacità di storage utilizzata. Quando si elimina un backup, vengono rimossi solo i dati esclusivi di quel backup. Con Amazon FSx, i risparmi in termini di efficienza di storage derivanti dalla deduplicazione e dalla compressione si applicano non solo allo storage SSD/HDD principale, ma anche ai backup.

Per fornire file-system-consistent backup durevoli e incrementali, Amazon FSx esegue il backup dei dati a livello di blocco. I dati sui volumi di storage del file system possono essere archiviati su più blocchi a seconda dello schema in cui sono stati scritti o sovrascritti. Di conseguenza, la dimensione totale dell'utilizzo del backup potrebbe non corrispondere alla dimensione esatta dei file e delle directory sul file system.

L'utilizzo e il costo complessivi del backup sono disponibili nella AWS Billing Dashboard o AWS Cost Management Console. Per calcolare le dimensioni e il costo dei backup dei singoli file system, puoi etichettare i singoli backup e abilitare i report di fatturazione basati su tag.

Protezione dei dati con copie shadow

Una copia shadow di Microsoft Windows è un'istantanea di un file system Windows in un determinato momento. Con le copie shadow abilitate, gli utenti possono recuperare rapidamente i file eliminati o modificati archiviati in rete e confrontare le versioni dei file. Gli amministratori dello storage possono facilmente pianificare l'esecuzione periodica di copie shadow utilizzando PowerShell i comandi di Windows.

Le copie shadow vengono archiviate insieme ai dati del file system e consumano la capacità di storage del file system solo per le parti modificate dei file. Tutte le copie shadow archiviate nel vostro file system sono incluse nei backup dei file system.

> **Note**
>
> Per impostazione predefinita, le copie shadow non sono abilitate su FSx for Windows File Server. Per proteggere i dati sul file system utilizzando copie shadow, è necessario abilitare le copie shadow e impostare una pianificazione delle copie shadow sul file system. Per ulteriori informazioni, consulta Configurazione delle copie shadow per utilizzare l'archiviazione e la pianificazione predefinite.

> **Warning**
>
> Le copie shadow non sostituiscono i backup. Se abilitate le copie shadow, assicuratevi di continuare a eseguire backup regolari.

Argomenti

- Procedure consigliate per l'utilizzo di copie shadow
- Configurazione di copie shadow
- Configurazione delle copie shadow per utilizzare l'archiviazione e la pianificazione predefinite
- Ripristino di singoli file e cartelle

- Impostazione della quantità massima di spazio di archiviazione per copie shadow
- Visualizzazione dello spazio di archiviazione delle copie shadow
- Eliminazione dello storage delle copie shadow, della pianificazione e di tutte le copie shadow
- Creazione di una pianificazione personalizzata delle copie shadow
- Visualizzazione della pianificazione delle copie shadow
- Eliminazione di una pianificazione di copie shadow
- Creazione di una copia shadow
- Visualizzazione delle copie shadow esistenti
- Eliminazione di copie shadow

Procedure consigliate per l'utilizzo di copie shadow

È possibile abilitare le copie shadow per il file system per consentire agli utenti finali di visualizzare e ripristinare singoli file o cartelle da un'istantanea precedente in Windows File Explorer. Amazon FSx utilizza la funzionalità di copie shadow fornita da Microsoft Windows Server. Utilizza queste best practice per le copie shadow:

- Assicurati che il tuo file system disponga di risorse prestazionali sufficienti: in base alla progettazione, Microsoft Windows utilizza un copy-on-write metodo per registrare le modifiche dal punto di copia shadow più recente e questa copy-on-write attività può comportare fino a tre operazioni di I/O per ogni operazione di scrittura di file.
- Usa l'archiviazione SSD e aumenta la capacità di throughput: poiché Windows richiede un livello elevato di prestazioni di I/O per conservare le copie shadow, consigliamo di utilizzare l'archiviazione SSD e aumentare la capacità di throughput fino a un valore tre volte superiore a quello del carico di lavoro previsto. Questo aiuta a garantire che il file system disponga di risorse sufficienti per evitare problemi come l'eliminazione indesiderata di copie shadow.
- Conservate solo il numero di copie shadow necessarie: se avete un gran numero di copie shadow, ad esempio più di 64 delle copie shadow più recenti, o copie shadow che occupano una grande quantità di storage (su scala TB) su un singolo file system, processi come il failover e il failback potrebbero richiedere un po' di tempo in più. Ciò è dovuto alla necessità che FSx for Windows esegua controlli di coerenza sullo storage shadow copy. È inoltre possibile riscontrare una maggiore latenza delle operazioni di I/O a causa della necessità che FSx for Windows esegua copy-on-write attività mantenendo le copie shadow. Per ridurre al minimo la disponibilità e l'impatto sulle prestazioni delle copie shadow, eliminate manualmente le copie shadow non utilizzate o configurate gli script per eliminare automaticamente le vecchie copie shadow dal file system.

> **Note**
>
> Durante gli eventi di failover per i file system Multi-AZ, FSx for Windows esegue un controllo di coerenza che richiede la scansione dello storage shadow copy sul file system prima che il nuovo file server attivo sia online. La durata del controllo di coerenza è correlata al numero di copie shadow sul file system e allo storage utilizzato. Per evitare eventi di failover e failback ritardati, si consiglia di conservare meno di 64 copie shadow sul file system e di seguire i passaggi seguenti per monitorare ed eliminare regolarmente le copie shadow più vecchie.

Configurazione di copie shadow

Abilita e pianifica copie shadow periodiche sul tuo file system utilizzando PowerShell i comandi Windows definiti da Amazon FSx. Di seguito sono riportate tre impostazioni principali per la configurazione delle copie shadow sul file system FSx for Windows File Server:

- Impostazione della quantità massima di storage che le copie shadow possono utilizzare sul file system
- (Facoltativo) Impostazione del numero massimo di copie shadow che possono essere archiviate nel file system. Il valore predefinito è 20.
- (Facoltativo) Impostazione di una pianificazione che definisca gli orari e gli intervalli in base ai quali scattare copie shadow, ad esempio giornaliere, settimanali e mensili

È possibile archiviare un massimo di 500 copie shadow per file system in qualsiasi momento; tuttavia, si consiglia di conservare meno di 64 copie shadow in qualsiasi momento per garantire disponibilità e prestazioni. Quando si raggiunge questo limite, la copia shadow successiva sostituisce la copia shadow più vecchia. Analogamente, quando viene raggiunto lo spazio di archiviazione massimo per le copie shadow, una o più delle copie shadow più vecchie vengono eliminate per creare spazio di archiviazione sufficiente per la copia shadow successiva.

Per informazioni su come abilitare e pianificare rapidamente copie shadow periodiche utilizzando le impostazioni predefinite di Amazon FSx, consulta. Configurazione delle copie shadow per utilizzare l'archiviazione e la pianificazione predefinite

Considerazioni sull'allocazione dello storage shadow copy

Una copia shadow è una copia a livello di blocco delle modifiche apportate ai file dopo l'ultima copia shadow. Non viene copiato l'intero file, ma solo le modifiche. Pertanto, le versioni precedenti

dei file in genere non occupano tanto spazio di archiviazione quanto il file corrente. La quantità di spazio di volume utilizzata per le modifiche può variare in base al carico di lavoro. Quando un file viene modificato, lo spazio di archiviazione utilizzato dalle copie shadow dipende dal carico di lavoro. Quando si determina la quantità di spazio di archiviazione da allocare per le copie shadow, è necessario tenere conto dei modelli di utilizzo del file system del carico di lavoro.

Quando si abilitano le copie shadow, è possibile specificare la quantità massima di spazio di archiviazione che le copie shadow possono consumare sul file system. Il limite predefinito è il 10 percento del file system. Ti consigliamo di aumentare il limite se gli utenti aggiungono o modificano spesso file. Se si imposta un limite troppo basso, è possibile che le copie shadow più vecchie vengano eliminate più spesso di quanto gli utenti si aspettino.

È possibile impostare lo storage delle copie shadow su unbounded ()`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`. Tuttavia, una configurazione illimitata può comportare un elevato numero di copie shadow che consumano lo storage del file system. Ciò potrebbe comportare una capacità di storage insufficiente per i carichi di lavoro. Se imposti uno storage illimitato, assicurati di scalare la capacità di archiviazione man mano che vengono raggiunti i limiti di shadow copy. Per informazioni sulla configurazione dello storage di copie shadow su una dimensione specifica o illimitato, consulta. Impostazione della quantità massima di spazio di archiviazione per copie shadow

Dopo aver abilitato le copie shadow, è possibile monitorare la quantità di spazio di archiviazione utilizzato dalle copie shadow. Per ulteriori informazioni, consulta Visualizzazione dello spazio di archiviazione delle copie shadow.

Considerazioni relative all'impostazione del numero massimo di copie shadow

Quando si abilitano le copie shadow, è possibile specificare il numero massimo di copie shadow memorizzate nel file system. Il limite predefinito è 20 e per ridurre al minimo la disponibilità e l'impatto sulle prestazioni delle copie shadow, Microsoft consiglia di configurare il numero massimo di copie shadow su meno di 64. Poiché Windows richiede un elevato livello di prestazioni di I/O per mantenere le copie shadow, si consiglia di utilizzare l'archiviazione SSD e aumentare la capacità di throughput fino a un valore tre volte superiore a quello del carico di lavoro previsto. Questo aiuta a garantire che il file system disponga di risorse sufficienti per evitare problemi come l'eliminazione indesiderata di copie shadow.

È possibile impostare il numero massimo di copie shadow fino a 500. Tuttavia, se si dispone di un numero elevato di copie shadow o copie shadow che occupano una grande quantità di storage (su scala TB) su un singolo file system, processi come il failover e il failback potrebbero richiedere

più tempo del previsto. Ciò è dovuto al fatto che Windows deve eseguire controlli di coerenza sullo storage shadow copy. È inoltre possibile riscontrare una maggiore latenza delle operazioni di I/O a causa della necessità che Windows esegua copy-on-write attività mantenendo le copie shadow.

Raccomandazioni relative ai file system per le copie shadow

Di seguito sono riportate le raccomandazioni relative ai file system per l'utilizzo delle copie shadow.

- Assicurati di fornire una capacità prestazionale sufficiente per le tue esigenze di carico di lavoro sul tuo file system. Amazon FSx offre la funzionalità Shadow Copies fornita da Microsoft Windows Server. In base alla progettazione, Microsoft Windows utilizza un copy-on-write metodo per registrare le modifiche dal punto di copia shadow più recente e questa copy-on-write attività può comportare fino a tre operazioni di I/O per ogni operazione di scrittura di file. Se Windows non è in grado di tenere il passo con la velocità in entrata delle operazioni di I/O al secondo, può causare l'eliminazione di tutte le copie shadow perché non è più in grado di gestire le copie shadow tramite. copy-on-write Pertanto, è importante fornire una capacità prestazionale di I/O sufficiente per le esigenze di carico di lavoro sul file system (sia la dimensione della capacità di throughput che determina le prestazioni di I/O del file server, sia il tipo e la capacità di storage che determinano le prestazioni di I/O dello storage).
- In genere si consiglia di utilizzare file system configurati con l'archiviazione SSD anziché l'archiviazione su HDD quando si abilitano le copie shadow, dato che Windows consuma prestazioni di I/O più elevate per mantenere le copie shadow e dato che lo storage su HDD offre una capacità di prestazioni inferiore per le operazioni di I/O.
- Il file system deve disporre di almeno 320 MB di spazio libero, oltre alla quantità massima di storage per copie shadow configurata (). `MaxSpace` Ad esempio, se sono stati assegnati 5 GB `MaxSpace` alle copie shadow, il file system deve sempre disporre di almeno 320 MB di spazio libero oltre ai 5 GB`MaxSpace`.

> **Warning**
>
> Quando configurate la pianificazione delle copie shadow, assicuratevi di non pianificare le copie shadow durante la migrazione dei dati o quando è pianificata l'esecuzione dei processi di deduplicazione dei dati. È necessario pianificare le copie shadow quando si prevede che il file system sia inattivo. Per informazioni sulla configurazione di una pianificazione personalizzata delle copie shadow, vedere. Creazione di una pianificazione personalizzata delle copie shadow

Configurazione delle copie shadow per utilizzare l'archiviazione e la pianificazione predefinite

Puoi configurare rapidamente copie shadow sul tuo file system utilizzando l'impostazione e la pianificazione predefinite dello storage shadow copy. L'impostazione predefinita di archiviazione delle copie shadow consente alle copie shadow di consumare al massimo il 10% della capacità di archiviazione del file system. Se si aumenta la capacità di storage del file system, la quantità di storage di copia shadow attualmente allocata non aumenta in modo analogo.

La pianificazione predefinita esegue automaticamente copie shadow ogni lunedì, martedì, mercoledì, giovedì e venerdì, alle 7:00 e alle 12:00 UTC.

Per impostare il livello predefinito di archiviazione delle copie shadow

1. Connect a un'istanza di calcolo Windows con connettività di rete con il file system.
2. Accedi all'istanza di calcolo di Windows come membro del gruppo di amministratori del file system. Nel AWS Managed Microsoft AD, quel gruppo è AWS Delegated FSx Administrators. In Microsoft AD autogestito, tale gruppo è Domain Admins o il gruppo personalizzato specificato per l'amministrazione al momento della creazione del file system. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
3. Imposta la quantità predefinita di shadow storage utilizzando il seguente comando. Sostituisci *FSxFileSystem-Remote-PowerShell-Endpoint* con l' PowerShell endpoint remoto Windows del file system che desideri amministrare. Puoi trovare l' PowerShell endpoint Windows Remote nella console Amazon FSx, nella sezione Rete e sicurezza della schermata dei dettagli del file system o nella risposta dell'operazione `DescribeFileSystem` dell'API.

   ```
   PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-FsxShadowStorage -Default}
   ```

   La risposta avrà il seguente aspetto.

   ```
   FSx Shadow Storage Configuration

   AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
   -------------- ---------    -------- -------------------
                0         0 10737418240                  20
   ```

Per impostare la pianificazione predefinita delle copie shadow

1. Connect a un'istanza di calcolo Windows con connettività di rete con il file system.
2. Accedi all'istanza di calcolo di Windows come membro del gruppo di amministratori del file system. Nel AWS Managed Microsoft AD, quel gruppo è AWS Delegated FSx Administrators. In Microsoft AD autogestito, tale gruppo è Domain Admins o il gruppo personalizzato specificato per l'amministrazione al momento della creazione del file system. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
3. Imposta la pianificazione di shadow copy predefinita utilizzando il seguente comando.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-FsxShadowCopySchedule -Default}
```

La risposta mostra la pianificazione predefinita che è ora impostata.

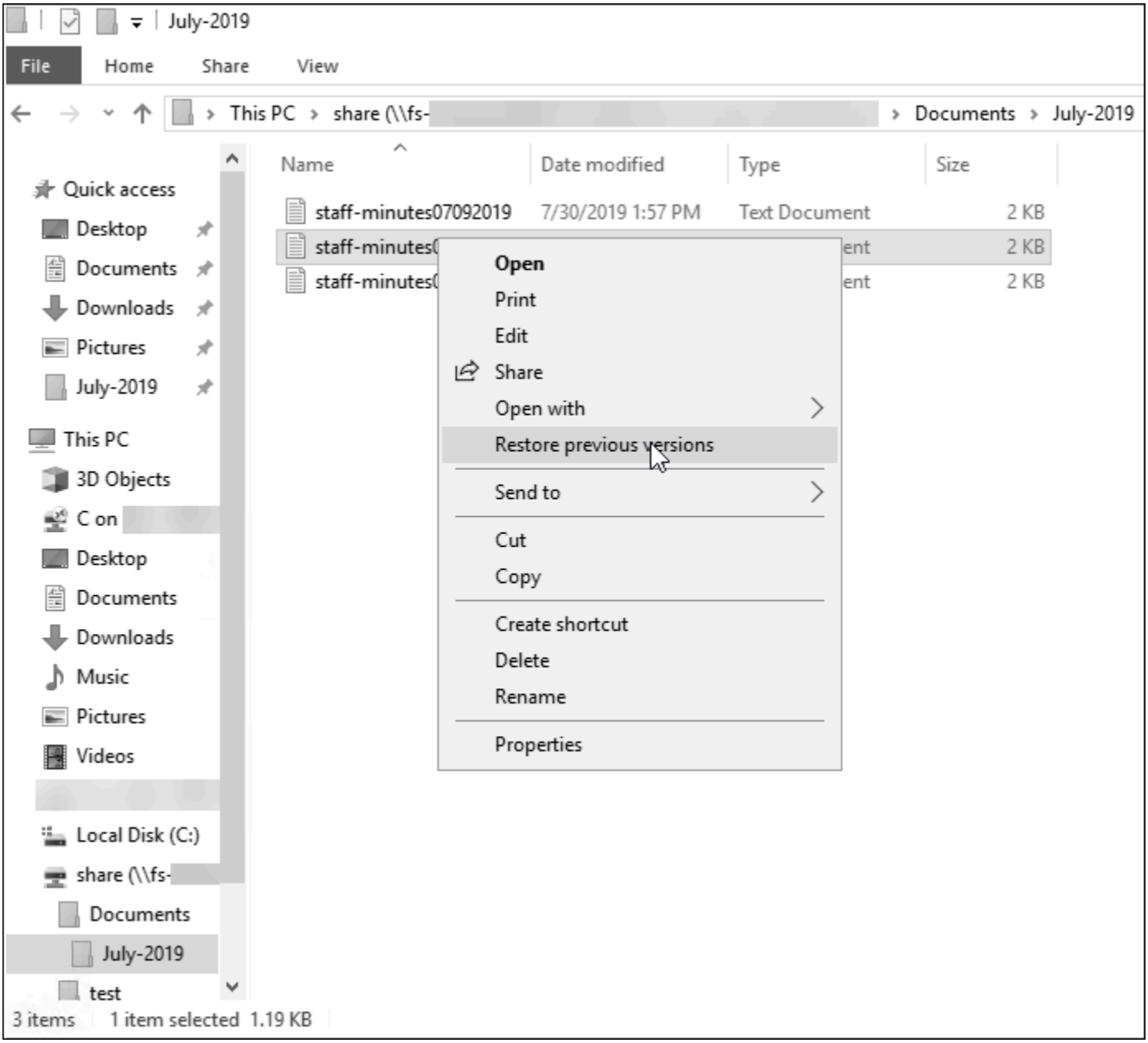
```
FSx Shadow Copy Schedule

Start Time                Days of week                            WeeksInterval
----------                ------------                            -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

Per ulteriori informazioni sulle opzioni aggiuntive e sulla creazione di una pianificazione personalizzata delle copie shadow, consultaCreazione di una pianificazione personalizzata delle copie shadow.

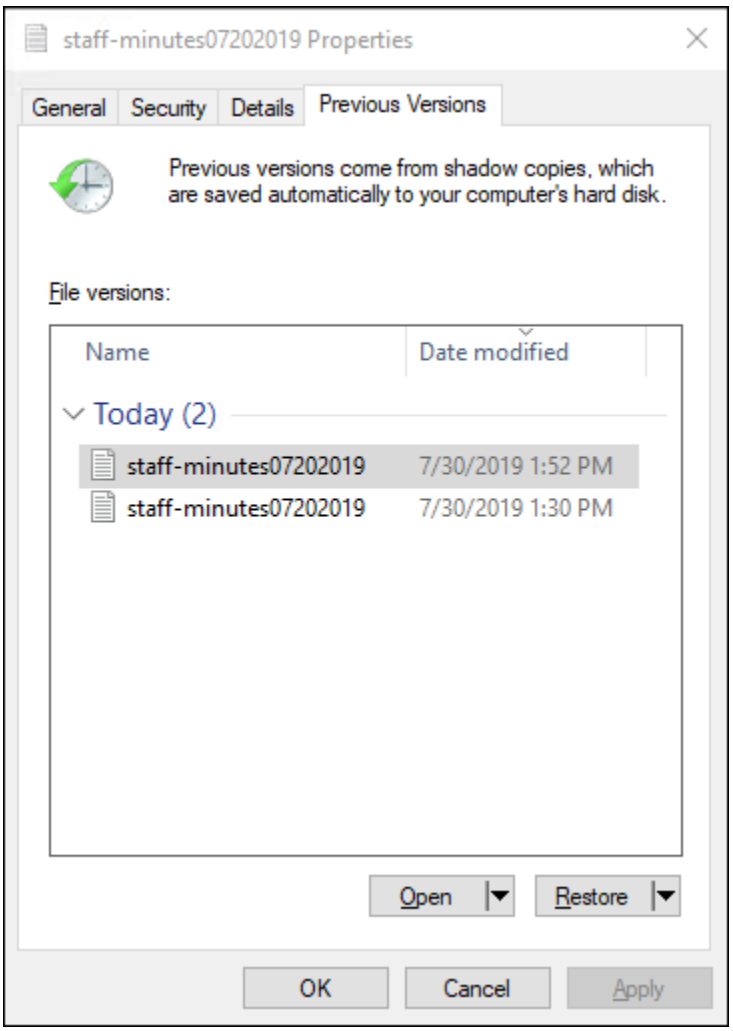
Ripristino di singoli file e cartelle

Dopo aver configurato le copie shadow sul file system Amazon FSx, gli utenti possono ripristinare rapidamente le versioni precedenti di singoli file o cartelle e recuperare i file eliminati.

Gli utenti ripristinano i file nelle versioni precedenti utilizzando la familiare interfaccia Windows File Explorer. Per ripristinare un file, scegli il file da ripristinare, quindi scegli Ripristina versioni precedenti dal menu contestuale (fai clic con il pulsante destro del mouse).



Gli utenti possono quindi visualizzare e ripristinare una versione precedente dall'elenco Versioni precedenti.



Impostazione della quantità massima di spazio di archiviazione per copie shadow

È possibile definire la quantità massima di spazio di archiviazione che le copie shadow possono utilizzare su un file system utilizzando il PowerShell comando `Set-FsxShadowStorage` personalizzato. È possibile specificare la dimensione massima che le copie shadow possono raggiungere utilizzando i `-Default` parametri `-Maxsize` o. Using `Default` imposta il valore massimo al 10% della capacità di archiviazione del file system. Non è possibile specificare i `-Default` parametri `-Maxsize` and nello stesso comando.

Utilizzando`-Maxsize`, è possibile definire l'archiviazione delle copie shadow come segue:

- In byte: `Set-FsxShadowStorage -Maxsize 2500000000`
- In kilobyte, megabyte, gigabyte o altre unità: o `Set-FsxShadowStorage -Maxsize (2500MB)` `Set-FsxShadowStorage -Maxsize (2.5GB)`

- In percentuale dello spazio di archiviazione complessivo: `Set-FsxShadowStorage -Maxsize "20%"`
- Senza limiti: `Set-FsxShadowStorage -Maxsize "UNBOUNDED"`

`-Default`Da utilizzare per impostare lo shadow storage in modo che utilizzi fino al 10 percento del file system:. `Set-FsxShadowStorage -Default` Per ulteriori informazioni sull'utilizzo dell'opzione predefinita, consulta[Configurazione delle copie shadow per utilizzare l'archiviazione e la pianificazione predefinite](#).

Per impostare la quantità di storage shadow copy su un file system FSx for Windows File Server

1. Connect a un'istanza di calcolo con connettività di rete con il file system come utente membro del gruppo di amministratori del file system. Nel AWS Managed Microsoft AD, quel gruppo è AWS Delegated FSx Administrators. In Microsoft AD autogestito, tale gruppo è Domain Admins o il gruppo personalizzato specificato per l'amministrazione al momento della creazione del file system. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
2. Apri una PowerShell finestra Windows sull'istanza di calcolo.
3. Usa il seguente comando per aprire una PowerShell sessione remota sul tuo file system Amazon FSx. Sostituiscilo *`FSxFileSystem-Remote-PowerShell-Endpoint`* con l' PowerShell endpoint Windows Remote del file system che desideri amministrare. Puoi trovare l' PowerShell endpoint Windows Remote nella console Amazon FSx, nella sezione Rete e sicurezza della schermata dei dettagli del file system o nella risposta dell'operazione `DescribeFileSystem` dell'API.

   ```
   PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-
   PowerShell-Endpoint -configurationname fsxremoteadmin
   ```

4. Verifica che lo storage shadow copy non sia già configurato sul file system utilizzando il seguente comando.

   ```
   [fs-1234567890abcef12]: PS>Get-FsxShadowStorage
   No Fsx Shadow Storage Configured
   ```

5. Impostate la quantità di storage shadow al 10% del volume e il numero massimo di copie shadow a 20 utilizzando l'`-Default`opzione.

   ```
   [fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
   ```

```
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 32530536858                 20
```

È possibile limitare il numero massimo di copie shadow consentite sul file system utilizzando il `Set-FSxShadowStorage` comando con il `-MaxShadowCopyNumber` parametro e specificando un valore compreso tra 1 e 500. Per impostazione predefinita, il numero massimo di copie shadow è impostato su 20, come consigliato da Microsoft per i carichi di lavoro attivi.

Visualizzazione dello spazio di archiviazione delle copie shadow

È possibile visualizzare la quantità di spazio di archiviazione attualmente utilizzata dalle copie shadow sul file system utilizzando il `Get-FsxShadowStorage` comando in una PowerShell sessione remota sul file system. Per istruzioni sull'avvio di una PowerShell sessione remota sul file system, consultaUtilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell.

```
[fs-1234567890abcef12]: PS>PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 10737418240                 20
```

L'output mostra la configurazione dello shadow storage, come segue:

- `AllocatedSpace`— La quantità di storage sul file system in byte attualmente allocata alle copie shadow. Inizialmente, questo valore è 0.
- `UsedSpace`— La quantità di spazio di archiviazione, in byte, attualmente utilizzata dalle copie shadow. Inizialmente, questo valore è 0.
- `MaxSpace`— La quantità massima di spazio di archiviazione, in byte, che lo shadow storage può raggiungere. Questo è il valore impostato per l'archiviazione delle copie shadow utilizzando il `Set-FsxShadowStorage` comando.
- `MaxShadowCopyNumber`— Il numero massimo di copie shadow che il file system può avere, compreso tra 1 e 500.

Quando la `UsedSpace` quantità raggiunge la quantità massima di archiviazione delle copie shadow configurata (`MaxSpace`) o il numero di copie shadow raggiunge il numero massimo di copie shadow configurato (`MaxShadowCopyNumber`), la copia shadow successiva che si esegue sostituisce la copia shadow più vecchia. Se non volete perdere le copie shadow più vecchie, controllate lo spazio di archiviazione delle copie shadow per assicurarvi di disporre di spazio di archiviazione sufficiente per le nuove copie shadow. Se avete bisogno di più spazio, potete eliminare le copie shadow esistenti o aumentare la quantità massima di spazio di archiviazione per le copie shadow.

> **Note**
>
> Quando le copie shadow vengono create automaticamente o manualmente, utilizzano la quantità di storage per copie shadow configurata come limite di archiviazione. Le dimensioni delle copie shadow aumentano nel tempo e utilizzano lo spazio di archiviazione disponibile indicato dalla CloudWatch `FreeStorageCapacity` metrica fino alla quantità massima di storage per copie shadow configurata ()`MaxSpace`.

Eliminazione dello storage delle copie shadow, della pianificazione e di tutte le copie shadow

È possibile eliminare la configurazione della copia shadow, incluse tutte le copie shadow esistenti, insieme alla pianificazione della copia shadow. Allo stesso tempo, è possibile rilasciare lo storage delle copie shadow sul file system.

Per fare ciò, inserisci il `Remove-FsxShadowStorage` comando in una PowerShell sessione remota sul tuo file system. Per istruzioni sull'avvio di una PowerShell sessione remota sul file system, consultaUtilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowStorage

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowStorage" on target "Removing all Shadow
 Copies, Shadow Copy Schedule, and Shadow Storage".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
FSx Shadow Storage Configuration
Removing Shadow Copy Schedule
Removing Shadow Copies
All shadow copies removed.
```

```
Removing Shadow Storage
Shadow Storage removed successfully.
```

Creazione di una pianificazione personalizzata delle copie shadow

Le pianificazioni delle copie shadow utilizzano i trigger delle attività pianificate in Microsoft Windows per specificare quando le copie shadow vengono eseguite automaticamente. Una pianificazione delle copie shadow può avere più trigger, il che offre molta flessibilità di pianificazione. Può esistere una sola pianificazione delle copie shadow alla volta. Prima di poter creare una pianificazione delle copie shadow, è necessario innanzitutto impostare la quantità di storage per le copie shadow.

Quando si esegue il `Set-FsxShadowCopySchedule` comando su un file system, si sovrascrive qualsiasi pianificazione di copia shadow esistente. Se il computer client è nel fuso orario UTC, puoi anche specificare il fuso orario per un trigger utilizzando i fusi orari di Windows e l'`-TimezoneId`opzione. Per un elenco dei fusi orari di Windows, consulta la documentazione del fuso orario predefinito di Microsoft o esegui quanto segue al prompt dei comandi di Windows:. `tzutil /l` Per ulteriori informazioni sui trigger delle attività di Windows, vedere Task Triggers nella documentazione del Microsoft Windows Developer Center.

È inoltre possibile utilizzare l'`-Default`opzione per impostare rapidamente una pianificazione predefinita per le copie shadow. Per ulteriori informazioni, consulta Configurazione delle copie shadow per utilizzare l'archiviazione e la pianificazione predefinite.

Per creare una pianificazione personalizzata delle copie shadow

1. Crea una serie di attivazioni pianificate di Windows per definire quando eseguire le copie shadow nella pianificazione delle copie shadow. Utilizzate il `new-scheduledTaskTrigger` comando in a PowerShell sul computer locale per impostare più trigger.

   L'esempio seguente crea una pianificazione delle copie shadow personalizzata che esegue copie shadow ogni lunedì-venerdì, alle 6:00 e alle 18:00 UTC. Per impostazione predefinita, gli orari sono espressi in UTC, a meno che non si specifichi un fuso orario nei trigger delle attività pianificate di Windows creati.

   ```
   PS C:\Users\delegateadmin> $trigger1 = new-scheduledTaskTrigger -weekly -DaysOfWeek
    Monday,Tuesday,Wednesday,Thursday,Friday -at 06:00
   PS C:\Users\delegateadmin> $trigger2 = new-scheduledTaskTrigger -weekly -DaysOfWeek
    Monday,Tuesday,Wednesday,Thursday,Friday -at 18:00
   ```

2. Utilizzare `invoke-command` per eseguire il comando. `scriptblock` In questo modo viene scritto uno script che imposta la pianificazione della copia dello shadow con il `new-scheduledTaskTrigger` valore appena creato. Sostituisci *`FSxFileSystem-Remote-PowerShell-Endpoint`* con l' PowerShell endpoint Windows Remote del file system che desideri amministrare. Puoi trovare l' PowerShell endpoint Windows Remote nella console Amazon FSx, nella sezione Rete e sicurezza della schermata dei dettagli del file system o nella risposta dell'operazione `DescribeFileSystem` dell'API.

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

3. Immetti la riga seguente al >> prompt per impostare la pianificazione della copia shadow utilizzando il comando. `set-fsxshadowcopyschedule`

```
>> set-fsxshadowcopyschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2
 -Confirm:$false }
```

La risposta visualizza la pianificazione della copia shadow configurata nel file system.

```
FSx Shadow Copy Schedule


Start Time:    : 2019-07-16T06:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcde1

Start Time:    : 2019-07-16T18:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcdef
```

Visualizzazione della pianificazione delle copie shadow

Per visualizzare la pianificazione della copia shadow esistente sul file system, immettete il seguente comando in una PowerShell sessione remota sul file system. Per istruzioni sull'avvio di una

PowerShell sessione remota sul file system, consultaUtilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell.

```
[fs-0123456789abcdef1]PS> Get-FsxShadowCopySchedule
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

Eliminazione di una pianificazione di copie shadow

Per eliminare la pianificazione della copia shadow esistente sul file system, immettete il seguente comando in una PowerShell sessione remota sul file system. Per istruzioni sull'avvio di una PowerShell sessione remota sul file system, consultaUtilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopySchedule

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowCopySchedule" on target "Removing FSx Shadow
 Copy Schedule".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y"): Y
[fs-0123456789abcdef1]PS>
```

Creazione di una copia shadow

Per creare manualmente una copia shadow, immettete il seguente comando in una PowerShell sessione remota sul file system. Per istruzioni sull'avvio di una PowerShell sessione remota sul file system, consultaUtilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell.

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

Visualizzazione delle copie shadow esistenti

Per visualizzare il set di copie shadow esistenti sul file system, immettete il seguente comando in una PowerShell sessione remota sul file system. Per istruzioni sull'avvio di una PowerShell sessione remota sul file system, consultaUtilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell.

```
[fs-0123456789abcdef1]PS>Get-FsxShadowCopies
FSx Shadow Copies: 2 total

Shadow Copy ID                          Creation Time
--------------                          -----------------
{ABCDEF12-3456-7890-ABCD-EF1234567890} 6/17/2019 7:11:09 AM
{FEDCBA21-6543-0987-0987-EF3214567892} 6/19/2019 11:24:19 AM
```

Eliminazione di copie shadow

È possibile eliminare una o più copie shadow esistenti sul file system utilizzando il `Remove-FsxShadowCopies` comando in una PowerShell sessione remota sul file system. Per istruzioni sull'avvio di una PowerShell sessione remota sul file system, consultaUtilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell.

Specificate quali copie shadow eliminare utilizzando una delle seguenti opzioni obbligatorie:

- `-Oldest`elimina la copia shadow più vecchia
- `-All`elimina tutte le copie shadow esistenti
- `-ShadowCopyId`elimina una copia shadow specifica per ID.

È possibile utilizzare solo un'opzione con il comando. Si verifica un errore se non si specifica quale copia shadow eliminare, se si specificano più ID di copia shadow o se si specifica un ID di copia shadow non valido.

Per eliminare la copia shadow più vecchia sul file system, immettete il seguente comando in una PowerShell sessione remota sul file system.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -Oldest
Confirm
Are you sure you want to perform this action?
```

```
Performing the operation "Remove-FSxShadowCopies" on target "Removing oldest shadow
 copy".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} deleted
```

Per eliminare una copia shadow specifica sul file system, immettete il seguente comando in una PowerShell sessione remota sul file system.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -ShadowCopyId "{ABCDEF12-3456-7890-
ABCD-EF1234567890}"
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing shadow copy
 {ABCDEF12-3456-7890-ABCD-EF1234567890}".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y":>Y
Shadow Copy \\AMZNFSXABCDE123\root\cimv2:Wind32_ShadowCopy.ID{ABCDEF12-3456-7890-ABCD-
EF1234567890}".ID deleted.
```

Per eliminare un certo numero di copie shadow più vecchie dal file system, aggiorna il `-MaxShadowCopyNumber` parametro inserendo il numero desiderato di copie shadow che desideri rimangano. Tuttavia, questa modifica avrà effetto solo dopo lo scatto della successiva istantanea della copia shadow, quando il sistema eliminerà automaticamente le copie shadow in eccesso. Utilizzate il seguente comando in una PowerShell sessione remota sul file system.

```
[fs-1234567890abcef12]: PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace MaxSpace    MaxShadowCopyNumber
-------------- --------- ----------- -------------------
     556679168  21659648 10737418240                  50

[fs-1234567890abcef12]: PS>Set-FsxShadowStorage  -MaxShadowCopyNumber 5
Validation
You have 50 shadow copies. Older versions of shadow copies will be deleted, keeping 5
 latest shadow copies on your file system.
Do you want to continue?
[Y] Yes  [N] No  [?] Help (default is "N"): y
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
     556679168  21659648 10737418240                   5
```

Replica pianificata utilizzando AWS DataSync

È possibile utilizzare AWS DataSync per pianificare la replica periodica del file system FSx for Windows File Server su un secondo file system. Questa funzionalità è disponibile sia per le implementazioni a livello locale che interregionale. Per ulteriori informazioni, consulta Migrazione di file esistenti su FSx for Windows File Server utilizzando AWS DataSync questa guida e Trasferimento dati tra servizi di AWS storage nella Guida per l'utente.AWS DataSync

Amministrazione dei file system

Questo capitolo descrive come accedere alla CLI Amazon FSx per la gestione remota su e come eseguire PowerShell le attività amministrative del file system disponibili. È inoltre possibile utilizzare l'interfaccia grafica utente (GUI) nativa di Microsoft Windows per eseguire alcune attività amministrative.

Argomenti

Utilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell

L'interfaccia a riga di comando di Amazon FSx per la gestione remota PowerShell attiva consente l'amministrazione del file system per gli utenti del gruppo di amministratori del file system. Per avviare una PowerShell sessione remota sul file system FSx for Windows File Server, è necessario innanzitutto soddisfare i seguenti prerequisiti:

- Essere in grado di connettersi a un'istanza di calcolo Windows con connettività di rete con il file system FSx for Windows File Server.

- Accedi all'istanza di calcolo di Windows come membro del gruppo degli amministratori del file system. Se si utilizza AWS Managed Microsoft AD, si tratta del gruppo AWS Delegated FSx Administrators. Se si utilizza un Microsoft Active Directory autogestito, si tratta del gruppo Domain Admins o del gruppo personalizzato specificato per l'amministrazione al momento della creazione del file system. Per ulteriori informazioni, consulta Procedure ottimali per Active Directory autogestita.
- Le regole in entrata del gruppo di sicurezza VPC del tuo file system consentono il traffico sulla porta 5985.

L'interfaccia a riga di comando di Amazon FSx per la gestione remota PowerShell utilizza le seguenti funzionalità di sicurezza:

- Le credenziali utente vengono autenticate utilizzando l'autenticazione Kerberos.
- Le comunicazioni della sessione di gestione tra il client connesso e il file system sono crittografate utilizzando Kerberos.

Sono disponibili due opzioni per eseguire i comandi CLI di gestione remota sul file system Amazon FSx:

- Puoi stabilire una PowerShell sessione remota di lunga durata ed eseguire i comandi all'interno della sessione.
- È possibile utilizzare il `Invoke-Command` per eseguire un singolo comando o un singolo blocco di comandi senza stabilire una sessione PowerShell remota di lunga durata.

Se si desidera impostare e passare variabili come parametri al comando di gestione remota, è necessario utilizzare`Invoke-Command`.

> **Note**
>
> Per i file system Multi-AZ, puoi utilizzare l'interfaccia a riga di comando di Amazon FSx per la gestione remota solo mentre il file system utilizza il suo file server preferito. Per ulteriori informazioni, consulta Disponibilità e durabilità: file system Single-AZ e Multi-AZ.

È necessario utilizzare l' PowerShell endpoint remoto Windows del file system quando si utilizza il telecomando. PowerShell Utilizzando AWS Management Console,

puoi trovare l'endpoint nella scheda Rete e sicurezza, nella pagina dei dettagli del file system. Utilizzando il AWS CLI `describe-file-systems` comando, la `RemoteAdministrationEndpoint` proprietà viene restituita nella risposta. L'endpoint di amministrazione remota utilizza il formato`amznfsxctlyaa1k.`*`ActiveDirectory-DNS-name`*, `amznfsxctlyaa1k.corp.example.com` ad esempio.

È possibile utilizzare il `Get-Command` cmdlet per ottenere informazioni sui cmdlet, le funzioni e gli alias disponibili in. PowerShell Per ulteriori informazioni, vedere la documentazione di Microsoft Get-Command.

Puoi anche eseguire l'interfaccia a riga di comando di Amazon FSx per la gestione remota sui PowerShell comandi del tuo file system utilizzando il `Invoke-Command` cmdlet, utilizzando la seguente sintassi.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName
 amznfsxctlyaa1k.corp.example.com -ConfigurationName FSxRemoteAdmin -scriptblock { fsx-
command}
```

Per istruzioni su come avviare una PowerShell sessione remota di lunga durata sul file system FSx for Windows File Server, vedere Avvio di una sessione remota Amazon FSx PowerShell

Avvio di una sessione remota Amazon FSx PowerShell

Questo argomento fornisce istruzioni per avviare una PowerShell sessione remota di lunga durata sul file server FSx for Windows File Server.

Per avviare una PowerShell sessione remota sul file system

1. Connect a un'istanza di calcolo con connettività di rete con il file system come utente membro del gruppo di amministratori FSx delegato scelto al momento della creazione del file system.
2. Apri una PowerShell finestra Windows sull'istanza di calcolo.
3. Nel PowerShell, inserisci il seguente comando per aprire una sessione remota di lunga durata sul tuo file system Amazon FSx. Sostituiscilo *`Remote-PowerShell-Endpoint`* con l' PowerShell endpoint Windows Remote del file system che desideri amministrare. Utilizza `FsxRemoteAdmin` come nome di configurazione della sessione.

   ```
   PS C:\Users\delegateadmin> enter-pssession -ComputerName Remote-PowerShell-Endpoint
    -ConfigurationName FsxRemoteAdmin
   ```

```
[fs-0123456789abcdef0]: PS>
```

Se la tua istanza non fa parte del dominio Amazon FSx Active Directory, ti viene richiesto di inserire le credenziali utente in un pop-up. Immettere le credenziali dell'utente membro del gruppo FSx Administrators. Se l'istanza è aggiunta al dominio, non ti verranno richieste le credenziali.

Gestione degli alias DNS

FSx for Windows File Server fornisce un nome DNS (Domain Name System) predefinito per ogni file system che è possibile utilizzare per accedere ai dati sul file system. È inoltre possibile accedere ai file system utilizzando un alias DNS di propria scelta. Con gli alias DNS, puoi continuare a utilizzare i nomi DNS esistenti per accedere ai dati archiviati su Amazon FSx durante la migrazione dello storage del file system da locale ad Amazon FSx, senza dover aggiornare strumenti o applicazioni. Per ulteriori informazioni, consulta Migrazione dello storage di file esistente su Amazon FSx.

> **Note**
>
> Il supporto per gli alias DNS è disponibile sui file system FSx for Windows File Server creati dopo le 12:00 ET del 9 novembre 2020. Per utilizzare gli alias DNS su un file system creato prima delle 12:00 ET del 9 novembre 2020, procedi come segue:
>
> 1. Effettua un backup del file system esistente. Per ulteriori informazioni, consulta Utilizzo dei backup avviati dall'utente.
> 2. Ripristina il backup su un nuovo file system. Per ulteriori informazioni, consulta Ripristino dei backup.
>
> Una volta che il nuovo file system sarà disponibile, sarà possibile utilizzare gli alias DNS per accedervi, utilizzando le informazioni fornite in questa sezione.

> **Note**
>
> Le informazioni qui presentate presuppongono che stiate lavorando interamente in Active Directory e che non stiate utilizzando provider DNS esterni. I provider DNS di terze parti possono causare comportamenti imprevisti.

Amazon FSx registra i record DNS per un file system solo se il dominio AD a cui ti stai unendo utilizza Microsoft DNS come DNS predefinito. Se utilizzi un DNS di terze parti, dovrai configurare manualmente le voci DNS per i tuoi file system Amazon FSx dopo aver creato il file system. Per ulteriori informazioni sulla scelta degli indirizzi IP corretti da utilizzare per il file system, consulta. Ottenere gli indirizzi IP corretti del file system da utilizzare per il DNS

È possibile associare gli alias DNS ai file system FSx for Windows File Server esistenti, quando si creano nuovi file system e quando si crea un nuovo file system da un backup. È possibile associare fino a 50 alias DNS a un file system contemporaneamente.

Oltre ad associare alias DNS al file system, per consentire ai client di connettersi al file system utilizzando gli alias DNS, è necessario eseguire anche le seguenti operazioni:

- Configura i nomi principali di servizio (SPN) per l'autenticazione e la crittografia Kerberos.
- Configura un record DNS CNAME per l'alias DNS che si risolve nel nome DNS predefinito per il tuo file system Amazon FSx.

Per ulteriori informazioni, consulta Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.

Un nome alias DNS per il file system FSx for Windows File Server deve soddisfare i seguenti requisiti:

- Deve essere formattato come nome di dominio completo (FQDN).
- Può contenere caratteri alfanumerici e trattini (-).
- Non può iniziare o terminare con un trattino (-).
- Può iniziare con un numerico.

Per i nomi alias DNS, Amazon FSx archivia i caratteri alfabetici come lettere minuscole (a-z), indipendentemente dal modo in cui li specifichi: come lettere maiuscole, minuscole o lettere corrispondenti in codici di escape.

Se si tenta di associare un alias già associato al file system, l'operazione non ha alcun effetto. Se tenti di dissociare un alias da un file system non associato al file system, Amazon FSx risponde con un errore di richiesta errata.

> **Note**
>
> Quando Amazon FSx aggiunge o rimuove alias su un file system, i client connessi vengono temporaneamente disconnessi e si riconnetteranno automaticamente al file system. Tutti i file aperti dai client che mappavano una condivisione non disponibile in modo continuo (non CA) al momento della disconnessione devono essere riaperti dal client.

Argomenti

Stato dell'alias DNS

Gli alias DNS possono avere uno dei seguenti valori di stato:

- Disponibile: l'alias DNS è associato a un file system Amazon FSx.
- Creazione: Amazon FSx crea l'alias DNS e lo associa al file system.
- Eliminazione: Amazon FSx dissocia l'alias DNS dal file system e lo elimina.
- Creazione non riuscita: Amazon FSx non è stato in grado di associare l'alias DNS al file system.
- Eliminazione non riuscita: Amazon FSx non è riuscito a dissociare l'alias DNS dal file system.

Utilizzo di alias DNS con autenticazione Kerberos

Ti consigliamo di utilizzare l'autenticazione e la crittografia basate su Kerberos in transito con Amazon FSx. Kerberos fornisce l'autenticazione più sicura per i client che accedono al file system. Per abilitare l'autenticazione Kerberos per i client che accedono al file system Amazon FSx utilizzando un alias DNS, è necessario configurare i nomi principali di servizio (SPN) che corrispondono all'alias DNS sull'oggetto computer Active Directory del file system.

Se hai degli SPN configurati per l'alias DNS che hai assegnato a un altro file system su un oggetto computer in Active Directory, devi prima rimuovere tali SPN prima di aggiungere SPN all'oggetto

computer del tuo file system. Per ulteriori informazioni, consulta Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.

Visualizzazione degli alias DNS per i file system e i backup

Puoi visualizzare gli alias DNS attualmente associati ai file system e ai backup utilizzando la console Amazon FSx, la AWS CLI e l'API. Questo argomento fornisce istruzioni su come visualizzare gli alias DNS per i file system e i backup.

Per visualizzare gli alias DNS associati ai file system

- Utilizzo della console: scegli un file system per visualizzare la pagina dei dettagli dei file system. Scegli la scheda Rete e sicurezza per visualizzare gli alias DNS.
- Utilizzo della CLI o dell'API: utilizza il comando `describe-file-system-aliases` CLI o l'operazione API. DescribeFileSystemAliases

Per visualizzare gli alias DNS associati ai backup

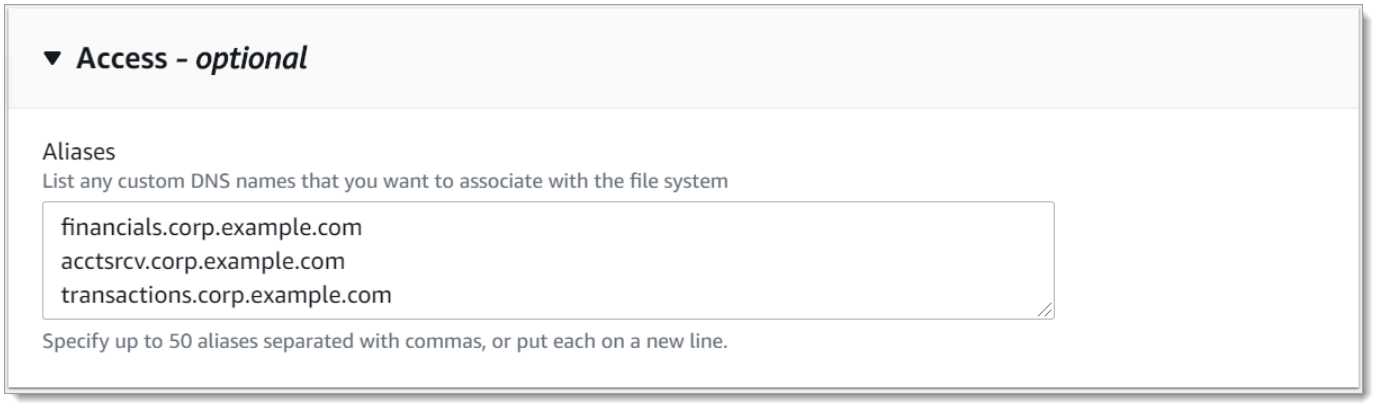
- Utilizzo della console: nel riquadro di navigazione, scegli Backup, quindi scegli il backup che desideri visualizzare. Nel riquadro Riepilogo, visualizza il campo Alias DNS.
- Utilizzo della CLI o dell'API: utilizza il comando `describe-backups` CLI o l'operazione API. DescribeBackups

Associazione degli alias DNS ai file system

Questo argomento descrive come associare gli alias DNS quando si crea un nuovo file system FSx for Windows File Server da zero o quando si crea un file system da un backup, utilizzando AWS Management Console l' AWS CLI API, e.

Per associare gli alias DNS durante la creazione di un nuovo file system (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo file system descritta Crea il tuo file system nella sezione Guida introduttiva.
3. Nella sezione Accesso - opzionale della procedura guidata per la creazione del file system, inserisci gli alias DNS che desideri associare al tuo file system.



4. Quando il file system è disponibile, è possibile accedervi utilizzando l'alias DNS configurando i nomi principali di servizio (SPN) e aggiornando o creando un record DNS CNAME per l'alias. Per ulteriori informazioni, consulta Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.

Per associare alias DNS durante la creazione di un nuovo file system Amazon FSx (CLI)

1. Quando crei un nuovo file system, usa la proprietà Alias con l'operazione CreateFileSystemAPI per associare gli alias DNS al nuovo file system.

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 2000 \
  --storage-type SSD \
  --subnet-ids subnet-123456 \
  --windows-configuration Aliases=[financials.corp.example.com,accts-
rcv.corp.example.com]
```

2. Quando il file system è disponibile, è possibile accedervi utilizzando l'alias DNS configurando i nomi principali di servizio (SPN) e aggiornando o creando un record DNS CNAME per l'alias. Per ulteriori informazioni, consulta Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.

Per aggiungere o rimuovere alias DNS durante il ripristino di un backup (CLI)

1. Quando si crea un nuovo file system da un backup di un file system esistente, è possibile utilizzare la proprietà Aliases con l'CreateFileSystemFromBackupoperazione API come segue:

- Tutti gli alias associati al backup sono associati al nuovo file system per impostazione predefinita.
- Per creare un file system senza conservare alcun alias dal backup, utilizzate la `Aliases` proprietà con un set vuoto.

  Per associare alias DNS aggiuntivi, utilizzate la `Aliases` proprietà e includete sia gli alias originali associati al backup sia i nuovi alias che desiderate associare.

Il seguente comando CLI associa due alias al file system che Amazon FSx sta creando da un backup.

```
aws fsx create-file-system-from-backup \
  --backup-id backup-0123456789abcdef0
  --storage-capacity 2000 \
  --storage-type HDD \
  --subnet-ids subnet-123456 \
  --windows-configuration Aliases=[transactions.corp.example.com,accts-
rcv.corp.example.com]
```

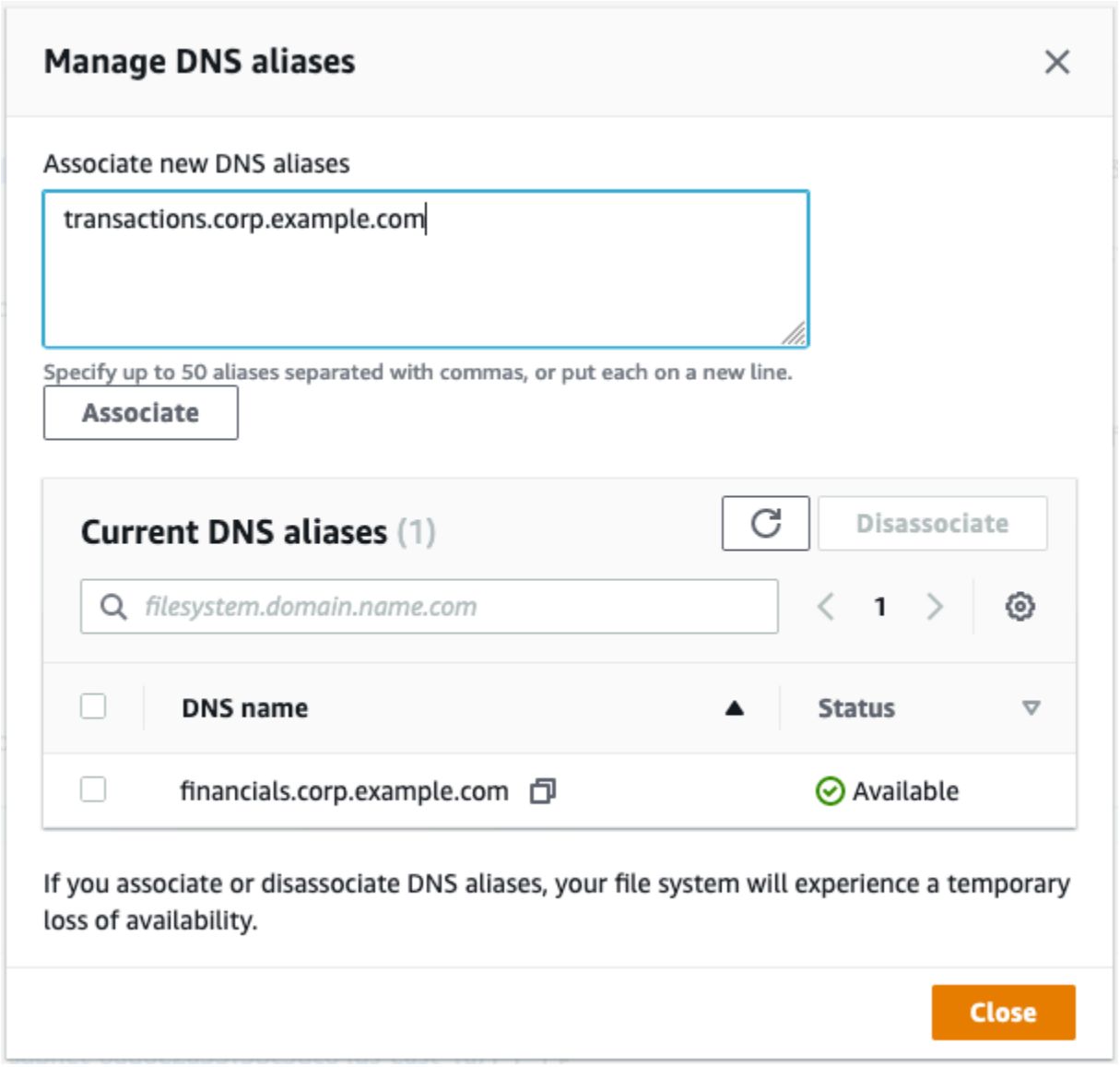
2. Quando il file system è disponibile, è possibile accedervi utilizzando l'alias DNS configurando i nomi principali di servizio (SPN) e aggiornando o creando un record DNS CNAME per l'alias. Per ulteriori informazioni, consulta Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.

Gestione degli alias DNS sui file system esistenti

Questo argomento descrive come utilizzare AWS Management Console e AWS CLI per aggiungere e rimuovere alias sui file system esistenti.

Per gestire gli alias DNS del file system (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il file system Windows per cui desideri gestire gli alias DNS.
3. Nella scheda Rete e sicurezza, scegliete Gestisci alias DNS per visualizzare la finestra di dialogo Gestisci alias DNS.



- Per associare alias DNS: nella casella Associa nuovi alias, inserisci gli alias DNS che desideri associare. Selezionare Associate (Associa).
- Per dissociare gli alias DNS: nell'elenco degli alias correnti, scegli gli alias da cui dissociarti. Scegli Dissocia.

Puoi monitorare lo stato degli alias che hai gestito nell'elenco degli alias correnti. Aggiorna l'elenco per aggiornare lo stato. Sono necessari fino a 2,5 minuti per associare o dissociare un alias da un file system.

4. Quando l'alias è disponibile, è possibile accedere al file system utilizzando l'alias DNS configurando i nomi principali di servizio (SPN) e aggiornando o creando un record DNS CNAME

per l'alias. Per ulteriori informazioni, consulta Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.

Per associare gli alias DNS ai file system esistenti (CLI)

1. Utilizzate il comando `associate-file-system-aliases` CLI o l'operazione AssociateFileSystemAliasesAPI per associare gli alias DNS a un file system esistente.

   La seguente richiesta CLI associa due alias al file system specificato.

   ```
   aws fsx associate-file-system-aliases \
     --file-system-id fs-0123456789abcdef0 \
     --aliases financials.corp.example.com transfers.corp.example.com
   ```

   La risposta mostra lo stato degli alias che Amazon FSx associa al file system.

   ```
   {
       "Aliases": [
           {
               "Name": "financials.corp.example.com",
               "Lifecycle": CREATING
           },
           {
               "Name": "transfers.corp.example.com",
               "Lifecycle": CREATING
           }
       ]
   }
   ```

2. Utilizza il comando `describe-file-system-aliases` CLI (DescribeFileSystemAliasesè l'operazione API equivalente) per monitorare lo stato degli alias che stai associando.

3. Se `Lifecycle` ha il valore AVAILABLE (un processo che richiede fino a 2,5 minuti), è possibile accedere al file system utilizzando l'alias DNS configurando i nomi principali di servizio (SPN) e aggiornando o creando un record DNS CNAME per l'alias. Per ulteriori informazioni, consulta Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.

Per dissociare gli alias DNS dai file system (CLI)

- Utilizzate il comando `disassociate-file-system-aliases` CLI o l'operazione DisassociateFileSystemAliasesAPI per dissociare gli alias DNS da un file system esistente.

  Il comando seguente dissocia un alias da un file system.

  ```
  aws fsx disassociate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com
  ```

  La risposta mostra lo stato degli alias che Amazon FSx sta dissociando dal file system.

  ```
  {
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": DELETING
          }
      ]
  }
  ```

  Utilizza il comando `describe-file-system-aliases` CLI (DescribeFileSystemAliasesè l'operazione API equivalente) per monitorare lo stato degli alias. L'eliminazione dell'alias richiede fino a 2,5 minuti.

Gestione delle condivisioni di file su file system FSx for Windows File Server

Questo argomento descrive come gestire le condivisioni di file eseguendo le seguenti attività.

- Creare una nuova condivisione di file
- Modifica una condivisione di file esistente
- Rimuovere una condivisione di file esistente

È possibile utilizzare la GUI delle cartelle condivise native di Windows e l'interfaccia a riga di comando di Amazon FSx per la gestione remota per gestire le condivisioni di file PowerShell sul

file system FSx for Windows File Server. Potrebbero verificarsi ritardi quando si utilizza la GUI delle cartelle condivise (fsmgmt.msc) alla prima apertura del menu contestuale per le condivisioni che si trovano su un file system diverso. Per evitare questi ritardi, utilizza questa opzione per gestire le condivisioni di file PowerShell che si trovano su più file system.

Tieni presente che esistono regole e limitazioni richieste per tutti i file system supportati da Windows sui nomi di file e directory.». Per garantire la corretta creazione e l'accesso ai dati, è necessario assegnare un nome ai file e alle directory in base a queste linee guida di Windows. Per ulteriori informazioni, vedere Convenzioni di denominazione.

> **Warning**
>
> Amazon FSx richiede che l'utente SYSTEM disponga delle autorizzazioni ACL NTFS Full control su ogni cartella su cui si crea una condivisione di file SMB. Non modificare le autorizzazioni NTFS ACL per questo utente sulle tue cartelle, in quanto ciò potrebbe rendere inaccessibili le tue condivisioni di file.

Gestione delle condivisioni di file con l'interfaccia grafica delle cartelle condivise

Per gestire le condivisioni di file sul tuo file system Amazon FSx, puoi utilizzare l'interfaccia grafica delle cartelle condivise. L'interfaccia grafica delle cartelle condivise fornisce una posizione centrale per la gestione di tutte le cartelle condivise su un server Windows. Le procedure seguenti descrivono come gestire le condivisioni di file.

Per connettere le cartelle condivise al file system FSx for Windows File Server

1. Avvia l'istanza Amazon EC2 e collegala a Microsoft Active Directory a cui è collegato il file system Amazon FSx. A tale scopo, scegli una delle seguenti procedure dalla Guida all'AWS Directory Service amministrazione:

   - Unisciti senza problemi a un'istanza Windows EC2
   - Unisciti manualmente a un'istanza Windows

2. Connect alla propria istanza come utente membro del gruppo di amministratori del file system. In AWS Managed Microsoft Active Directory, questo gruppo è denominato AWS Delegated FSx Administrators. In Microsoft Active Directory autogestito, questo gruppo è denominato Domain Admins o il nome personalizzato per il gruppo di amministratori fornito durante la creazione. Per

ulteriori informazioni, consulta Connect to your Windows nella Amazon Elastic Compute Cloud User Guide for Windows Instances.

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 (Domain Name System) per il tuo file system Amazon FSx, ad esempio. **`amznfsxabcd0123.corp.example.com`**

   Per trovare il nome DNS del tuo file system sulla console Amazon FSx, scegli File system, scegli il tuo file system, quindi controlla la sezione Rete e sicurezza della pagina dei dettagli del file system. Puoi anche ottenere il nome DNS nella risposta dell'operazione DescribeFileSystems API.
6. Scegli OK. Viene quindi visualizzata una voce relativa al file system Amazon FSx nell'elenco dello strumento Cartelle condivise.

Ora che Shared Folders è connesso al tuo file system Amazon FSx, puoi gestire le condivisioni di file Windows sul file system. Viene chiamata `\share` la condivisione predefinita. È possibile farlo con le seguenti azioni:

- Crea una nuova condivisione di file: nello strumento Cartelle condivise, scegli Condivisioni nel riquadro a sinistra per visualizzare le condivisioni attive per il tuo file system Amazon FSx. 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: fai clic su «Sfoglia» quando specifichi il percorso della cartella locale e fai clic su «Crea nuova cartella» per creare la cartella locale.
  - Utilizzando la riga di comando:

    ```
    New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share
    \MyNewShare
    ```

- Modifica una condivisione di file: nello strumento Cartelle condivise, apri il menu contestuale (fai clic con il pulsante destro del mouse) per la condivisione di file che desideri modificare nel riquadro destro e scegli Proprietà. Modifica le proprietà e scegli 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 destro, quindi scegli Interrompi condivisione.

> **Note**
>
> Per i file system Single-AZ 2 e Multi-AZ, rimuovere le condivisioni di file o modificare le condivisioni di file (incluso l'aggiornamento delle autorizzazioni, dei limiti utente e altre proprietà) utilizzando lo strumento GUI delle cartelle condivise è possibile solo se ci si connette a fsmgmt.msc utilizzando il nome DNS del file system Amazon FSx. Lo strumento GUI delle cartelle condivise non supporta queste azioni se ti connetti utilizzando l'indirizzo IP o il nome alias DNS del file system.

> **Note**
>
> Se si utilizza lo strumento GUI delle cartelle condivise fsmgmt.msc per accedere alle condivisioni situate su più file system FSx, potrebbero verificarsi ritardi quando si apre per la prima volta il menu contestuale di condivisione file per una condivisione situata su un file system diverso. Per evitare questi ritardi, è possibile gestire le condivisioni di file utilizzando la procedura descritta di seguito. PowerShell

Gestione delle condivisioni di file con PowerShell

È possibile gestire le condivisioni di file utilizzando comandi di gestione remota personalizzati per. PowerShell Questi comandi possono aiutarti ad automatizzare più facilmente queste attività:

- Migrazione di condivisioni di file su file server esistenti su Amazon FSx
- Sincronizzazione delle condivisioni di file tra AWS regioni per il disaster recovery
- Gestione programmatica delle condivisioni di file per flussi di lavoro continui, come il provisioning della condivisione di file tra team

Per informazioni su come utilizzare l'interfaccia a riga di comando di Amazon FSx per la gestione remota, consulta. PowerShell Utilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell

La tabella seguente elenca i PowerShell comandi di gestione remota dell'interfaccia a riga di comando di Amazon FSx che puoi utilizzare per gestire le condivisioni di file sui file system FSx for Windows File Server.

Condividi comando di gestione	Descrizione
New-FSxSmbShare	Crea una nuova condivisione di file.
Remove-FSxSmbShare	Rimuove una condivisione di file.
Get-FSxSmbShare	Recupera le condivisioni di file esistenti.
Set-FSxSmbShare	Imposta le proprietà per una condivisione.
Get-FSxSmbShareAccess	Recupera l'elenco di controllo degli accessi (ACL) di una condivisione.
Grant-FSxSmbShareAccess	Aggiunge una voce ACE (allow access control entry) per un trustee al descrittore di sicurezza di una condivisione.
Revoke-FSxSmbShareAccess	Rimuove tutti gli ACE di autorizzazione per un trustee dal descrittore di sicurezza di una condivisione.
Block-FSxSmbShareAccess	Aggiunge un ACE di rifiuto per un fiduciario al descrittore di sicurezza di una condivisione.
Unblock-FSxSmbShareAccess	Rimuove tutti gli ACE di rifiuto per un trustee dal descrittore di sicurezza di una condivisione.

La guida in linea di ogni comando fornisce un riferimento a tutte le opzioni di comando. Per accedere a questa guida, esegui il comando con`-?`, ad esempio`New-FSxSmbShare -?`.

Passare le credenziali a New-F SxSmb Share

È possibile passare le credenziali a New-F in SxSmbShare modo da poterlo eseguire in un ciclo continuo per creare centinaia o migliaia di condivisioni senza dover reinserire le credenziali ogni volta.

Preparate l'oggetto credenziale necessario per creare le condivisioni di file sul file server FSx for Windows File Server utilizzando una delle seguenti opzioni.

- Per generare l'oggetto credenziale in modo interattivo, utilizzate il comando seguente.

```
$credential = Get-Credential
```

- Per generare l'oggetto credenziale utilizzando una AWS Secrets Manager risorsa, utilizzate il comando seguente.

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

Creazione di una condivisione a disponibilità continua (CA)

Puoi creare condivisioni a disponibilità continua (CA) utilizzando l'interfaccia a riga di comando di Amazon FSx per la gestione remota su. PowerShell Le condivisioni CA create su un file system FSx for Windows File Server Multi-AZ sono estremamente resistenti e altamente disponibili. Un file system Amazon FSx Single-AZ è costruito su un cluster a nodo singolo. Di conseguenza, le condivisioni CA create su un file system Single-AZ sono altamente durevoli, ma non sono altamente disponibili. Utilizzate il `New-FSxSmbShare` comando con l'`-ContinuouslyAvailable`opzione impostata su `$True` per specificare che la condivisione è una condivisione a disponibilità continua. Di seguito è riportato un comando di esempio per creare una condivisione CA.

```
New-FSxSmbShare -Name "New CA Share" -Path "D:\share\new-share" -Description "CA share"
 -ContinuouslyAvailable $True
```

È possibile modificare l'`-ContinuouslyAvailable`opzione su una condivisione di file esistente utilizzando il `Set-FSxSmbShare` comando.

Determina se una condivisione di file esistente è sempre disponibile

Utilizzare il comando seguente per visualizzare il valore della proprietà Continuously Available per una condivisione di file esistente.

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { get-fsxsmbshare -name share_name }
```

Se CA è abilitato, l'output includerà la riga seguente:

```
[...]
ContinuouslyAvailable : True
[...]
```

Se CA non è abilitato, l'output includerà la seguente riga:

```
[...]
ContinuouslyAvailable : False
[...]
```

Per abilitare Continually Available su una condivisione di file esistente, utilizzate il seguente comando:

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { set-fsxsmbshare -name share_name -ContinuouslyAvailable $True}
```

Controllo dell'accesso ai file

Amazon FSx for Windows File Server supporta il controllo dell'accesso degli utenti finali a file, cartelle e condivisioni di file. Puoi scegliere di inviare i registri degli eventi di controllo di un file system ad altri AWS servizi che offrono un ricco set di funzionalità. Queste includono l'abilitazione delle interrogazioni, l'elaborazione, l'archiviazione e l'archiviazione dei log, l'emissione di notifiche e l'attivazione di azioni per migliorare ulteriormente gli obiettivi di sicurezza e conformità.

Per ulteriori informazioni sull'utilizzo del controllo degli accessi ai file per ottenere informazioni dettagliate sui modelli di accesso e implementare notifiche di sicurezza per l'attività degli utenti finali, vedere Informazioni sui modelli di accesso allo storage dei file e Implementazione delle notifiche di sicurezza per l'attività degli utenti finali.

Il controllo dell'accesso ai file consente di registrare gli accessi degli utenti finali a singoli file, cartelle e condivisioni di file in base ai controlli di controllo definiti dall'utente. I controlli di controllo sono noti anche come elenchi di controllo degli accessi al sistema NTFS (SACL). Se hai già impostato i controlli di audit sui tuoi dati di file esistenti, puoi sfruttare il controllo degli accessi ai file creando un nuovo file system Amazon FSx for Windows File Server e migrando i tuoi dati.

Amazon FSx supporta i seguenti eventi di controllo di Windows per gli accessi a file, cartelle e condivisioni di file:

- Per l'accesso ai file, supporta: Tutti, Traverse folder/Execute file, List folder/Leggi dati, Leggi attributi, Crea file/Scrivi dati, Crea cartelle/Aggiungi dati, Write attributes, Elimina sottocartelle e file, Elimina, Leggi le autorizzazioni, Modifica le autorizzazioni e Assumi la proprietà.
- Per gli accessi alla condivisione di file, supporta: Connect a una condivisione di file.

Per tutti gli accessi a file, cartelle e condivisioni di file, Amazon FSx supporta la registrazione dei tentativi riusciti (ad esempio un utente con autorizzazioni sufficienti che accede con successo a un file o a una condivisione di file), dei tentativi falliti o di entrambi.

È possibile configurare se si desidera il controllo degli accessi solo su file e cartelle, solo sulle condivisioni di file o su entrambi. È inoltre possibile configurare i tipi di accesso da registrare (solo tentativi riusciti, solo tentativi falliti o entrambi). È inoltre possibile disattivare il controllo degli accessi ai file in qualsiasi momento.

> **Note**
>
> Il controllo dell'accesso ai file registra i dati di accesso degli utenti finali solo dal momento in cui è abilitato. In altre parole, il controllo dell'accesso ai file non genera registri degli eventi di controllo delle attività di accesso a file, cartelle e condivisioni di file effettuate dall'utente finale prima dell'attivazione del controllo dell'accesso ai file.

La frequenza massima di eventi di controllo degli accessi supportati è di 5.000 eventi al secondo. Gli eventi di controllo degli accessi non vengono generati per ogni operazione di lettura e scrittura dei file, ma una volta per operazione sui metadati dei file, ad esempio quando un utente crea, apre o elimina un file.

Argomenti

Controlla le destinazioni del registro degli eventi

Quando abiliti il controllo degli accessi ai file, devi configurare un AWS servizio a cui Amazon FSx invia i log degli eventi di controllo. Puoi inviare i log degli eventi di controllo a un flusso di log di Amazon CloudWatch Logs in un gruppo di log CloudWatch Logs o a un flusso di distribuzione Amazon Data Firehose. Puoi scegliere la destinazione dei log degli eventi di controllo quando crei il file system Amazon FSx for Windows File Server o in qualsiasi momento successivo aggiornando un file system esistente. Per ulteriori informazioni, consulta Gestione del controllo degli accessi ai file.

Di seguito sono riportati alcuni consigli che possono aiutarti a decidere quale destinazione dei log degli eventi di controllo scegliere:

- Scegli CloudWatch Logs se desideri archiviare, visualizzare e cercare i log degli eventi di controllo nella CloudWatch console Amazon, eseguire query sui log utilizzando CloudWatch Logs Insights e attivare CloudWatch allarmi o funzioni Lambda.
- Scegli Firehose se desideri trasmettere continuamente gli eventi allo storage in Amazon S3, a un database in Amazon Redshift, ad OpenSearch Amazon Service o alle soluzioni dei partner (come Splunk o Datadog) AWS per ulteriori analisi.

Per impostazione predefinita, Amazon FSx creerà e utilizzerà un gruppo di log CloudWatch Logs predefinito nel tuo account come destinazione del registro degli eventi di controllo. Se si desidera utilizzare un gruppo di log CloudWatch Logs personalizzato o utilizzare Firehose come destinazione del registro degli eventi di controllo, ecco i requisiti per i nomi e le posizioni della destinazione del registro degli eventi di controllo:

- Il nome del gruppo di CloudWatch log Logs deve iniziare con il prefisso. `/aws/fsx/` Se non disponi di un gruppo di log CloudWatch Logs esistente quando crei o aggiorni un file system sulla console, Amazon FSx può creare e utilizzare un flusso di log predefinito nel CloudWatch gruppo di log `/aws/fsx/windows` Logs. Se non desideri utilizzare il gruppo di log predefinito, l'interfaccia utente di configurazione ti consente di creare un gruppo di log CloudWatch Logs quando crei o aggiorni il file system sulla console.
- Il nome del flusso di distribuzione di Firehose deve iniziare con il `aws-fsx-` prefisso. Se non disponi di un flusso di distribuzione Firehose esistente, puoi crearne uno quando crei o aggiorni il file system sulla console.
- Il flusso di distribuzione Firehose deve essere configurato per essere utilizzato `Direct PUT` come sorgente. Non è possibile utilizzare un flusso di dati Kinesis esistente come origine dati per il flusso di distribuzione.

- La destinazione (CloudWatch Logs log group o Firehose delivery stream) deve trovarsi nella AWS stessa partizione Regione AWS e nel file system Amazon FSx. Account AWS

È possibile modificare la destinazione del registro degli eventi di controllo in qualsiasi momento (ad esempio, da CloudWatch Logs a Firehose). Quando si esegue questa operazione, i nuovi registri degli eventi di controllo vengono inviati solo alla nuova destinazione.

Il massimo impegno è controllare la consegna del registro degli eventi.

In genere, i record del registro degli eventi di controllo vengono consegnati a destinazione in pochi minuti, ma a volte possono richiedere più tempo. In occasioni molto rare, i record del registro degli eventi di controllo potrebbero non essere registrati. Se il tuo caso d'uso richiede una semantica particolare (ad esempio, garantendo che nessun evento di controllo venga perso), ti consigliamo di tenere conto degli eventi persi durante la progettazione dei flussi di lavoro. È possibile verificare la presenza di eventi persi eseguendo la scansione della struttura dei file e delle cartelle sul file system.

Migrazione dei controlli di audit

Se disponi di controlli di audit (SACL) già configurati sui dati di file esistenti, puoi creare un file system Amazon FSx e migrare i dati nel nuovo file system. Ti consigliamo di AWS DataSync utilizzarlo per trasferire i dati e i SACL associati al tuo file system Amazon FSx. Come soluzione alternativa, puoi usare Robocopy (Robust File Copy). Per ulteriori informazioni, consulta Migrazione dello storage di file esistente su Amazon FSx.

Visualizzazione dei registri degli eventi

Puoi visualizzare i log degli eventi di controllo dopo che Amazon FSx ha iniziato a emetterli. Dove e come vengono visualizzati i log dipende dalla destinazione del registro degli eventi di controllo:

- È possibile visualizzare CloudWatch i log dei log accedendo alla CloudWatch console e scegliendo il gruppo di log e il flusso di log a cui vengono inviati i log degli eventi di controllo. Per ulteriori informazioni, consulta Visualizza i dati di log inviati a CloudWatch Logs nella Amazon CloudWatch Logs User Guide.

  Puoi utilizzare CloudWatch Logs Insights per cercare e analizzare in modo interattivo i tuoi dati di log. Per ulteriori informazioni, consulta Analyzing Log Data with CloudWatch Logs Insights, nella Amazon CloudWatch Logs User Guide.

Puoi anche esportare i log degli eventi di controllo in Amazon S3. Per ulteriori informazioni, consulta Esportazione dei dati di registro su Amazon S3, sempre nella CloudWatch Amazon Logs User Guide.

- Non è possibile visualizzare i registri degli eventi di controllo su Firehose. Tuttavia, è possibile configurare Firehose per inoltrare i log a una destinazione da cui è possibile leggere. Le destinazioni includono Amazon S3, Amazon Redshift, OpenSearch Amazon Service e soluzioni partner come Splunk e Datadog. Per ulteriori informazioni, consulta Choose destination nella Amazon Data Firehose Developer Guide.

Controlla i campi degli eventi

Questa sezione fornisce descrizioni delle informazioni contenute nei registri degli eventi di controllo ed esempi di eventi di controllo.

Di seguito sono riportate le descrizioni dei campi salienti di un evento di controllo di Windows.

- EventID si riferisce all'ID degli eventi del registro eventi di Windows definito da Microsoft. Consulta la documentazione Microsoft per informazioni sugli eventi del file system e sugli eventi di condivisione dei file.
- SubjectUserNamesi riferisce all'utente che effettua l'accesso.
- ObjectNamesi riferisce al file, alla cartella o alla condivisione di file di destinazione a cui è stato effettuato l'accesso.
- ShareNameè disponibile per gli eventi generati per l'accesso alla condivisione di file. Ad esempio, `EventID 5140` viene generato quando si accede a un oggetto di condivisione di rete.
- IpAddresssi riferisce al client che ha avviato l'evento per gli eventi di condivisione di file.
- Le parole chiave, se disponibili, indicano se l'accesso ai file ha avuto esito positivo o negativo. Per gli accessi riusciti, il valore è`0x8020000000000000`. Per gli accessi non riusciti, il valore è. `0x8010000000000000`
- TimeCreated SystemTimesi riferisce all'ora in cui l'evento è stato generato nel sistema e visualizzato in <YYYY-MM-DDThh:mm:ss.s>formato Z.
- Computer si riferisce al nome DNS del file system Windows Remote PowerShell Endpoint e può essere utilizzato per identificare il file system.
- AccessMask, se disponibile, si riferisce al tipo di accesso ai file eseguito (ad esempio ReadData, WriteData).

- AccessListsi riferisce all'accesso richiesto o concesso a un oggetto. Per i dettagli, consulta la tabella seguente e la documentazione Microsoft (ad esempio nell'evento 4556).

Tipo di accesso	Maschera di accesso	Valore
Leggi i dati o la directory degli elenchi	0x1	%%4416
Scrivi dati o aggiungi file	0x2	%%4417
Aggiungi dati o aggiungi sottodirectory	0x4	%%4418
Leggi gli attributi estesi	0x8	%%4419
Scrivi attributi estesi	0x10	%%4420
Eseguire/Traversa	0x20	%%4421
Elimina bambino	0x40	%4422
Leggi gli attributi	0x80	%%4423
Attributi di scrittura	0x100	%%4424
Eliminazione	0x10000	%%1537
Leggi ACL	0x20000	%%1538
Scrivi ACL	0x40000	%%1539
Scrivi proprietario	0x80000	%%1540
Sincronizza	0x100000	%%1541
Access Security ACL	0x1000000	%%1542

Di seguito sono riportati alcuni eventi chiave con esempi. Si noti che il codice XML è formattato per garantire la leggibilità.

L'ID evento 4660 viene registrato quando un oggetto viene eliminato.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4660</EventID><Version>0</Version><Level>0</Level>
<Task>12800</Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-05-18T04:51:56.916563800Z'/>
<EventRecordID>315452</EventRecordID><Correlation/>
<Execution ProcessID='4' ThreadID='5636'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x50932f71</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='HandleId'>0x12e0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data></EventData></
Event>
```

L'ID evento 4659 viene registrato su una richiesta di eliminazione di un file.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4659</EventID><Version>0</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-0603T19:18:09.951551200Z'/>
<EventRecordID>308888</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5540'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\shar
\event.txt</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1537
    %%4423
```

```
    </Data><Data Name='AccessMask'>0x10080</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='ProcessId'>0x4</Data></EventData></Event>
```

L'ID evento 4663 viene registrato quando è stata eseguita un'operazione specifica sull'oggetto. L'esempio seguente mostra la lettura di dati da un file, da cui è possibile interpretare. `AccessList %%4416`

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663< /EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:10:13.887145400Z'/>
<EventRecordID>308831</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='6916'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData>< Data
 Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113< /Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0x101c</Data><Data Name='AccessList'>%%4416
    </Data>
<Data Name='AccessMask'>0x1</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data>
</EventData></Event>
```

L'esempio seguente mostra la scrittura/aggiunta di dati da un file, da cui è possibile interpretare. `AccessList %%4417`

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:12:16.813827100Z'/>
<EventRecordID>308838</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5828'/>
```

```
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0xa38</Data><Data Name='AccessList'>%%4417
    </Data><Data Name='AccessMask'>0x2</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data></
EventData></Event>
```

L'ID evento 4656 indica che è stato richiesto un accesso specifico per un oggetto. Nell'esempio seguente, la richiesta di lettura è stata avviata su ObjectName «permtest» ed è stata un tentativo fallito, come indicato nel valore Keywords di. `0x8010000000000000`

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4656</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:22:55.113783500Z'/>
<EventRecordID>308919</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='4924'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1541
    %%4416
    %%4423
    </Data><Data Name='AccessReason'>%%1541: %%1805
    %%4416: %%1805
    %%4423: %%1811 D:(A;OICI;0x1301bf;;;AU)
    </Data><Data Name='AccessMask'>0x100081</Data><Data Name='PrivilegeList'>-</Data>
```

```
<Data Name='RestrictedSidCount'>0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='ResourceAttributes'>-</Data></EventData></Event>
```

L'ID evento 4670 viene registrato quando vengono modificate le autorizzazioni per un oggetto. L'esempio seguente mostra che l'utente «admin» ha modificato l'autorizzazione su «permtest» per aggiungere autorizzazioni al SID ObjectName «S-1-5-21-658495921-4185342820-3824891517-1113". Consulta la documentazione Microsoft per ulteriori informazioni su come interpretare le autorizzazioni.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4670</EventID><Version>0</Version><Level>0</Level>
<Task>13570</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='2021-06-03T19:39:47.537129500Z'/><EventRecordID>308992</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='2776'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0xcc8</Data>
<Data Name='OldSd'>D:PAI(A;OICI;FA;;;SY)
(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-2622)</Data>
<Data Name='NewSd'>D:PARAI(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-1113)
(A;OICI;FA;;;SY)(A;OICI;FA;;;
S-1-5-21-658495921-4185342820-3824891517-2622)</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data></EventData></Event>
```

L'ID evento 5140 viene registrato ogni volta che si accede a una condivisione di file.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5140</EventID><Version>1</Version><Level>0</Level><Task>12808</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:32:07.535208200Z'/>
```

```
<EventRecordID>308947</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='3120'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-2620</
Data>
<Data Name='SubjectUserName'>EC2AMAZ-1GP4HMN$</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2d4ca529</Data><Data Name='ObjectType'>File</Data><Data
 Name='IpAddress'>172.45.6.789</Data>
<Data Name='IpPort'>49730</Data><Data Name='ShareName'>\\AMZNFSXCYDKLDZZ\share</Data>
<Data Name='ShareLocalPath'>\??\D:\share</Data><Data Name='AccessMask'>0x1</Data><Data
 Name='AccessList'>%%4416
    </Data></EventData></Event>
```

L'ID evento 5145 viene registrato quando l'accesso viene negato a livello di condivisione dei file. L'esempio seguente mostra che l'accesso a ShareName «demoshare01" è stato negato.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5145</EventID><Version>0</Version><Level>0</Level>
<Task>12811</Task><Opcode>0</Opcode><Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime='2021-05-19T22:30:40.485188700Z'/><EventRecordID>282939</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='344'/><Channel>Security</Channel>
<Computer>amznfsxtmn9autz.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-
1113</Data><Data Name='SubjectUserName'>Admin</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x95b3fb7</Data><Data Name='ObjectType'>File</Data>
<Data Name='IpAddress'>172.31.7.112</Data><Data Name='IpPort'>59979</Data>
<Data Name='ShareName'>\\AMZNFSXDPNTE0DC\demoshare01</Data><Data Name='ShareLocalPath'>
\??\D:\demoshare01</Data>
<Data Name='RelativeTargetName'>Desktop.ini</Data><Data Name='AccessMask'>0x120089</
Data>
<Data Name='AccessList'>%%1538 %%1541 %%4416 %%4419 %%4423 </Data><Data
 Name='AccessReason'>%%1538:
%%1804 %%1541: %%1805 %%4416: %%1805 %%4419: %%1805 %%4423: %%1805 </Data></
EventData></Event>
```

Se si utilizza CloudWatch Logs Insights per cercare i dati di registro, è possibile eseguire query sui campi degli eventi, come illustrato dai seguenti esempi:

- Per richiedere un ID evento specifico:

```
fields @message
   | filter @message like /4660/
```

- Per interrogare tutti gli eventi che corrispondono a un particolare nome di file:

```
fields @message
   | filter @message like /event.txt/
```

Per ulteriori informazioni sul linguaggio di query CloudWatch Logs Insights, consulta Analyzing Log Data with CloudWatch Logs Insights, nella Amazon CloudWatch Logs User Guide.

Impostazione dei controlli di controllo di file e cartelle

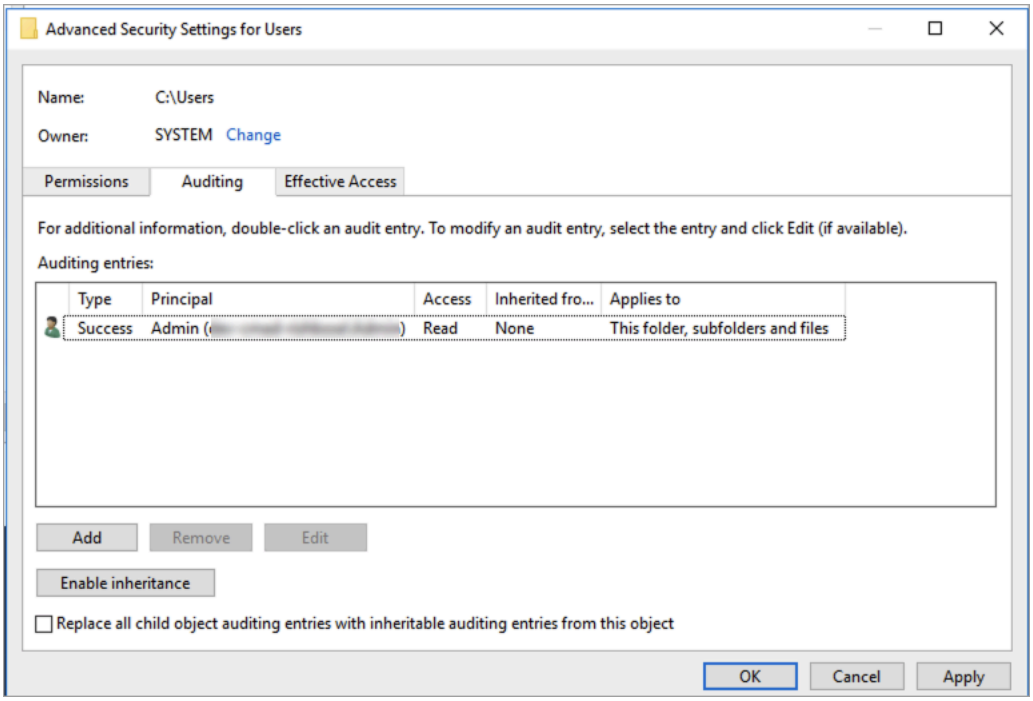
È necessario impostare i controlli di controllo sui file e sulle cartelle che si desidera controllare per i tentativi di accesso degli utenti. I controlli di controllo sono noti anche come elenchi di controllo degli accessi di sistema NTFS (SACL).

I controlli di controllo vengono configurati utilizzando l'interfaccia GUI nativa di Windows o a livello di codice utilizzando i comandi di Windows. PowerShell Se l'ereditarietà è abilitata, in genere è necessario impostare i controlli di controllo solo sulle cartelle di primo livello per le quali si desidera registrare gli accessi.

Utilizzo della GUI di Windows per impostare l'accesso di controllo

Per utilizzare una GUI per impostare i controlli di controllo su file e cartelle, utilizzate Windows File Explorer. Su un determinato file o cartella, apri Windows File Explorer e seleziona la scheda Proprietà > Sicurezza > Avanzate > Controllo.

Il seguente esempio di controllo di controllo verifica gli eventi riusciti per una cartella. Una voce del registro degli eventi di Windows verrà emessa ogni volta che l'handle viene aperto per la lettura correttamente dall'utente amministratore.



Il campo Tipo indica le azioni che si desidera controllare. Imposta questo campo su Operazione riuscita per controllare i tentativi riusciti, Controllo non riuscito dei tentativi falliti o Tutto per controllare sia i tentativi riusciti che quelli non riusciti.

Per ulteriori informazioni sui campi di immissione di controllo, consulta Applicare un criterio di controllo di base su un file o una cartella nella documentazione Microsoft.

Utilizzo dei PowerShell comandi per impostare l'accesso di controllo

È possibile utilizzare il `Set-Acl` comando Microsoft Windows per impostare il SACL di controllo su qualsiasi file o cartella. Per informazioni su questo comando, vedere la documentazione di Microsoft Set-Acl.

Di seguito è riportato un esempio di utilizzo di una serie di PowerShell comandi e variabili per impostare l'accesso di controllo in caso di tentativi riusciti. È possibile adattare questi comandi di esempio in base alle esigenze del file system.

```
$path = "C:\Users\TestUser\Desktop\DemoTest\"

$ACL = Get-Acl $path

$ACL | Format-List
```

```
$AuditUser = "TESTDOMAIN\TestUser"

$AuditRules = "FullControl"

$InheritType = "ContainerInherit,ObjectInherit"

$AuditType = "Success"

$AccessRule = New-Object System.Security.AccessControl.FileSystemAuditRule($AuditUser,
$AuditRules,$InheritType,"None",$AuditType)

$ACL.SetAuditRule($AccessRule)

$ACL | Set-Acl $path

Get-Acl $path -Audit | Format-List
```

Gestione del controllo degli accessi ai file

Puoi abilitare il controllo dell'accesso ai file quando crei un nuovo file system Amazon FSx for Windows File Server. Il controllo dell'accesso ai file è disattivato per impostazione predefinita quando crei un file system dalla console Amazon FSx.

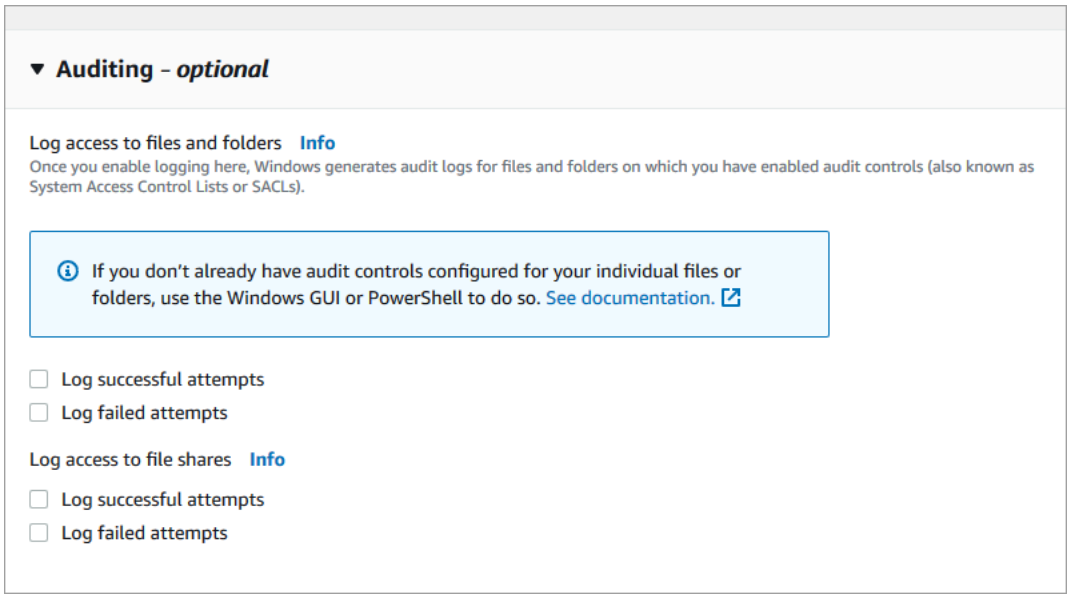
Sui file system esistenti in cui è abilitato il controllo dell'accesso ai file, puoi modificare le impostazioni di controllo dell'accesso ai file, inclusa la modifica dei tipi di tentativo di accesso per gli accessi a file e condivisioni di file e della destinazione del registro degli eventi di controllo. Puoi eseguire queste attività utilizzando la console o l'API Amazon FSx. AWS CLI

> **Note**
>
> Il controllo dell'accesso ai file è supportato solo sui file system Amazon FSx for Windows File Server con una capacità di throughput di 32 MB/s o superiore. Non è possibile creare o aggiornare un file system con una capacità di throughput inferiore a 32 MB/s se il controllo dell'accesso ai file è abilitato. È possibile modificare la capacità di trasmissione in qualsiasi momento dopo la creazione del file system. Per ulteriori informazioni, consulta Gestione della capacità di throughput.

Per abilitare il controllo dell'accesso ai file durante la creazione di un file system (console)

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

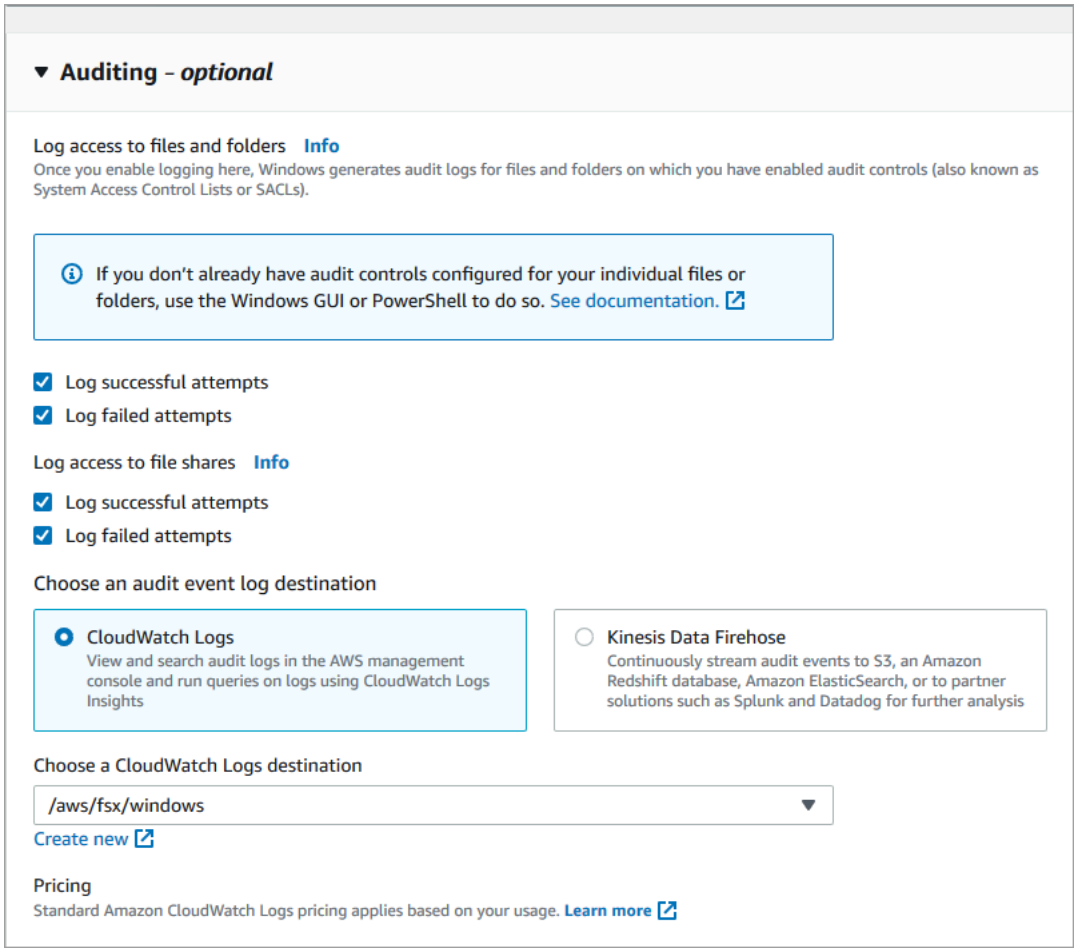
2. Segui la procedura per creare un nuovo file system descritta Crea il tuo file system nella sezione Guida introduttiva.
3. Apri la sezione Auditing - opzionale. Il controllo dell'accesso ai file è disabilitato per impostazione predefinita.



4. Per abilitare e configurare il controllo dell'accesso ai file, procedi come segue.

   - Per Log access a file e cartelle, selezionate la registrazione dei tentativi riusciti e/o falliti. La registrazione è disattivata per file e cartelle se non si effettua una selezione.
   - Per Log access alle condivisioni di file, seleziona la registrazione dei tentativi riusciti e/o falliti. La registrazione è disabilitata per le condivisioni di file se non si effettua una selezione.
   - Per Scegli una destinazione per il registro degli eventi di controllo, scegli CloudWatch Logs o Firehose. Quindi scegli un registro o un flusso di consegna esistente o creane uno nuovo. Per CloudWatch i log, Amazon FSx può creare e utilizzare un flusso di log predefinito nel CloudWatch gruppo `/aws/fsx/windows` Logs log.

   Di seguito è riportato un esempio di configurazione di controllo dell'accesso ai file che verificherà i tentativi di accesso riusciti e falliti degli utenti finali per file, cartelle e condivisioni di file. I registri degli eventi di controllo verranno inviati alla destinazione predefinita del gruppo di `/aws/fsx/windows` log CloudWatch Logs.



5. Continuare con la sezione successiva della procedura guidata per la creazione del file system.

Quando il file system è disponibile, la funzionalità di controllo dell'accesso ai file è abilitata.

Per abilitare il controllo dell'accesso ai file durante la creazione di un file system (CLI)

1. Quando create un nuovo file system, utilizzate la `AuditLogConfiguration` proprietà con l'operazione CreateFileSystemAPI per abilitare il controllo dell'accesso ai file per il nuovo file system.

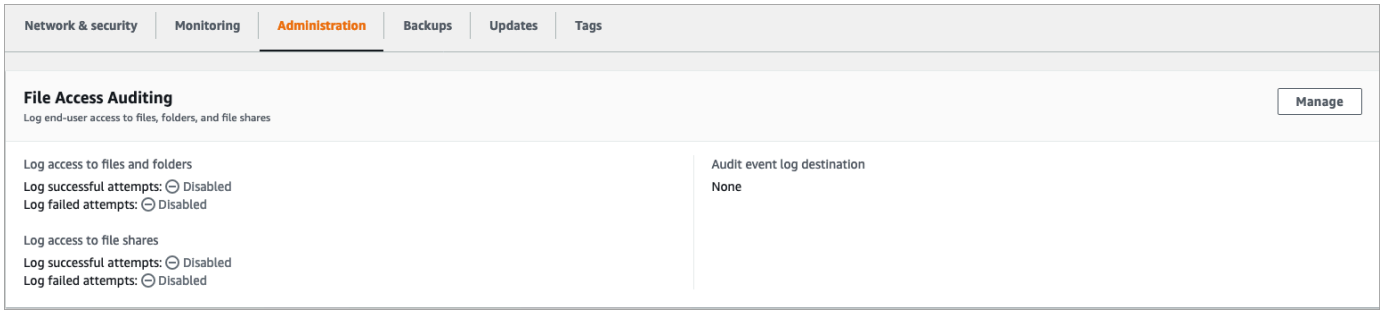
```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
```

```
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-customer-log-group"}'
```

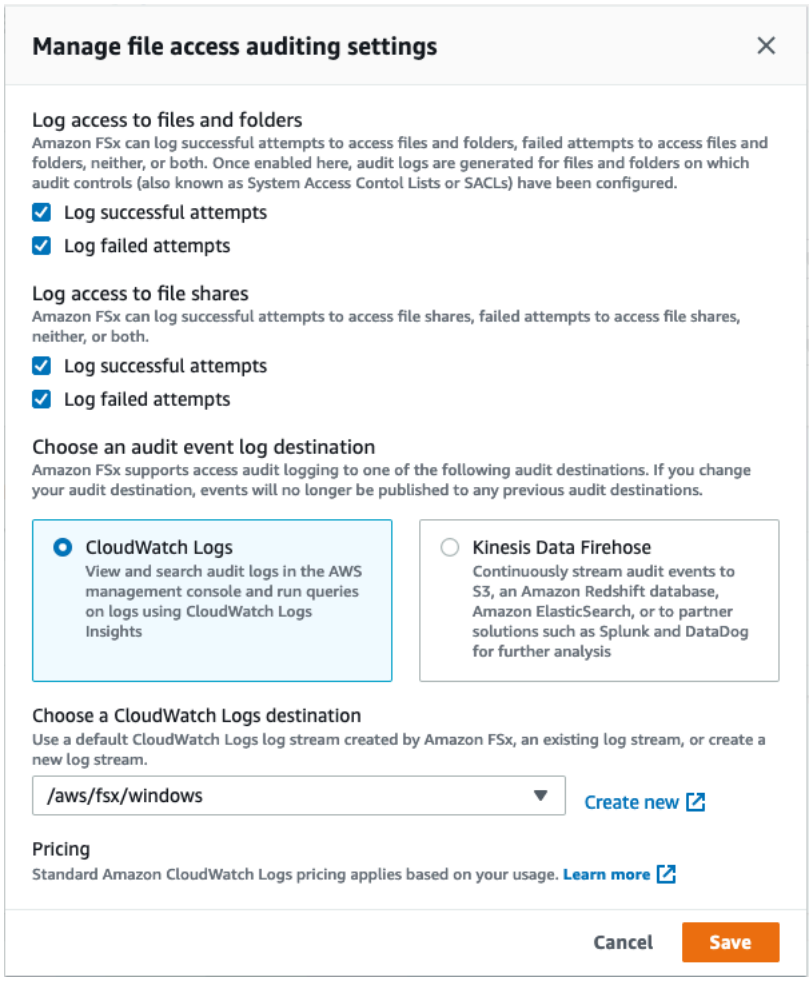
2. Quando il file system è disponibile, la funzionalità di controllo dell'accesso ai file è abilitata.

Per modificare la configurazione del controllo dell'accesso ai file (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il file system Windows per cui desideri gestire il controllo degli accessi ai file.
3. Scegli la scheda Amministrazione.
4. Nel pannello File Access Auditing, scegli Gestisci.



5. Nella finestra di dialogo Gestisci le impostazioni di controllo dell'accesso ai file, modificare le impostazioni desiderate.



- Per Log access a file e cartelle, selezionare la registrazione dei tentativi riusciti e/o falliti. La registrazione è disattivata per file e cartelle se non si effettua una selezione.
- Per Log access alle condivisioni di file, seleziona la registrazione dei tentativi riusciti e/o falliti. La registrazione è disabilitata per le condivisioni di file se non si effettua una selezione.
- Per Scegli una destinazione per il registro degli eventi di controllo, scegli CloudWatch Logs o Firehose. Quindi scegli un registro o un flusso di consegna esistente o creane uno nuovo.

6. Selezionare Salva.

Per modificare la configurazione di controllo dell'accesso ai file (CLI)

- Utilizza il comando `update-file-system`CLI o l'operazione `UpdateFileSystem`API equivalente.

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

```
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_ONLY", \
    FileShareAccessAuditLogLevel="FAILURE_ONLY", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

Sessioni utente e file aperti

È possibile monitorare le sessioni utente connesse e aprire file sul file system FSx for Windows File Server utilizzando lo strumento Cartelle condivise. Lo strumento Cartelle condivise fornisce una posizione centrale per monitorare chi è connesso al file system, oltre a quali file sono aperti e da chi. È possibile utilizzare questo strumento per effettuare le seguenti operazioni:

- Ripristina l'accesso ai file bloccati.
- Disconnetti una sessione utente, chiudendo tutti i file aperti da quell'utente.

Puoi utilizzare lo strumento GUI delle cartelle condivise nativo di Windows e l'interfaccia a riga di comando di Amazon FSx per la gestione remota per gestire le sessioni utente e aprire file PowerShell sul file system FSx for Windows File Server.

Utilizzo della GUI per gestire utenti e sessioni

Le seguenti procedure descrivono in dettaglio come gestire le sessioni utente e aprire file sul file system Amazon FSx utilizzando lo strumento per le cartelle condivise di Microsoft Windows.

Per avviare lo strumento per le cartelle condivise

1. Avvia l'istanza Amazon EC2 e collegala a Microsoft Active Directory a cui è collegato il file system Amazon FSx. A tale scopo, scegli una delle seguenti procedure dalla Guida all'AWS Directory Service amministrazione:

   - Unisciti senza problemi a un'istanza Windows EC2
   - Unisciti manualmente a un'istanza Windows

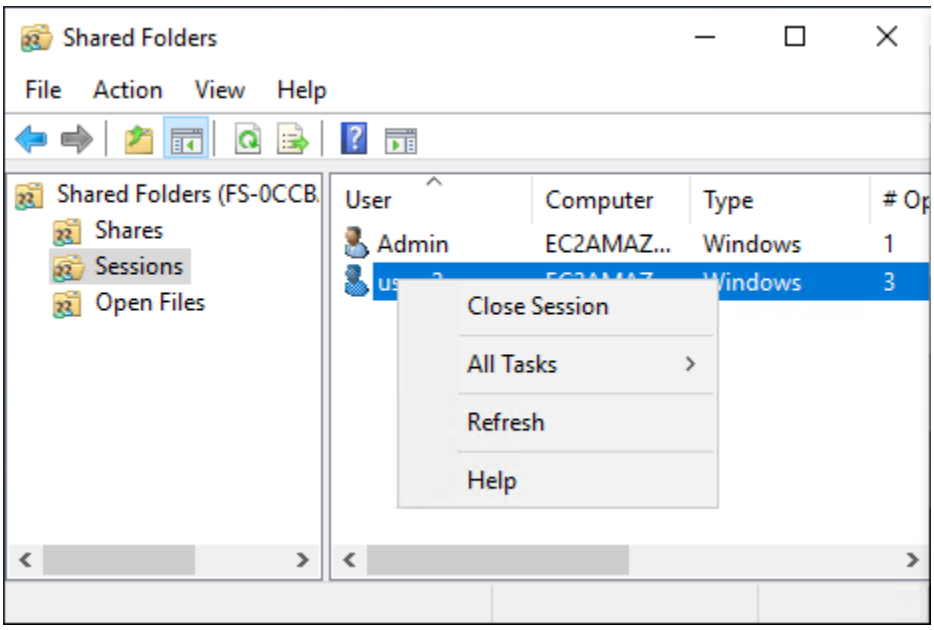
2. Connect alla propria istanza come utente membro del gruppo di amministratori del file system. In AWS Managed Microsoft Active Directory, questo gruppo è denominato AWS Delegated FSx Administrators. In Microsoft Active Directory autogestito, questo gruppo è denominato Domain Admins o il nome personalizzato per il gruppo di amministratori fornito durante la creazione.

Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.

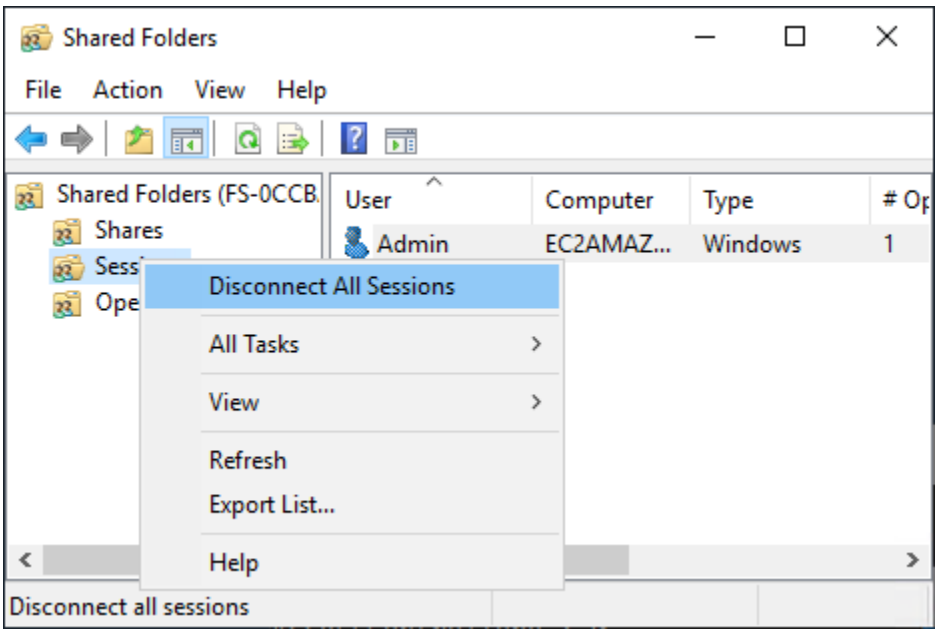
3. Apri il menu Start ed esegui fsmgmt.msc utilizzando. `Run As Administrator` In questo modo si apre lo strumento GUI delle cartelle condivise.
4. Per Azione, scegli Connetti a un altro computer.
5. Per un altro computer, inserisci ad esempio il nome DNS del tuo file system Amazon FSx. `fs-`*`0123456789012345678`*`.`*`ad-domain`*`.com`
6. Scegli OK. Viene quindi visualizzata una voce relativa al file system Amazon FSx nell'elenco dello strumento Cartelle condivise.

Per gestire le sessioni utente (GUI)

Nello strumento Cartelle condivise, scegliete Sessioni per visualizzare tutte le sessioni utente connesse al file system FSx for Windows File Server. Se un utente o un'applicazione accede a una condivisione di file sul tuo file system Amazon FSx, questo snap-in mostra la relativa sessione. Puoi disconnettere le sessioni aprendo il menu contestuale (fai clic con il pulsante destro del mouse) per una sessione e scegliendo Chiudi sessione.

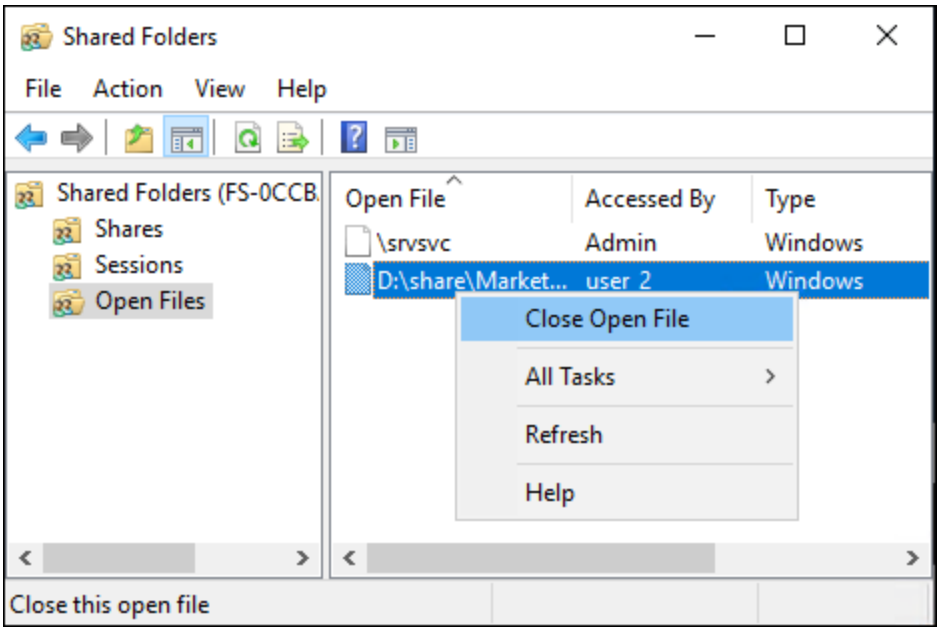


Per disconnettere tutte le sessioni aperte, aprite il menu contestuale (con il pulsante destro del mouse) per Sessioni, scegliete Disconnetti tutte le sessioni e confermate l'azione.

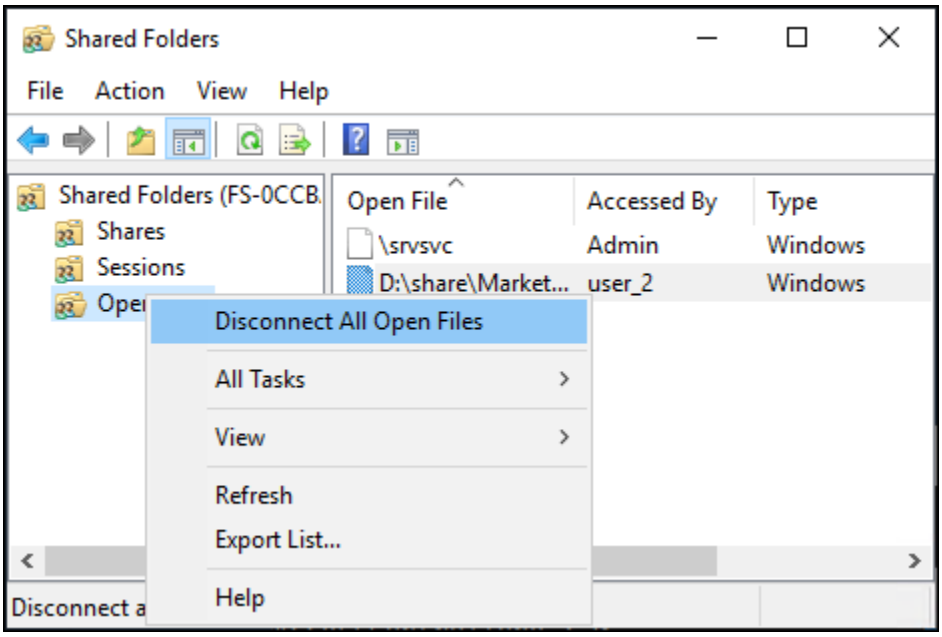


Per gestire i file aperti (GUI)

Nello strumento Cartelle condivise, scegli Apri file per visualizzare tutti i file attualmente aperti sul sistema. La visualizzazione mostra anche quali utenti hanno i file o le cartelle aperti. Queste informazioni possono essere utili per capire perché gli altri utenti non possono aprire determinati file. È possibile chiudere qualsiasi file aperto da qualsiasi utente semplicemente aprendo il menu contestuale (con il pulsante destro del mouse) relativo alla voce del file nell'elenco e scegliendo Chiudi Apri file.



Per disconnettere tutti i file aperti sul file system, apri il menu contestuale (fai clic con il pulsante destro del mouse) per Apri file e scegli Disconnetti tutti i file aperti e conferma l'azione.



Utilizzato PowerShell per gestire le sessioni utente e aprire file

Puoi gestire sessioni utente attive e aprire file sul tuo file system utilizzando l'Amazon FSx CLI per la gestione remota su. PowerShell Per informazioni su come utilizzare questa CLI, consulta. Utilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell

Di seguito sono riportati i comandi che è possibile utilizzare per la gestione delle sessioni utente e dei file aperti.

Comando	Descrizione
Get-FSxSmbSession	Recupera informazioni sulle sessioni Server Message Block (SMB) attualmente stabilite tra il file system e i client associati.
Close-FSxSmbSession	Termina una sessione SMB.
Get-FSxSmbOpenFile	Recupera informazioni sui file aperti per i client connessi al file system.
Close-FSxSmbOpenFile	Chiude un file aperto per uno dei client del server SMB.

La guida in linea di ogni comando fornisce un riferimento a tutte le opzioni di comando. Per accedere a questa guida, esegui il comando con-?, ad esempioGet-FSxSmbSession -?.

Deduplicazione dei dati

FSx supporta l'uso di Microsoft Data Deduplication per identificare ed eliminare i dati ridondanti. I set di dati di grandi dimensioni spesso contengono dati ridondanti, il che aumenta i costi di archiviazione dei dati. Ad esempio, con le condivisioni di file utente, più utenti possono archiviare più copie o versioni dello stesso file. Con le condivisioni di sviluppo software, molti file binari rimangono invariati da una build all'altra.

È possibile ridurre i costi di archiviazione dei dati attivando la deduplicazione dei dati per il file system. La deduplicazione dei dati riduce o elimina i dati ridondanti archiviando parti duplicate del set di dati una sola volta. La compressione dei dati è abilitata per impostazione predefinita quando si utilizza la deduplicazione dei dati, riducendo ulteriormente la quantità di archiviazione dei dati comprimendo i dati dopo la deduplicazione. La deduplicazione dei dati viene eseguita come un processo in background che analizza e ottimizza continuamente e automaticamente il file system ed è trasparente per gli utenti e i client connessi.

I risparmi di storage che è possibile ottenere con la deduplicazione dei dati dipendono dalla natura del set di dati, inclusa la quantità di duplicazione esistente tra i file. I risparmi tipici sono in media del 50-60% per le condivisioni di file per uso generico. Nell'ambito delle azioni, i risparmi vanno dal 30 al 50 percento per i documenti degli utenti al 70-80 percento per i set di dati di sviluppo software. È possibile misurare i potenziali risparmi derivanti dalla deduplicazione utilizzando il comando descritto di seguito. `Measure-FSxDedupFileMetadata`

È inoltre possibile personalizzare la deduplicazione dei dati per soddisfare esigenze di storage specifiche. Ad esempio, è possibile configurare la deduplicazione in modo che venga eseguita solo su determinati tipi di file oppure è possibile creare una pianificazione dei processi personalizzata. Poiché i processi di deduplicazione possono consumare risorse del file server, si consiglia di monitorare lo stato dei processi di deduplicazione utilizzando il comando descritto di seguito. `Get-FSxDedupStatus`

Per ulteriori informazioni sulla deduplicazione dei dati, consulta la documentazione di Microsoft Understanding Data Deduplication.

> **Note**
>
> Consulta le nostre best practice per. Le migliori pratiche per l'utilizzo della deduplicazione dei dati Se riscontri problemi nel far funzionare correttamente i processi di deduplicazione dei dati, consulta. Risoluzione dei problemi di deduplicazione dei dati

> **Warning**
>
> Non è consigliabile eseguire determinati comandi Robocopy con deduplicazione dei dati perché questi comandi possono influire sull'integrità dei dati del Chunk Store. Per ulteriori informazioni, consulta la documentazione sull'interoperabilità di Microsoft Data Deduplication.

Le migliori pratiche per l'utilizzo della deduplicazione dei dati

Ecco alcune best practice per l'utilizzo della deduplicazione dei dati:

- Pianifica l'esecuzione dei processi di deduplicazione dei dati quando il file system è inattivo: la pianificazione predefinita include un `GarbageCollection` processo settimanale alle 2:45 UTC del sabato. Il completamento dell'operazione può richiedere diverse ore se il file system blocca una grande quantità di dati. Se questo periodo non è ideale per il tuo carico di lavoro, pianifica l'esecuzione di questo processo in un momento in cui prevedi uno scarso traffico sul tuo file system.
- Configura una capacità di throughput sufficiente per completare la deduplicazione dei dati: capacità di throughput più elevate forniscono livelli di memoria più elevati. Microsoft consiglia di disporre di 1 GB di memoria per 1 TB di dati logici per eseguire la deduplicazione dei dati. Utilizza la tabella delle prestazioni di Amazon FSx per determinare la memoria associata alla capacità di throughput del file system e assicurati che le risorse di memoria siano sufficienti per le dimensioni dei tuoi dati.
- Personalizza le impostazioni di deduplicazione dei dati per soddisfare le tue esigenze di storage specifiche e ridurre i requisiti di prestazioni: puoi limitare l'ottimizzazione per eseguirla su tipi di file o cartelle specifici o impostare una dimensione e un'età minime del file per l'ottimizzazione. Per ulteriori informazioni, consulta Deduplicazione dei dati.

Gestione della deduplicazione dei dati

Puoi gestire la deduplicazione dei dati sul tuo file system utilizzando l'interfaccia a riga di comando di Amazon FSx per la gestione remota su. PowerShell Per informazioni su come utilizzare questa CLI, consulta. Utilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell

Di seguito sono riportati i comandi che è possibile utilizzare per la deduplicazione dei dati.

Comando di deduplicazione dei dati	Descrizione
Enable-FSxDedup	Abilita la deduplicazione dei dati nella condivisione di file. La compressione dei dati dopo la deduplicazione è abilitata per impostazione predefinita quando si abilita la deduplicazione dei dati.
Disable-FSxDedup	Disattiva la deduplicazione dei dati nella condivisione di file.
Get-FSxDedupConfiguration	Recupera le informazioni di configurazione della deduplica zione, tra cui la dimensione e la data minime del file per l'ottimiz zazione, le impostazioni di compressione e i tipi di file e le cartelle esclusi.
Set-FSxDedupConfiguration	Modifica le impostazioni di configurazione della deduplica zione, tra cui la dimensione e la data minime dei file per l'ottimiz zazione, le impostazioni di compressione e i tipi di file e le cartelle esclusi.
Get-FSxDedupStatus	Recupera lo stato della deduplicazione e include proprietà di sola lettura che descrivono i risparmi e lo stato dell'ottimizzazion e sul file system, i tempi e lo stato di completamento degli ultimi lavori sul file system.
Get-FSxDedupMetadata	Recupera i metadati di ottimizzazione della deduplicazione.
Update-FSxDedupStatus	Calcola e recupera informazioni aggiornate sui risparmi sulla deduplicazione dei dati.

Comando di deduplicazione dei dati	Descrizione
Measure-FSxDedupFileMetadata	Misura e recupera lo spazio di archiviazione potenziale che è possibile recuperare sul file system se si elimina un gruppo di cartelle. Spesso i file hanno blocchi condivisi tra altre cartelle e il motore di deduplicazione calcola quali blocchi sono unici e quali verrebbero eliminati.
Get-FSxDedupSchedule	Recupera le pianificazioni di deduplicazione attualmente definite.
New-FSxDedupSchedule	Crea e personalizza una pianificazione di deduplicazione dei dati.
Set-FSxDedupSchedule	Modifica le impostazioni di configurazione per i piani di deduplicazione dei dati esistenti.
Remove-FSxDedupSchedule	Elimina una pianificazione di deduplicazione.
Get-FSxDedupJob	Ottiene lo stato e le informazioni per tutti i processi di deduplicazione attualmente in esecuzione o in coda.
Stop-FSxDedupJob	Annulla uno o più processi di deduplicazione dei dati specificati.

La guida in linea di ogni comando fornisce un riferimento a tutte le opzioni di comando. Per accedere a questa guida, esegui il comando con-?, ad esempioEnable-FSxDedup -?.

Abilitare la deduplicazione dei dati

È possibile abilitare la deduplicazione dei dati su una condivisione di file Amazon FSx for Windows File Server utilizzando `Enable-FSxDedup` il comando seguente.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {Enable-FsxDedup }
```

Quando abiliti la deduplicazione dei dati, vengono create una pianificazione e una configurazione predefinite. È possibile creare, modificare e rimuovere pianificazioni e configurazioni utilizzando i comandi seguenti.

È possibile utilizzare il `Disable-FSxDedup` comando per disabilitare completamente la deduplicazione dei dati sul file system.

Creazione di una pianificazione per la deduplicazione dei dati

Anche se la pianificazione predefinita funziona bene nella maggior parte dei casi, è possibile creare una nuova pianificazione di deduplicazione utilizzando il `New-FsxDedupSchedule` comando, illustrato di seguito. Le pianificazioni di deduplicazione dei dati utilizzano l'ora UTC.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
New-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Wed,Sat -
Start 08:00 -DurationHours 7
}
```

Questo comando crea una pianificazione denominata `CustomOptimization` che viene eseguita nei giorni di lunedì, mercoledì e sabato, con inizio del processo alle 8:00 (UTC) di ogni giorno, con una durata massima di 7 ore, dopodiché il processo si interrompe se è ancora in esecuzione.

Si noti che la creazione di nuove pianificazioni dei processi di deduplicazione personalizzate non sostituisce né rimuove la pianificazione predefinita esistente. Prima di creare un processo di deduplicazione personalizzato, è possibile disabilitare il processo predefinito se non è necessario.

È possibile disabilitare la pianificazione di deduplicazione predefinita utilizzando il `Set-FsxDedupSchedule` comando, illustrato di seguito.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com
 -ConfigurationName FSxRemoteAdmin -ScriptBlock {Set-FSxDedupSchedule -Name
 “BackgroundOptimization” -Enabled $false}
```

È possibile rimuovere una pianificazione di deduplicazione utilizzando il comando. `Remove-FSxDedupSchedule -Name "ScheduleName"` Si noti che la pianificazione di `BackgroundOptimization` deduplicazione predefinita non può essere modificata o rimossa e dovrà invece essere disabilitata.

Modifica di una pianificazione di deduplicazione dei dati

È possibile modificare una pianificazione di deduplicazione esistente utilizzando il `Set-FsxDedupSchedule` comando, illustrato di seguito.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
Set-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days
 Mon,Tues,Wed,Sat -Start 09:00 -DurationHours 9
}
```

Questo comando modifica la `CustomOptimization` pianificazione esistente in modo che venga eseguita nei giorni dal lunedì al mercoledì e al sabato, avviando il processo alle 9:00 (UTC) di ogni giorno, con una durata massima di 9 ore, dopodiché il processo si interrompe se è ancora in esecuzione.

Per modificare l'età minima del file prima di ottimizzare l'impostazione, utilizzare il comando. `Set-FSxDedupConfiguration`

Visualizzazione della quantità di spazio risparmiato

Per visualizzare la quantità di spazio su disco risparmiata dall'esecuzione della deduplicazione dei dati, utilizzare il `Get-FSxDedupStatus` comando seguente.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FsxRemoteAdmin -ScriptBlock {
Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate

OptimizedFilesCount OptimizedFilesSize SavedSpace OptimizedFilesSavingsRate
------------------- ------------------ ---------- -------------------------
              12587           31163594   25944826                        83
```

> **Note**
>
> I valori mostrati nella risposta al comando per i seguenti parametri non sono affidabili e non è necessario utilizzare questi valori: Capacity,, FreeSpace UsedSpace UnoptimizedSize, e. SavingsRate

Risoluzione dei problemi di deduplicazione dei dati

Esistono diverse cause potenziali dei problemi di deduplicazione dei dati, come descritto nella sezione seguente.

Argomenti

La deduplicazione dei dati non funziona

Utilizzando le istruzioni contenute nella nostra documentazione sulla deduplicazione dei dati, esegui il `Get-FSxDedupStatus` comando per visualizzare lo stato di completamento dei processi di deduplicazione più recenti. Se uno o più processi falliscono, è possibile che non si verifichi un aumento della capacità di archiviazione gratuita sul file system.

Il motivo più comune per cui i processi di deduplicazione non riescono è la memoria insufficiente.

- Microsoft consiglia di disporre in modo ottimale di 1 GB di memoria per 1 TB di dati logici (o almeno 300 MB+ 50 MB per 1 TB di dati logici). Utilizza la tabella delle prestazioni di Amazon FSx per determinare la memoria associata alla capacità di throughput del file system e assicurarti che le risorse di memoria siano sufficienti per le dimensioni dei tuoi dati.
- I processi di deduplicazione sono configurati con l'allocazione di memoria predefinita consigliata da Windows del 25%, il che significa che per un file system con 32 GB di memoria, saranno disponibili 8 GB per la deduplicazione. L'allocazione della memoria è configurabile (utilizzando il `Set-FSxDedupSchedule` comando con parametro`-Memory`), ma il consumo di memoria aggiuntiva può influire sulle prestazioni del file system.
- È possibile modificare la configurazione dei processi di deduplicazione per ridurre ulteriormente i requisiti di memoria. Ad esempio, è possibile limitare l'ottimizzazione in modo che venga eseguita su tipi di file o cartelle specifici oppure impostare una dimensione e una durata minime del file per l'ottimizzazione. Si consiglia inoltre di configurare i processi di deduplicazione in modo che vengano eseguiti durante i periodi di inattività quando il carico sul file system è minimo.

È inoltre possibile che vengano visualizzati errori se il tempo di completamento dei processi di deduplicazione non è sufficiente. Potrebbe essere necessario modificare la durata massima dei lavori, come descritto in. Modifica di una pianificazione di deduplicazione dei dati

Se i processi di deduplicazione non funzionano da molto tempo e durante questo periodo sono state apportate modifiche ai dati sul file system, i processi di deduplicazione successivi potrebbero richiedere più risorse per essere completati correttamente per la prima volta.

I valori di deduplicazione sono inaspettatamente impostati su 0

I valori per `SavedSpace` e `OptimizedFilesSavingsRate` sono inaspettatamente 0 per un file system su cui è stata configurata la deduplicazione dei dati.

Ciò può verificarsi durante il processo di ottimizzazione dello storage quando si aumenta la capacità di archiviazione del file system. Quando aumenti la capacità di storage di un file system, Amazon FSx annulla i processi di deduplicazione dei dati esistenti durante il processo di ottimizzazione dello storage, che migra i dati dai vecchi dischi ai nuovi dischi più grandi. Amazon FSx riprende la deduplicazione dei dati sul file system una volta completato il processo di ottimizzazione dello storage. Per ulteriori informazioni sull'aumento della capacità di storage e sull'ottimizzazione dello storage, consulta. Gestione della capacità di archiviazione

Dopo l'eliminazione dei file non viene liberato spazio sul file system

Il comportamento previsto della deduplicazione dei dati è che se i dati eliminati erano contenuti su cui dedup aveva consentito di risparmiare spazio, lo spazio sul file system non viene effettivamente liberato fino all'esecuzione del processo di raccolta dei rifiuti.

Una pratica che potrebbe risultare utile consiste nell'impostare la pianificazione per l'esecuzione del processo di raccolta dei rifiuti subito dopo aver eliminato un gran numero di file. Al termine del processo di raccolta dei rifiuti, puoi riportare la pianificazione della raccolta dei rifiuti alle impostazioni originali. In questo modo puoi vedere rapidamente lo spazio risultante dalle tue eliminazioni.

Utilizzare la procedura seguente per impostare il processo di raccolta dei rifiuti in modo che venga eseguito tra 5 minuti.

1. Per verificare che la deduplicazione dei dati sia abilitata, utilizzare il comando. `Get-FSxDedupStatus` Per ulteriori informazioni sul comando e sull'output previsto, vedere. Visualizzazione della quantità di spazio risparmiato
2. Usa quanto segue per impostare la pianificazione per eseguire il processo di raccolta dei rifiuti tra 5 minuti.

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
```

```
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. Dopo che il processo di raccolta dei rifiuti è stato eseguito e lo spazio è stato liberato, riporta la pianificazione alle impostazioni originali.

Quote di archiviazione

È possibile configurare le quote di archiviazione degli utenti sui file system per limitare la quantità di spazio di archiviazione dei dati che gli utenti possono consumare. Dopo aver impostato le quote, è possibile tenere traccia dello stato delle quote per monitorare l'utilizzo e vedere quando gli utenti superano le proprie quote.

È inoltre possibile applicare le quote impedendo agli utenti che raggiungono le rispettive quote di scrivere nello spazio di archiviazione. Quando si applicano le quote, un utente che supera la propria quota riceve un messaggio di errore «spazio su disco insufficiente».

Puoi impostare queste soglie per le impostazioni delle quote:

- Avviso: utilizzato per monitorare se un utente o un gruppo si sta avvicinando al limite di quota, rilevante solo per il monitoraggio.
- Limite: il limite di quota di archiviazione per un utente o un gruppo.

È possibile configurare quote predefinite da applicare ai nuovi utenti che accedono a un file system e quote da applicare a utenti o gruppi specifici. Puoi anche visualizzare un rapporto sulla quantità di spazio di archiviazione utilizzata da ciascun utente o gruppo e sull'eventuale superamento delle quote.

Il consumo di storage a livello di utente viene monitorato in base alla proprietà dei file. Il consumo di storage viene calcolato utilizzando la dimensione logica del file, non lo spazio di archiviazione fisico effettivo occupato dai file. Le quote di archiviazione degli utenti vengono tracciate nel momento in cui i dati vengono scritti su un file.

L'aggiornamento delle quote per più utenti richiede l'esecuzione del comando update una volta per ogni utente oppure l'organizzazione degli utenti in un gruppo e l'aggiornamento della quota per quel gruppo.

Gestione delle quote di archiviazione degli utenti

Puoi gestire le quote di storage degli utenti sul tuo file system utilizzando l'interfaccia a riga di comando di Amazon FSx per la gestione remota su. PowerShell Per informazioni su come utilizzare questa CLI, consulta. Utilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell

Di seguito sono riportati i comandi che è possibile utilizzare per gestire le quote di archiviazione degli utenti.

Comando User Storage Quotas	Descrizione
Enable-FSxUserQuotas	Inizia a tracciare o far rispettare le quote di archiviazione degli utenti, o entrambe.
Disable-FSxUserQuotas	Interrompe il monitoraggio e l'applicazione delle quote di archiviazione degli utenti.
Get-FSxUserQuotaSettings	Recupera le impostazioni correnti delle quote di archiviazione utente per il file system.
Get-FSxUserQuotaEntries	Recupera le voci correnti relative alle quote di archiviazione degli utenti per singoli utenti e gruppi sul file system.
Set-FSxUserQuotas	Imposta la quota di archiviazione utente per un singolo utente o gruppo. I valori delle quote sono specificati in byte.

La guida in linea di ogni comando fornisce un riferimento a tutte le opzioni di comando. Per accedere a questa guida, esegui il comando con-?, ad esempioEnable-FSxUserQuotas -?.

Gestione della crittografia in transito

È possibile utilizzare un set di PowerShell comandi personalizzati per controllare la crittografia dei dati in transito tra il file system FSx for Windows File Server e i client. È possibile limitare l'accesso al file system solo ai client che supportano la crittografia SMB in modo che data-in-transit sia sempre crittografata. Quando è attivata la crittografia di data-in-transit, gli utenti che accedono al file system da client che non supportano la crittografia SMB 3.0 non saranno in grado di accedere alle condivisioni di file per le quali è attivata la crittografia.

È inoltre possibile controllare la crittografia a livello di data-in-transit condivisione di file anziché a livello di file server. È possibile utilizzare i controlli di crittografia a livello di condivisione di file per disporre di una combinazione di condivisioni di file crittografate e non crittografate sullo stesso file system se si desidera applicare la crittografia in transito per alcune condivisioni di file che contengono dati sensibili e consentire a tutti gli utenti di accedere ad altre condivisioni di file. La crittografia a livello di server ha la precedenza sulla crittografia a livello di condivisione. Se la crittografia globale è abilitata, non è possibile disabilitare selettivamente la crittografia per determinate condivisioni.

Puoi gestire la crittografia in transito degli utenti sul tuo file system utilizzando l'interfaccia a riga di comando di Amazon FSx per la gestione remota su. PowerShell Per informazioni su come utilizzare questa CLI, consulta. Utilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell

Di seguito sono riportati i comandi che è possibile utilizzare per gestire la crittografia in transito degli utenti sul file system.

Encryption in Transit Command	Descrizione
Get-FSxSmbServerConfiguration	Recupera la configurazione del server Server Message Block (SMB).
Set-FSxSmbServerConfiguration	Questo comando ha due opzioni per configurare la crittografia in transito: • `-EncryptData $True\|$False` — Imposta questo parametro su per `True` attivare la crittografia dei dati in transito. Imposta questo parametro su per `False` disattivare la crittografia dei dati in transito. • `-RejectUnencryptedAccess $True\|$False` — Impostate questo parametro per `True` impedire ai client che non supportano la crittografia di accedere al file system. Impostare questo parametro per consentire `False` ai client che non supportano la crittografia di accedere al file system.

La guida in linea di ogni comando fornisce un riferimento a tutte le opzioni di comando. Per accedere a questa guida, esegui il comando con-?, ad esempioGet-FSxSmbServerConfiguration -?.

Gestione della configurazione dello storage

La configurazione di storage del file system include la capacità di archiviazione, il tipo di storage e gli IOPS SSD. È possibile configurare queste risorse insieme alla capacità di throughput per raggiungere il livello di prestazioni desiderato per il carico di lavoro, durante e dopo la creazione del file system. Per ulteriori informazioni, consulta i seguenti argomenti.

Argomenti

Gestione della capacità di archiviazione

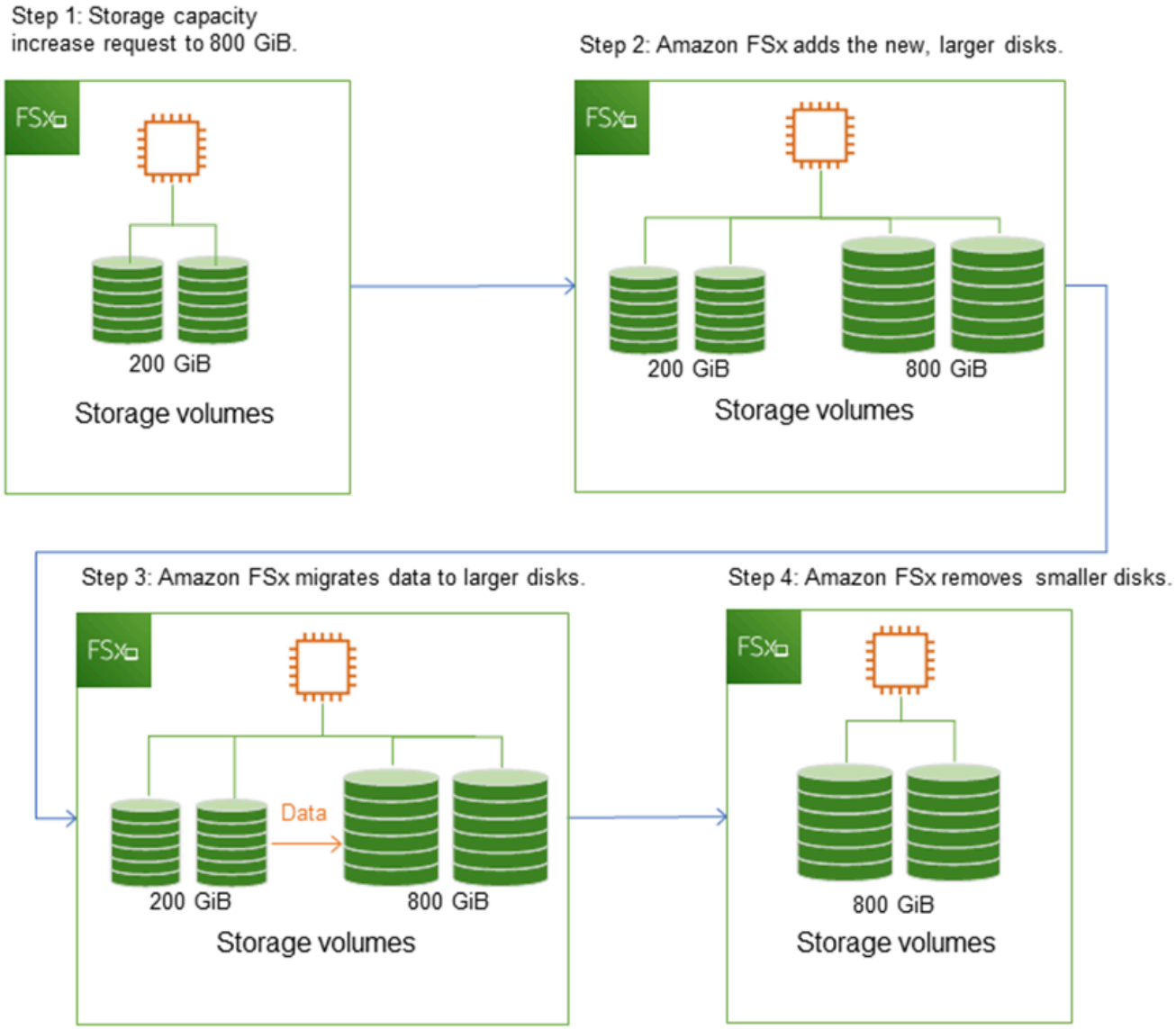
È possibile aumentare la capacità di storage configurata sul file system FSx for Windows File Server in base alle proprie esigenze. Puoi farlo utilizzando la console Amazon FSx, l'API Amazon FSx o (). AWS Command Line Interface AWS CLI Puoi solo aumentare la quantità di capacità di storage per un file system; non puoi diminuire la capacità di storage.

> **Note**
>
> Non è possibile aumentare la capacità di archiviazione per i file system creati prima del 23 giugno 2019 o per i file system ripristinati da un backup appartenente a un file system creato prima del 23 giugno 2019.

Quando aumenti la capacità di storage del tuo file system Amazon FSx, Amazon FSx aggiunge un nuovo set di dischi più grande al tuo file system dietro le quinte. Amazon FSx esegue quindi un processo di ottimizzazione dello storage in background per migrare in modo trasparente i dati dai vecchi dischi ai nuovi dischi. L'ottimizzazione dello storage può richiedere da alcune ore a qualche giorno, con un impatto minimo evidente sulle prestazioni del carico di lavoro. Durante questa ottimizzazione, l'utilizzo del backup è temporaneamente maggiore, poiché sia il vecchio che il nuovo volume di storage sono inclusi nei backup a livello di file system. Entrambi i set di volumi di storage sono inclusi per garantire che Amazon FSx possa eseguire e ripristinare con successo i backup anche durante l'attività di scalabilità dello storage. L'utilizzo del backup torna al livello di base precedente dopo che i vecchi volumi di storage non sono più inclusi nella cronologia dei

backup. Quando la nuova capacità di archiviazione diventa disponibile, ti viene fatturata solo la nuova capacità di archiviazione.

L'illustrazione seguente mostra le quattro fasi principali del processo utilizzato da Amazon FSx per aumentare la capacità di storage di un file system.



Puoi monitorare i progressi dell'ottimizzazione dello storage, gli aumenti della capacità di storage SSD o gli aggiornamenti IOPS degli SSD in qualsiasi momento utilizzando la console Amazon

FSx, la CLI o l'API. Per ulteriori informazioni, consulta Monitoraggio dell'aumento della capacità di archiviazione.

Argomenti

Punti importanti da sapere quando si aumenta la capacità di storage

Ecco alcuni elementi importanti da considerare quando si aumenta la capacità di archiviazione:

- Solo aumento: è possibile solo aumentare la quantità di capacità di archiviazione per un file system, non è possibile diminuire la capacità di archiviazione.
- Aumento minimo: ogni aumento della capacità di storage deve essere pari almeno al 10% della capacità di storage corrente del file system, fino al valore massimo consentito di 65.536 GiB.
- Capacità di throughput minima: per aumentare la capacità di archiviazione, un file system deve avere una capacità di throughput minima di 16 MB/s. Questo perché la fase di ottimizzazione dello storage è un processo che richiede un elevato livello di throughput.
- Tempo tra un aumento e l'altro: non è possibile aumentare ulteriormente la capacità di archiviazione su un file system fino a 6 ore dopo l'ultima richiesta di aumento o fino al completamento del processo di ottimizzazione dello storage, a seconda di quale periodo sia più lungo. Il completamento dell'ottimizzazione dello storage può richiedere da alcune ore a qualche giorno. Per ridurre al minimo il tempo necessario per il completamento dell'ottimizzazione dello storage, si consiglia di aumentare la capacità di trasmissione del file system prima di aumentare la capacità di storage (la capacità di throughput può essere ridotta nuovamente al termine del ridimensionamento dello storage) e di aumentare la capacità di storage quando il traffico sul file system è minimo.

> **Note**
>
> Alcuni eventi del file system possono consumare le risorse prestazionali di I/O del disco. Ad esempio:
> La fase di ottimizzazione della scalabilità della capacità di archiviazione può generare un aumento della velocità effettiva del disco e potenzialmente causare avvisi sulle prestazioni. Per ulteriori informazioni, consulta Avvertenze e consigli sulle prestazioni.

Quando aumentare la capacità di archiviazione

Aumenta la capacità di storage del file system quando la capacità di storage disponibile sta per esaurirsi. Utilizza la `FreeStorageCapacity` CloudWatch metrica per monitorare la quantità di spazio di archiviazione gratuito disponibile sul file system. Puoi creare un CloudWatch allarme Amazon in base a questa metrica e ricevere una notifica quando scende al di sotto di una soglia specifica. Per ulteriori informazioni, consulta Monitoraggio delle metriche con Amazon CloudWatch.

Ti consigliamo di mantenere sempre almeno il 10% della capacità di archiviazione gratuita sul tuo file system. L'utilizzo di tutta la capacità di storage può influire negativamente sulle prestazioni e introdurre incongruenze nei dati.

È possibile aumentare automaticamente la capacità di storage del file system quando la quantità di capacità di archiviazione libera scende al di sotto di una soglia definita dall'utente. Utilizza il AWS CloudFormation modello personalizzato AWS sviluppato da -per distribuire tutti i componenti necessari per implementare la soluzione automatizzata. Per ulteriori informazioni, consulta Aumento dinamico della capacità di storage.

Aumento della capacità di storage e delle prestazioni del file system

La maggior parte dei carichi di lavoro ha un impatto minimo sulle prestazioni, mentre Amazon FSx esegue il processo di ottimizzazione dello storage in background dopo che la nuova capacità di storage è disponibile. Le applicazioni ad alta intensità di scrittura con set di dati attivi di grandi dimensioni potrebbero subire temporaneamente una riduzione fino alla metà delle prestazioni di scrittura. In questi casi, è possibile aumentare la capacità di trasmissione del file system prima di aumentare la capacità di archiviazione. Ciò consente di continuare a fornire lo stesso livello di velocità effettiva per soddisfare le esigenze di prestazioni dell'applicazione. Per ulteriori informazioni, consulta Gestione della capacità di throughput.

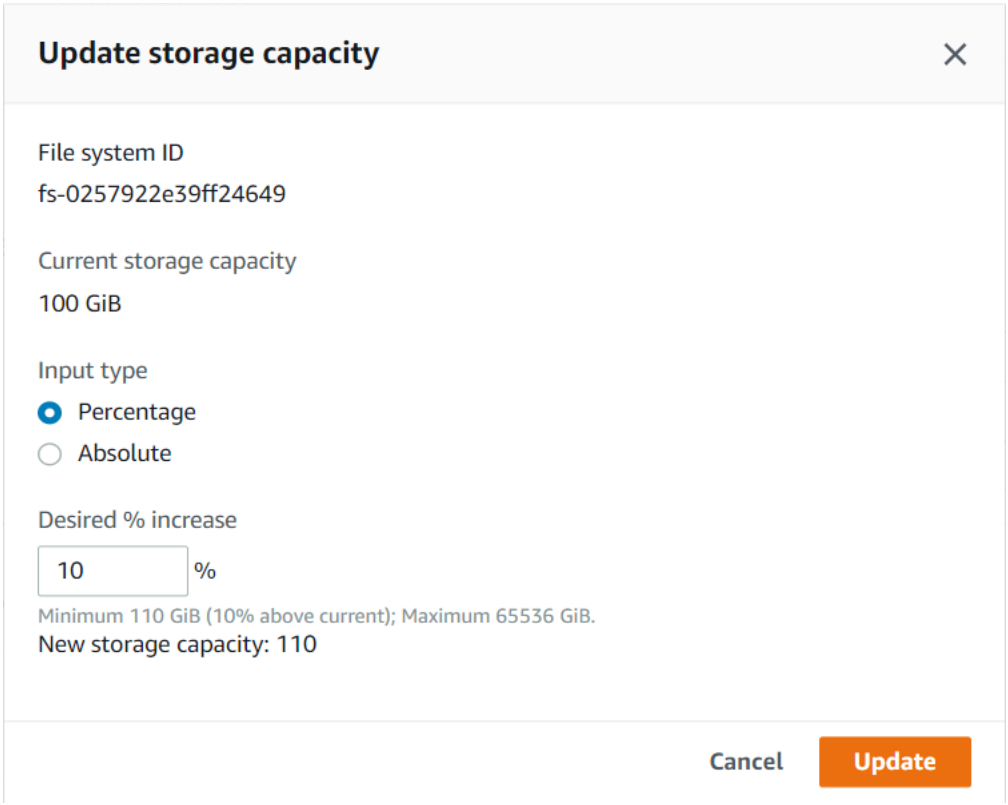
Come aumentare la capacità di archiviazione

Puoi aumentare la capacità di storage di un file system utilizzando la console Amazon FSxAWS CLI, o l'API Amazon FSx.

Per aumentare la capacità di storage di un file system (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il file system Windows per cui desideri aumentare la capacità di storage.
3. Per Azioni, scegli Aggiorna archiviazione. Oppure, nel pannello Riepilogo, scegli Aggiorna accanto alla capacità di archiviazione del file system.

   Viene visualizzata la finestra Aggiorna capacità di archiviazione.



4. Per Tipo di input, scegli Percentuale per inserire la nuova capacità di archiviazione come variazione percentuale rispetto al valore corrente oppure scegli Assoluto per inserire il nuovo valore in GiB.
5. Inserisci la capacità di archiviazione desiderata.

> **Note**
>
> Il valore di capacità desiderato deve essere almeno il 10 percento maggiore del valore attuale, fino al valore massimo di 65.536 GiB.

6. Scegli Aggiorna per avviare l'aggiornamento della capacità di archiviazione.
7. È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system, nella scheda Aggiornamenti.

Per aumentare la capacità di archiviazione per un file system (CLI)

Per aumentare la capacità di archiviazione di un file system FSx for Windows File Server, utilizzare AWS CLI il update-file-systemcomando. Imposta i seguenti parametri:

- `--file-system-id`dall'ID del file system che si sta aggiornando.
- `--storage-capacity`a un valore superiore di almeno il 10 percento rispetto al valore corrente.

È possibile monitorare lo stato di avanzamento dell'aggiornamento utilizzando il AWS CLI comando describe-file-systems. Cerca il `administrative-actions` nell'output.

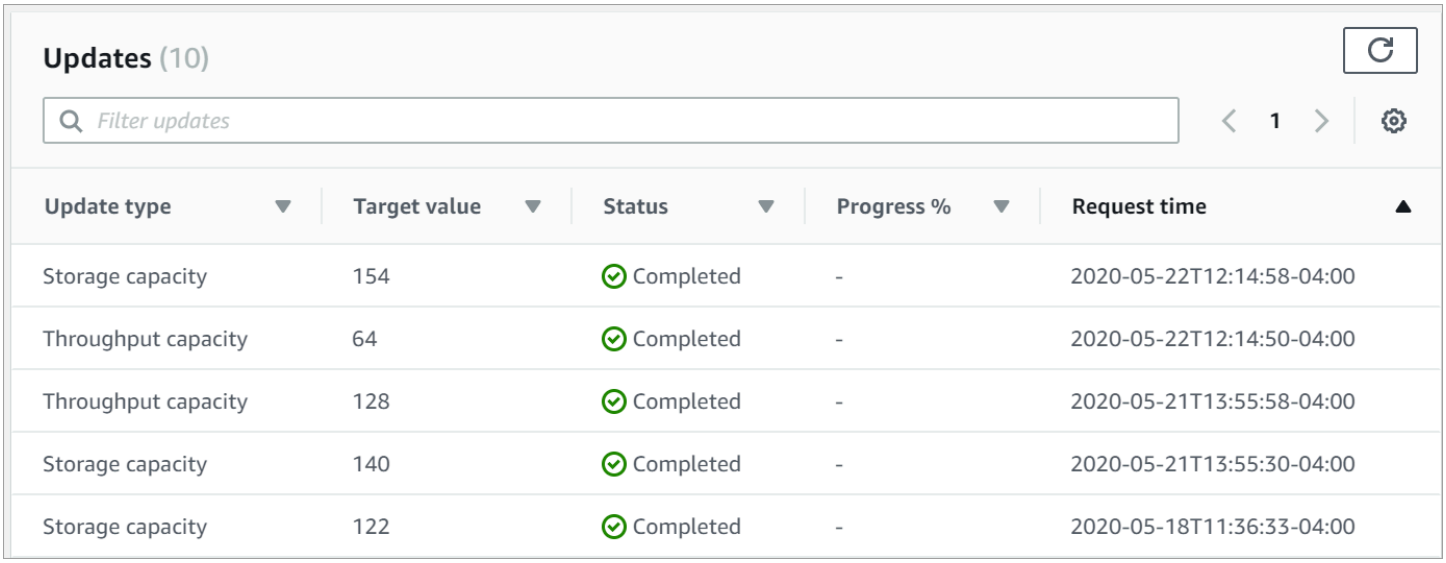
Per ulteriori informazioni, vedere AdministrativeAction.

Monitoraggio dell'aumento della capacità di archiviazione

Puoi monitorare l'avanzamento di un aumento della capacità di storage utilizzando la console Amazon FSx, l'API o il. AWS CLI

Monitoraggio degli aumenti della console

Nella scheda Aggiornamenti della finestra dei dettagli del file system, puoi visualizzare i 10 aggiornamenti più recenti per ogni tipo di aggiornamento.



Per gli aggiornamenti della capacità di archiviazione, è possibile visualizzare le seguenti informazioni.

Tipo di aggiornamento

I valori possibili sono Capacità di archiviazione.

Target value (Valore target)

Il valore desiderato a cui aggiornare la capacità di archiviazione del file system.

Stato

Lo stato attuale dell'aggiornamento. Per gli aggiornamenti della capacità di archiviazione, 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.
- Ottimizzazione aggiornata: Amazon FSx ha aumentato la capacità di storage del file system. Il processo di ottimizzazione dello storage sta ora spostando i dati del file system sui nuovi dischi più grandi.
- Completato: l'aumento della capacità di archiviazione è stato completato con successo.
- Fallito: l'aumento della capacità di archiviazione non è riuscito. Scegli il punto interrogativo (?) per visualizzare i dettagli sul motivo per cui l'aggiornamento dello storage non è riuscito.

Progresso%

Visualizza l'avanzamento del processo di ottimizzazione dello storage come percentuale di completamento.

Orario della richiesta

L'ora in cui Amazon FSx ha ricevuto la richiesta di azione di aggiornamento.

Il monitoraggio aumenta con l'API AWS CLI and

È possibile visualizzare e monitorare le richieste di aumento della capacità di archiviazione del file system utilizzando il describe-file-systemsAWS CLIcomando e l'azione DescribeFileSystemsAPI. L'`AdministrativeActions`array elenca le 10 azioni di aggiornamento più recenti per ogni tipo di azione amministrativa. Quando si aumenta la capacità di archiviazione di un file system, `AdministrativeActions` ne vengono generate due: una `FILE_SYSTEM_UPDATE` e un'`STORAGE_OPTIMIZATIO`Nazione.

L'esempio seguente mostra un estratto della risposta di un comando CLIdescribe-file-systems. Il file system ha una capacità di archiviazione di 300 GB ed è in corso un'azione amministrativa per aumentare la capacità di archiviazione a 1000 GB.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 1000
                     }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
```

```
                    "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 è mostrato nel seguente estratto della risposta di un comando CLIdescribe-file-systems.

La `ProgressPercent` proprietà mostra lo stato di avanzamento del processo di ottimizzazione dello storage. Una volta completato correttamente il processo di ottimizzazione dello storage, lo stato dell'`FILE_SYSTEM_UPDATE`azione cambia in `COMPLETED` e l'`STORAGE_OPTIMIZATIO`Nazione non viene più visualizzata.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 1000
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

Se l'aumento della capacità di archiviazione fallisce, lo stato dell'`FILE_SYSTEM_UPDATE`azione cambia in`FAILED`. La `FailureDetails` proprietà fornisce informazioni sull'errore, illustrate nell'esempio seguente.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 1000
                }
            ]
```

Per informazioni sulla risoluzione dei problemi relativi alle azioni non riuscite, vedereGli aggiornamenti della capacità di storage o di throughput falliscono.

Aumento dinamico della capacità di storage di un file system FSx for Windows File Server

È possibile utilizzare la seguente soluzione per aumentare dinamicamente la capacità di storage di un file system FSx for Windows File Server quando la quantità di capacità di storage libera scende al di sotto di una soglia definita dall'utente. Questo AWS CloudFormation modello distribuisce automaticamente tutti i componenti necessari per definire la soglia di capacità di storage libera, l' CloudWatchallarme Amazon basato su tale soglia e la AWS Lambda funzione che aumenta la capacità di storage del file system.

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

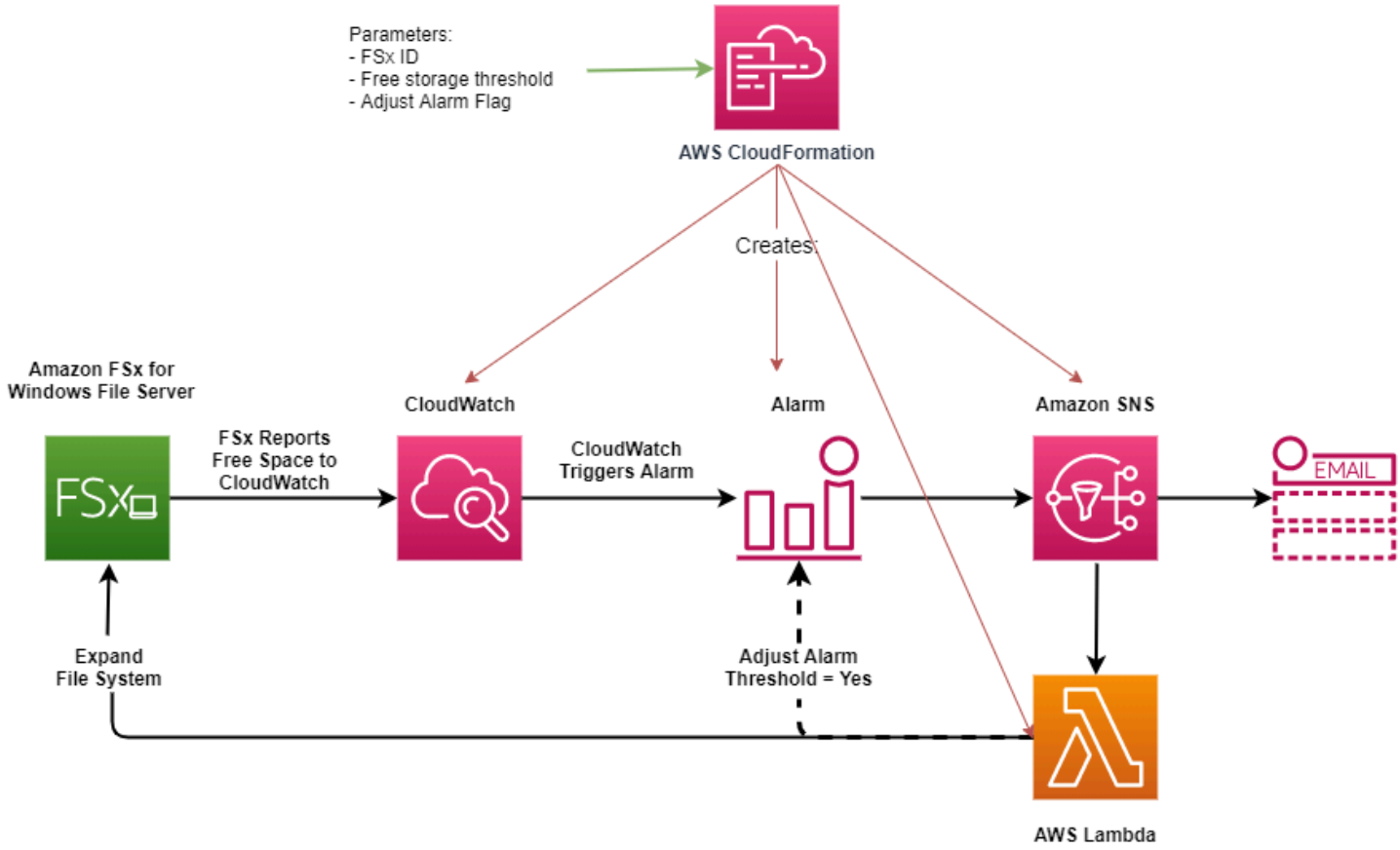
- L'ID del file system

- La soglia di capacità di archiviazione gratuita (valore numerico)
- Unità di misura (percentuale [impostazione predefinita] o GiB)
- La percentuale con cui aumentare la capacità di archiviazione (%)
- L'indirizzo e-mail per l'abbonamento SNS
- Regola la soglia di allarme (Sì/No)

Argomenti

Panoramica dell'architettura

L'implementazione di questa soluzione crea le seguenti risorse nel cloud. AWS



Il diagramma illustra i passaggi seguenti:

1. Il AWS CloudFormation modello implementa 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 libera del file system scende al di sotto della soglia specificata e invia un messaggio alla coda di Amazon SNS.
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. La funzione Lambda può facoltativamente regolare la soglia di capacità di archiviazione libera in modo che sia uguale a una percentuale specificata della nuova capacità di archiviazione del file system.
6. 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.

Modello AWS CloudFormation

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

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

FileSystemId

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

LowFreeDataStorageCapacityThreshold

Nessun valore predefinito. Speciifica la soglia iniziale di capacità di archiviazione libera alla quale attivare un allarme e aumentare automaticamente la capacità di archiviazione del file system,

specificata in GiB o come percentuale (%) della capacità di archiviazione corrente del file system. Se espresso in percentuale, il CloudFormation modello viene ricalcolato in GiB in modo che corrisponda alle impostazioni di allarme. CloudWatch

LowFreeDataStorageCapacityThresholdUnit

L'impostazione predefinita è%. Specificate le unità per`LowFreeDataStorageCapacityThreshold`, in GiB o come percentuale della capacità di archiviazione corrente.

AlarmModificationNotification

L'impostazione predefinita è Sì. Se impostato su Sì, il valore iniziale `LowFreeDataStorageCapacityThreshold` viene aumentato proporzionalmente al valore delle soglie `PercentIncrease` di allarme successive.

Ad esempio, se `PercentIncrease` è impostata su 20 e AlarmModificationNotification impostata su Sì, la soglia di spazio libero disponibile (`LowFreeDataStorageCapacityThreshold`) specificata in GiB viene aumentata del 20% per i successivi eventi di aumento della capacità di archiviazione.

EmailAddress

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

PercentIncrease

Nessun valore predefinito. Speciifica la quantità di cui aumentare la capacità di archiviazione, espressa come percentuale della capacità di archiviazione corrente.

Implementazione automatizzata con AWS CloudFormation

La procedura seguente configura e implementa uno AWS CloudFormation stack per aumentare automaticamente la capacità di archiviazione di un file system FSx for Windows File Server. L'implementazione richiede circa 5 minuti.

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

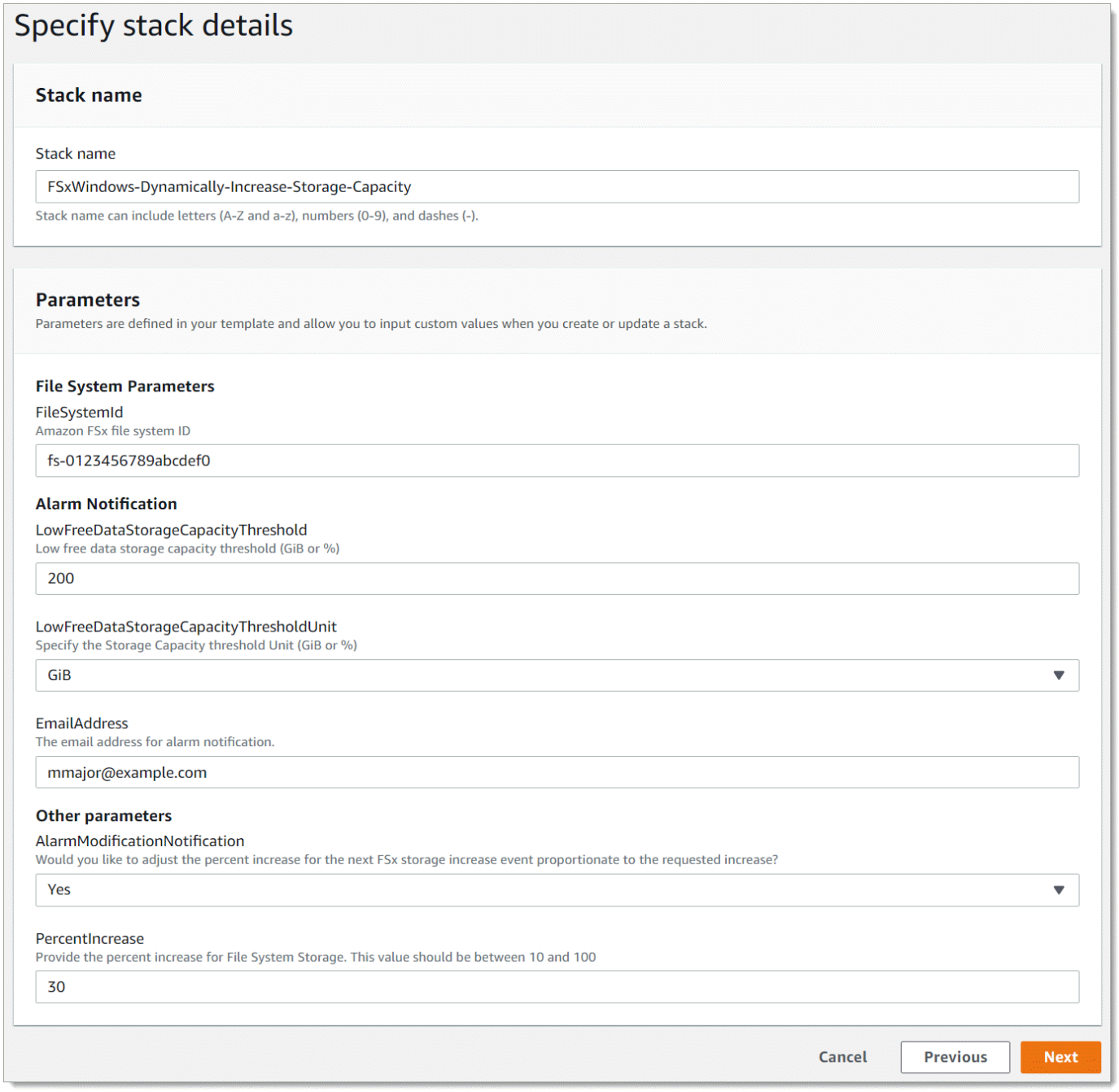
Prima di iniziare, devi avere l'ID del file system Amazon FSx in esecuzione su Amazon Virtual Private Cloud (Amazon VPC) nel tuo account. AWS Per ulteriori informazioni sulla creazione di risorse Amazon FSx, consulta. Guida introduttiva ad Amazon FSx for Windows File Server

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

1. Scarica il modello IncreaseF SxSizeAWS CloudFormation. Per ulteriori informazioni sulla creazione di uno CloudFormation stack, consulta Creazione di uno stack sulla AWS CloudFormation console nella Guida per l'AWS CloudFormationutente.

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

2. In Specificare i dettagli dello stack, inserisci i valori per la tua soluzione di aumento automatico della capacità di storage.



3. Immettete il nome dello stack.
4. Per Parametri, esaminate i parametri del modello e modificateli in base alle esigenze del file system. Quindi scegli Next (Successivo).
5. Immettete le impostazioni delle opzioni desiderate per la soluzione personalizzata, quindi scegliete Avanti.
6. Per Revisione, rivedi e conferma le impostazioni della soluzione. È necessario selezionare la casella di controllo per confermare che il modello crea risorse IAM.

7. Scegliere Create (Crea) per distribuire lo stack.

Puoi visualizzare lo stato dello stack nella console AWS CloudFormation nella colonna Status (Stato). Dovresti vedere lo stato di CREATE_COMPLETE tra circa 5 minuti.

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 CloudFormationutente.

Gestione del tipo di storage

FSx for Windows File Server offre tipi di storage su unità a stato solido (SSD) e unità disco rigido magnetico (HDD). Lo storage SSD è progettato per i carichi di lavoro con le prestazioni più elevate e la maggior parte dei carichi di lavoro sensibili alla latenza, inclusi database, carichi di lavoro di elaborazione multimediale e applicazioni di analisi dei dati. Lo storage su HDD è progettato per un ampio spettro di carichi di lavoro, tra cui home directory, condivisioni di file tra utenti e dipartimenti e sistemi di gestione dei contenuti.

Puoi modificare il tipo di storage del file system da HDD a SSD utilizzando la console Amazon FSx o l'API Amazon FSx. Non puoi modificare il tipo di storage del file system da SSD a HDD. Tieni presente che non puoi aggiornare nuovamente la configurazione del file system prima di 6 ore dopo la richiesta dell'ultimo aggiornamento o fino al completamento del processo di ottimizzazione dello storage, a seconda di quale periodo sia più lungo. Il completamento dell'ottimizzazione dello storage può richiedere da alcune ore a qualche giorno. Per ridurre al minimo questo tempo, ti consigliamo di aggiornare il tipo di archiviazione quando il traffico sul file system è minimo.

Puoi anche modificare il tipo di storage del file system da HDD a SSD ripristinando un backup disponibile per creare un nuovo file system e selezionando un nuovo tipo di archiviazione. Per ulteriori informazioni, consulta Ripristino dei backup.

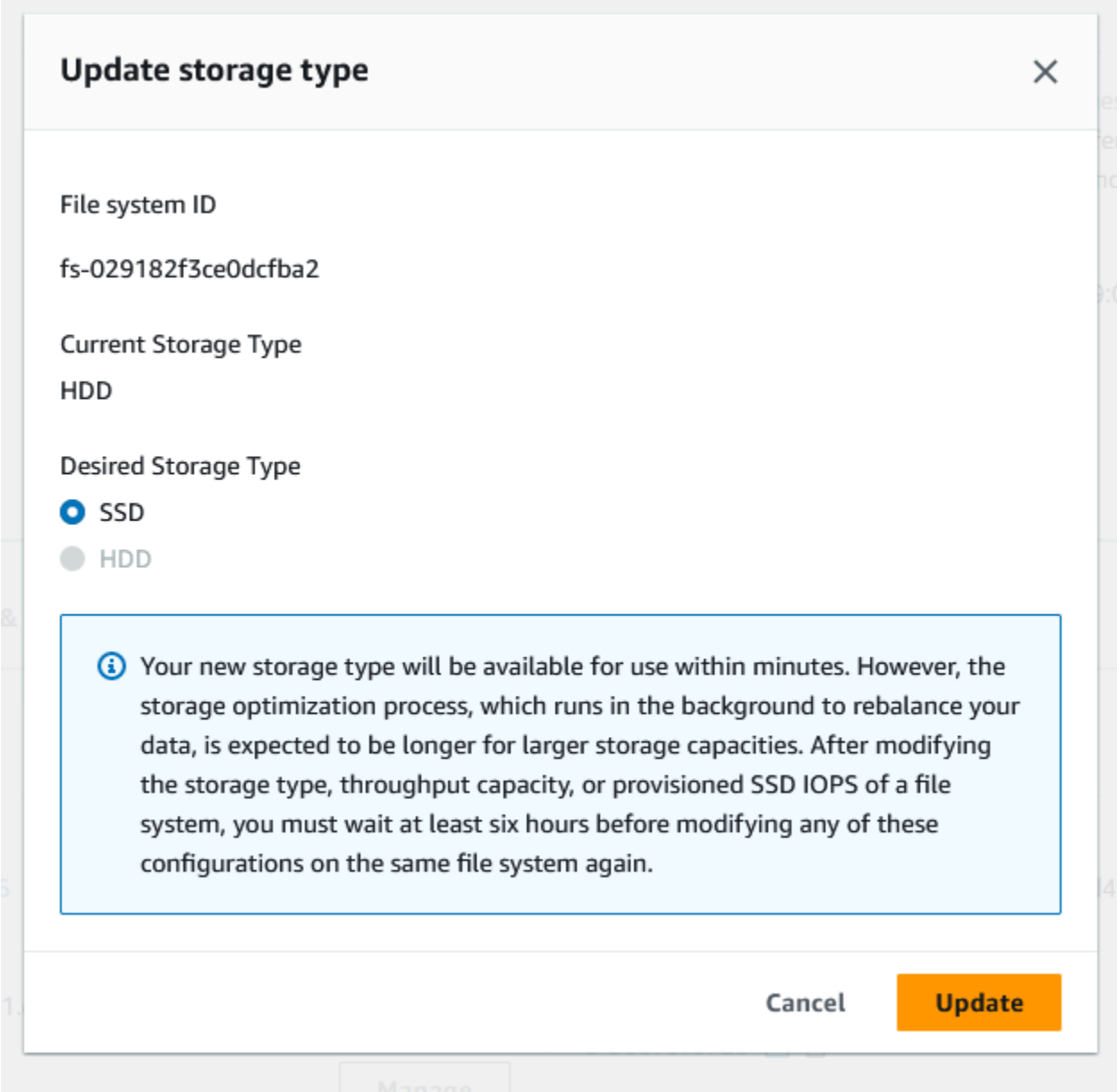
Come aggiornare il tipo di archiviazione

Puoi aggiornare il tipo di storage di un file system utilizzando la console Amazon FSxAWS CLI, o l'API Amazon FSx.

Per aggiornare il tipo di storage per un file system (console)

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

2. Passa a File system e scegli il file system Windows per cui desideri aggiornare il tipo di storage.
3. In Azioni, scegli Aggiorna tipo di archiviazione. Oppure, nel pannello Riepilogo, seleziona il pulsante Aggiorna accanto a HDD. Viene visualizzata la finestra del tipo di archiviazione dell'aggiornamento.



4. Per Tipo di archiviazione desiderato, scegli SSD. Scegli Aggiorna per avviare l'aggiornamento del tipo di archiviazione.
5. È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system, nella scheda Aggiornamenti.

Per aggiornare il tipo di archiviazione per un file system (CLI)

Per aggiornare il tipo di storage per un file system FSx for Windows File Server, utilizzare AWS CLI il update-file-systemcomando. Imposta i seguenti parametri:

- `--file-system-id`all'ID del file system che si desidera aggiornare.
- `--storage-type`su SSD. Non è possibile passare dal tipo di archiviazione SSD al tipo di archiviazione HDD.

È possibile monitorare lo stato di avanzamento dell'aggiornamento utilizzando il AWS CLI comando. describe-file-systems Cerca il `administrative-actions` nell'output.

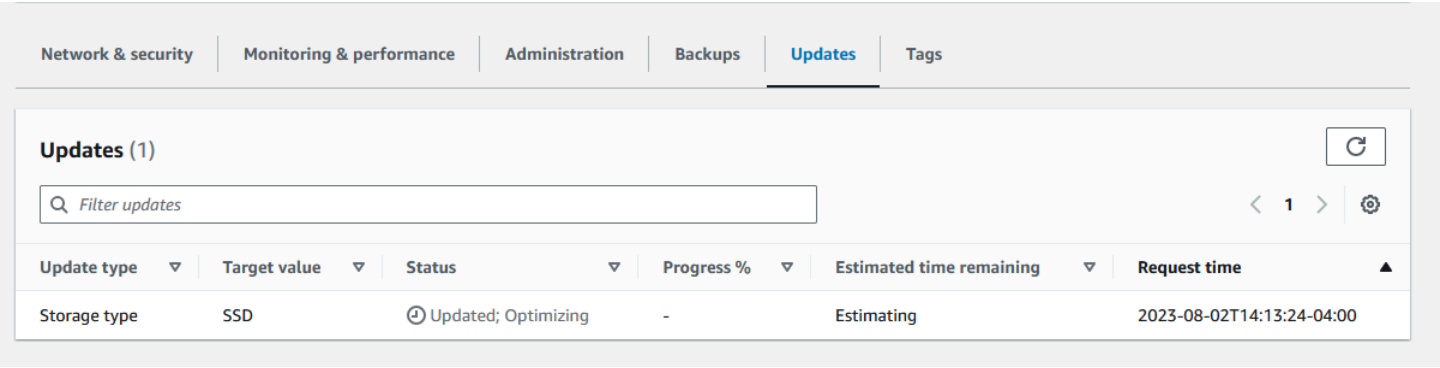
Per ulteriori informazioni, vedere AdministrativeAction.

Monitoraggio degli aggiornamenti dei tipi di archiviazione

Puoi monitorare lo stato di avanzamento di un aggiornamento del tipo di storage utilizzando la console Amazon FSx, l'API o il. AWS CLI

Monitoraggio degli aggiornamenti nella console

Nella scheda Aggiornamenti della finestra dei dettagli del file system, puoi visualizzare i 10 aggiornamenti più recenti per ogni tipo di aggiornamento.



Per gli aggiornamenti dei tipi di archiviazione, è possibile visualizzare le seguenti informazioni.

Tipo di aggiornamento

Il valore possibile è Tipo di archiviazione.

Target value (Valore target)

SSD

Stato

Lo stato attuale dell'aggiornamento. Per gli aggiornamenti dei tipi di archiviazione, 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.
- Ottimizzazione aggiornata: le prestazioni dello storage SSD sono disponibili per le operazioni di scrittura del carico di lavoro. L'aggiornamento entrerà in uno stato di ottimizzazione Aggiornato, che in genere dura alcune ore, durante il quale le operazioni di lettura del carico di lavoro avranno livelli di prestazioni compresi tra HDD e SSD. Una volta completata l'operazione di aggiornamento, le prestazioni del nuovo SSD sono disponibili sia in lettura che in scrittura.
- Completato: l'aggiornamento del tipo di archiviazione è stato completato correttamente.
- Non riuscito: l'aggiornamento del tipo di archiviazione non è riuscito. Scegli il punto interrogativo (?) per vedere i dettagli.

Progresso%

Visualizza l'avanzamento del processo di ottimizzazione dello storage in base alla percentuale di completamento.

Orario della richiesta

L'ora in cui Amazon FSx ha ricevuto la richiesta di azione di aggiornamento.

Monitoraggio degli aggiornamenti con l'API AWS CLI and

È possibile visualizzare e monitorare le richieste di aggiornamento del tipo di storage del file system utilizzando il describe-file-systemsAWS CLIcomando e l'azione DescribeFileSystemsAPI. L'`AdministrativeActions`array elenca le 10 azioni di aggiornamento più recenti per ogni tipo di azione amministrativa. Quando si aumentano gli IOPS SSD di un file system, ne `AdministrativeActions` vengono generate due: una `FILE_SYSTEM_UPDATE` e un'`STORAGE_TYPE_OPTIMIZATIO`Nazione.

Gestione degli IOPS SSD

Per i volumi di archiviazione SSD, puoi selezionare e scalare gli IOPS indipendentemente dalla capacità di archiviazione. Il numero massimo di IOPS SSD che è possibile fornire dipende dalla

quantità di capacità di archiviazione e dalla capacità di throughput selezionate per il file system. Se si tenta di aumentare gli IOPS dell'SSD oltre il limite supportato dalla capacità di throughput, potrebbe essere necessario aumentare la capacità di throughput per supportare il livello di IOPS SSD richiesto. Per ulteriori informazioni, consultare Prestazioni di FSx for Windows File Server e Gestione della capacità di throughput.

Argomenti

Punti importanti da sapere durante l'aggiornamento degli IOPS SSD

Ecco alcuni elementi importanti da considerare durante l'aggiornamento degli IOPS SSD:

- Per specificare la quantità di IOPS SSD assegnati per il file system, è necessario scegliere una delle due modalità IOPS:
  - Automatico: Amazon FSx ridimensiona automaticamente gli IOPS SSD per mantenere 3 IOPS SSD per GiB di capacità di storage, fino a 400.000 IOPS SSD per file system.
  - Fornito dall'utente: specifichi il numero di IOPS SSD nell'intervallo 96-400.000. Specificare un numero compreso tra 3 e 50 IOPS per GiB di capacità di storage per tutti i paesi in cui è disponibile Regioni AWS Amazon FSx o tra 3 e 500 IOPS per GiB di capacità di storage negli Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti orientali (Ohio), Europa (Irlanda), Asia Pacifico (Tokyo) e Asia Pacifico (Singapore). Se la quantità di IOPS SSD non è almeno 3 IOPS per GiB, la richiesta ha esito negativo. Per livelli più elevati di IOPS SSD assegnati, si paga per gli IOPS medi superiori a 3 IOPS per GiB per file system.
- Aggiornamenti della capacità di storage: se aumenti la capacità di storage e la nuova capacità richiede un livello di IOPS SSD più elevato rispetto al livello IOPS SSD fornito dall'utente, Amazon FSx passa automaticamente il file system alla modalità Automatica.
- Aggiornamenti della capacità di throughput: se aumenti la capacità di throughput e il numero massimo di IOPS SSD supportato dalla nuova capacità di throughput è superiore al livello di IOPS SSD fornito dall'utente, Amazon FSx passa automaticamente il file system alla modalità Automatica.
- Tempo tra un aumento e l'altro: non è possibile aumentare ulteriormente gli IOPS SSD, aumentare la capacità di throughput o aggiornare il tipo di storage su un file system fino a 6 ore dopo l'ultima

richiesta di aumento o fino al completamento del processo di ottimizzazione dello storage, a seconda di quale periodo sia più lungo. Il completamento dell'ottimizzazione dello storage può richiedere da alcune ore a qualche giorno. Per ridurre al minimo il tempo necessario per il completamento dell'ottimizzazione dello storage, consigliamo di scalare gli IOPS SSD quando il traffico sul file system è minimo.

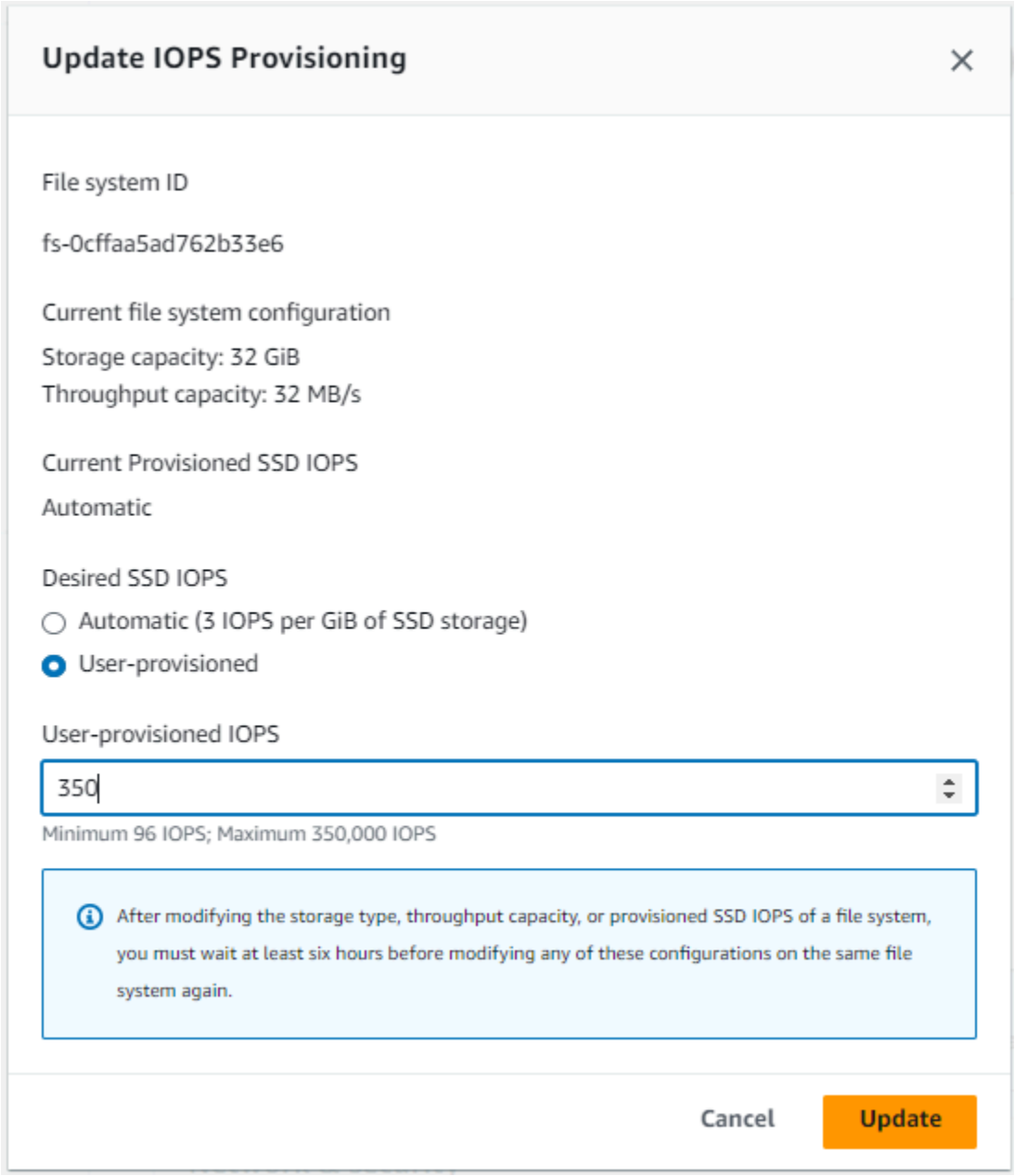
> **Note**
>
> Tieni presente che i livelli di capacità di throughput pari o superiori a 4.608 MBps sono supportati solo nei seguenti paesiRegioni AWS: Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti orientali (Ohio), Europa (Irlanda), Asia Pacifico (Tokyo) e Asia Pacifico (Singapore).

Come aggiornare gli IOPS SSD

Puoi aggiornare gli IOPS SSD per un file system utilizzando la console Amazon FSx, AWS CLI o l'API Amazon FSx.

Per aggiornare gli IOPS SSD per un file system (console)

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Passa a File system e scegli il file system Windows per cui desideri aggiornare gli IOPS SSD.
3. In Azioni, scegli Aggiorna IOPS SSD. Oppure, nel pannello Riepilogo, seleziona il pulsante Aggiorna accanto a Provisioned SSD IOPS. Viene visualizzata la finestra di provisioning Update IOPS.



4. Per Modalità, scegli Automatico o Provisionato dall'utente. Se scegli Automatic, Amazon FSx fornisce automaticamente 3 IOPS SSD per GiB di capacità di storage per il tuo file system. Se scegli User-provisioned, inserisci un numero intero compreso tra 96 e 400.000.
5. Scegli Aggiorna per avviare l'aggiornamento IOPS dell'SSD fornito.
6. Puoi monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system, nella scheda Aggiornamenti.

Per aggiornare gli IOPS SSD per un file system (CLI)

Per aggiornare gli IOPS SSD per un file system FSx for Windows File Server, utilizzare la proprietà. `--windows-configuration DiskIopsConfiguration` Questa proprietà ha due parametri e: `Iops Mode`

- Se desideri specificare il numero di IOPS SSD`Iops=`*`number_of_IOPS`*, utilizza fino a un massimo di 400.000 nelle regioni supportate AWS e. `Mode=USER_PROVISIONED`
- Se desideri che Amazon FSx aumenti automaticamente gli IOPS degli SSD, usa `Mode=AUTOMATIC` e non usare il parametro. `Iops` Amazon FSx mantiene automaticamente 3 IOPS SSD per GiB di capacità di storage sul file system, fino a un massimo di 400.000 nelle regioni supportate. AWS

È possibile monitorare lo stato di avanzamento dell'aggiornamento utilizzando il comando. AWS CLI describe-file-systems Cerca il `administrative-actions` nell'output.

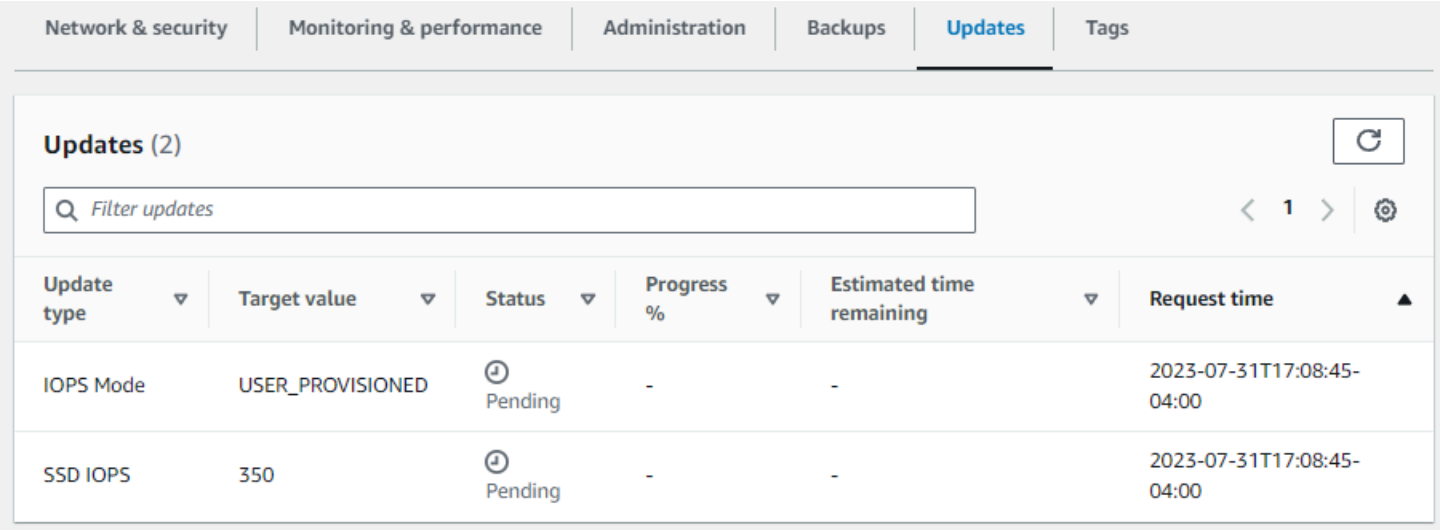
Per ulteriori informazioni, vedere AdministrativeAction.

Monitoraggio degli aggiornamenti IOPS degli SSD forniti

Puoi monitorare lo stato di avanzamento di un aggiornamento IOPS SSD fornito utilizzando la console Amazon FSx, l'API o il. AWS CLI

Monitoraggio degli aggiornamenti nella console

Nella scheda Aggiornamenti della finestra dei dettagli del file system, puoi visualizzare i 10 aggiornamenti più recenti per ogni tipo di aggiornamento.



Per gli aggiornamenti IOPS degli SSD forniti, è possibile visualizzare le seguenti informazioni.

Tipo di aggiornamento

I valori possibili sono IOPS Mode e SSD IOPS.

Target value (Valore target)

Il valore desiderato a cui aggiornare la modalità IOPS e gli IOPS SSD del file system.

Stato

Lo stato attuale dell'aggiornamento. Per gli aggiornamenti IOPS SSD, 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.
- Ottimizzazione aggiornata: il nuovo livello IOPS è disponibile per le operazioni di scrittura del carico di lavoro. L'aggiornamento entra in uno stato di ottimizzazione Aggiornato, che in genere dura alcune ore, durante il quale le operazioni di lettura del carico di lavoro hanno prestazioni IOPS comprese tra il livello precedente e il nuovo livello. Una volta completata l'azione di aggiornamento, il nuovo livello IOPS è disponibile sia per la lettura che per la scrittura.
- Completato: l'aggiornamento IOPS dell'SSD è stato completato con successo.
- Non riuscito: l'aggiornamento IOPS dell'SSD non è riuscito. Scegli il punto interrogativo (?) per visualizzare i dettagli sul motivo per cui l'aggiornamento dello storage non è riuscito.

Progresso%

Visualizza l'avanzamento del processo di ottimizzazione dello storage come percentuale di completamento.

Orario della richiesta

L'ora in cui Amazon FSx ha ricevuto la richiesta di azione di aggiornamento.

Monitoraggio degli aggiornamenti con l'API AWS CLI and

È possibile visualizzare e monitorare le richieste di aggiornamento IOPS SSD del file system utilizzando il describe-file-systemsAWS CLIcomando e l'azione DescribeFileSystemsAPI. L'`AdministrativeActions`array elenca le 10 azioni di aggiornamento più recenti per ogni tipo di azione amministrativa. Quando si aumentano gli IOPS SSD di un file system,

ne `AdministrativeActions` vengono generate due: una `FILE_SYSTEM_UPDATE` e un'`IOPS_OPTIMIZATIONAzione`.

Gestione della capacità di throughput

Ogni file system FSx per Windows File Server ha una capacità di throughput che viene configurata al momento della creazione del file system. È possibile modificare la capacità di trasmissione del file system in qualsiasi momento, in base alle esigenze. La capacità di trasmissione è un fattore che determina la velocità con cui il file server che ospita il file system può gestire i dati dei file. I livelli più elevati di capacità di throughput comportano anche livelli più elevati di operazioni di I/O al secondo (IOPS) e più memoria per la memorizzazione nella cache dei dati sul file server. Per ulteriori informazioni, consulta Prestazioni di FSx for Windows File Server.

Quando modifichi la capacità di throughput del tuo file system, Amazon FSx disattiva il file server del file system dietro le quinte. Per i file system Multi-AZ, ciò comporta un failover e un failback automatici mentre Amazon FSx disattiva i file server preferiti e secondari. Per i sistemi Single-AZ, il file system non sarà disponibile per alcuni minuti durante la scalabilità della capacità di throughput. La nuova quantità di capacità di throughput viene fatturata una volta che questa sarà disponibile nel file system.

> **Note**
>
> Durante un'operazione di manutenzione sul back-end, le modifiche al sistema (come una modifica della capacità di produzione) potrebbero subire ritardi. La manutenzione può far sì che queste modifiche rimangano in coda fino alla prossima elaborazione.

Argomenti

- Quando modificare la capacità di produzione
- Come modificare la capacità di produzione
- Monitoraggio delle variazioni della capacità di produzione

Quando modificare la capacità di produzione

Amazon FSx si integra con AmazonCloudWatch, che consente di monitorare i livelli di utilizzo continuo del throughput del file system. Le prestazioni (throughput e IOPS) che è possibile gestire

tramite il file system dipendono dalle caratteristiche specifiche del carico di lavoro, oltre alla capacità di throughput, alla capacità di archiviazione e al tipo di storage del file system. Puoi usareCloudWatchmetriche per determinare quali di queste dimensioni modificare per migliorare le prestazioni. Per ulteriori informazioni, consulta Monitoraggio delle metriche con Amazon CloudWatch.

Per i file system Multi-AZ, la scalabilità della capacità di throughput comporta un failover e un failback automatici, mentre Amazon FSx disattiva i file server preferiti e secondari. Durante le sostituzioni dei file server, che si verificano durante la scalabilità della capacità di throughput, la manutenzione del file system e le interruzioni impreviste del servizio, il traffico in corso verso il file system verrà gestito dal file server rimanente. Quando il file server sostituito tornerà online, FSx for Windows eseguirà un processo di risincronizzazione per garantire che i dati vengano nuovamente sincronizzati con il file server appena sostituito.

FSx for Windows è progettato per ridurre al minimo l'impatto di questa attività di risincronizzazione su applicazioni e utenti. Tuttavia, il processo di risincronizzazione prevede la sincronizzazione dei dati in blocchi di grandi dimensioni. Ciò significa che un blocco di dati di grandi dimensioni può richiedere la sincronizzazione anche se viene aggiornata solo una piccola parte. Di conseguenza, la quantità di risincronizzazione dipende non solo dalla quantità di abbandono dei dati, ma anche dalla natura dell'abbandono dei dati nel file system. Se il carico di lavoro è gravoso in termini di scrittura e IOPS, il processo di sincronizzazione dei dati potrebbe richiedere più tempo e risorse prestazionali aggiuntive.

Il file system continuerà a essere disponibile durante questo periodo, ma per ridurre la durata della sincronizzazione dei dati, si consiglia di modificare la capacità di throughput durante i periodi di inattività in cui il carico sul file system è minimo. Si consiglia inoltre di verificare che il file system disponga di una capacità di throughput sufficiente per eseguire il processo di sincronizzazione in aggiunta al carico di lavoro, al fine di ridurre la durata della sincronizzazione dei dati. Infine, consigliamo di testare l'impatto dei failover quando il file system ha un carico inferiore.

Come modificare la capacità di produzione

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

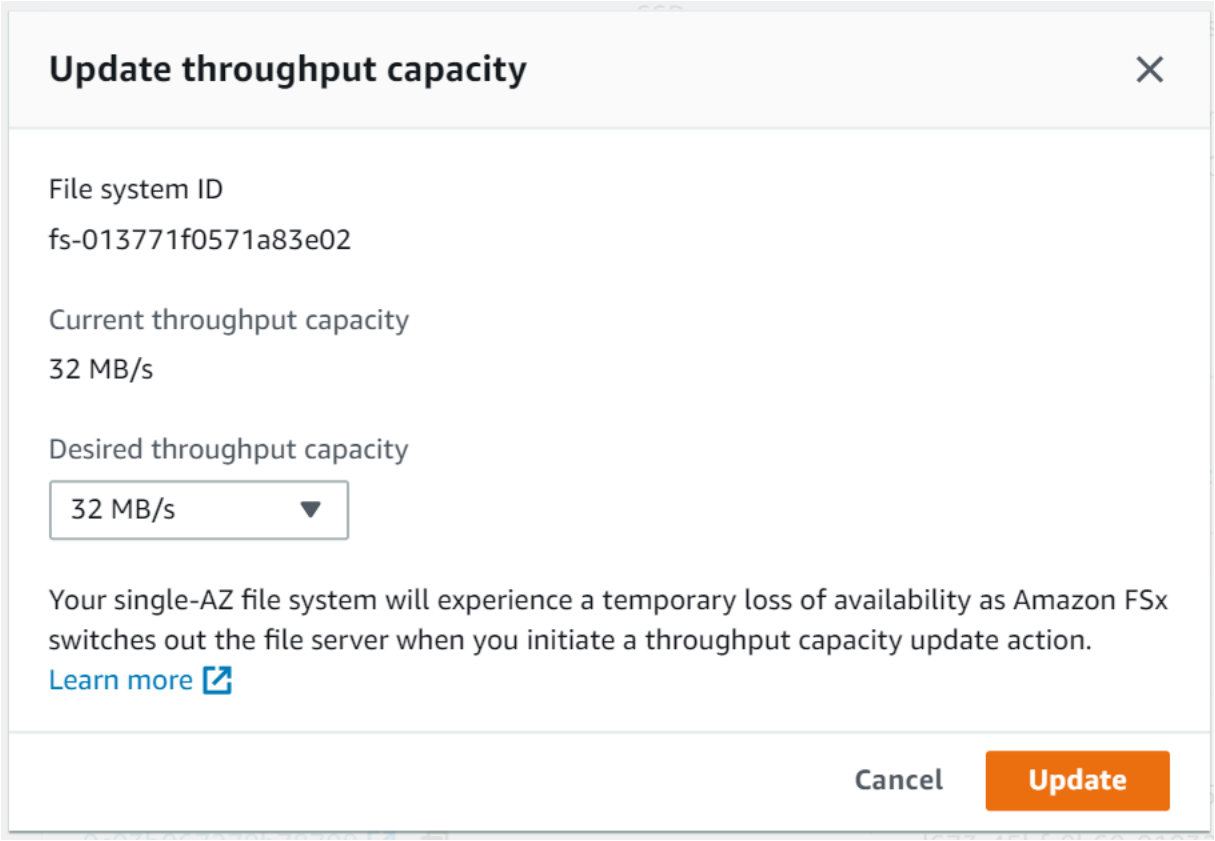
Per modificare la capacità di throughput di un file system (console)

1. Apri la console Amazon FSx all'indirizzohttps://console.aws.amazon.com/fsx/.
2. Naviga versoSistemi di filee scegli il file system di Windows per il quale desideri aumentare la capacità di throughput.

3. PerAzioni, scegliAggiorna la velocità effettiva. Oppure, nelRiepilogopannello, scegliAggiornamentoaccanto a quello del file systemCapacità di produzione.

   LaAggiorna la capacità di throughputviene visualizzata una finestra.

4. Scegli il nuovo valore perCapacità di produzionedall'elenco.



5. ScegliAggiornamentoper avviare l'aggiornamento della capacità di throughput.

> **Note**
>
> I file system Multi-AZ eseguono il failover e il failback durante l'aggiornamento della scalabilità della velocità effettiva e sono completamente disponibili. I file system Single-AZ presentano un brevissimo periodo di indisponibilità durante l'aggiornamento.

6. È possibile monitorare l'avanzamento dell'aggiornamento sulSistemi di filepagina di dettaglio, nellaAggiornamentilinguetta.

   Puoi monitorare l'avanzamento dell'aggiornamento utilizzando la console Amazon FSx,AWS CLIe l'API. Per ulteriori informazioni, consulta Monitoraggio delle variazioni della capacità di produzione.

Per modificare la capacità di throughput (CLI) di un file system

Per modificare la capacità di throughput di un file system, utilizzareAWS CLIcomandoupdate-file-system. Imposta i seguenti parametri:

- `--file-system-id`all'ID del file system che si sta aggiornando.
- `ThroughputCapacity`al valore desiderato a cui aggiornare il file system.

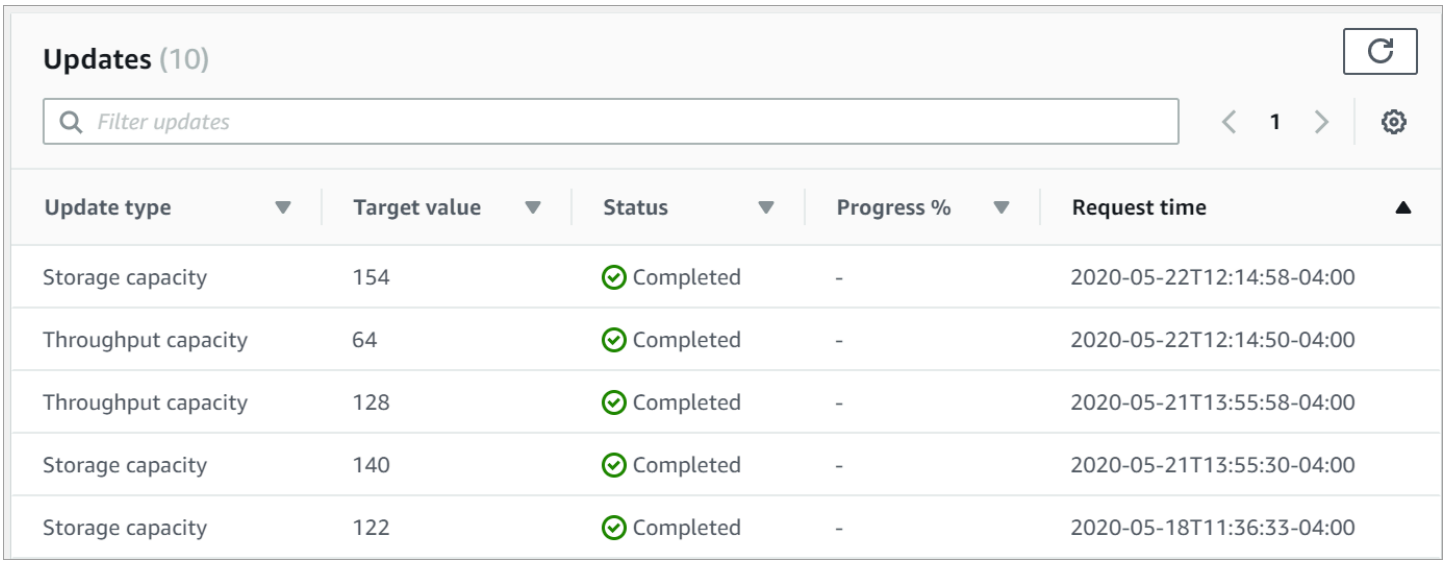
Puoi monitorare l'avanzamento dell'aggiornamento utilizzando la console Amazon FSx,AWS CLIe l'API. Per ulteriori informazioni, consulta Monitoraggio delle variazioni della capacità di produzione.

Monitoraggio delle variazioni della capacità di produzione

Puoi monitorare l'avanzamento di una modifica della capacità di throughput utilizzando la console Amazon FSx, l'API e ilAWS CLI.

Monitoraggio delle variazioni della capacità di throughput nella console

NelAggiornamentischeda nelDettagli del file systemfinestra, 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 trasmissione, è possibile visualizzare le seguenti informazioni.

Tipo di aggiornamento

Il valore possibile èCapacità di produzione.

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 trasmissione, 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.
- Ottimizzazione aggiornata— Amazon FSx ha aggiornato gli I/O di rete, la CPU e le risorse di memoria del file system. Il nuovo livello di prestazioni I/O del disco è disponibile per le operazioni di scrittura. Le operazioni di lettura determineranno le prestazioni di I/O del disco tra il livello precedente e il nuovo livello fino a quando il file system non sarà più in questo stato.
- Completato— L'aggiornamento della capacità di throughput è stato completato con successo.
- Fallito— L'aggiornamento della capacità di throughput non è riuscito. Scegli il punto interrogativo (?) per visualizzare i dettagli sul motivo per cui l'aggiornamento della velocità effettiva non è riuscito.

Orario della richiesta

L'ora in cui Amazon FSx ha ricevuto la richiesta di aggiornamento.

Monitoraggio delle modifiche conAWS CLIe API

È possibile visualizzare e monitorare le richieste di modifica della capacità effettiva del file system utilizzandodescribe-file-systemsComando CLI eDescribeFileSystemsAzione API. La`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,`FILE_SYSTEM_UPDATE`viene generata un'azione amministrativa.

L'esempio seguente mostra l'estratto della risposta di un`describe-file-systems`Comando CLI. Il file system ha una capacità di trasmissione di 8 MB/s e la capacità di throughput di destinazione di 256 MB/s.

```
.
.
```

```
.
    "ThroughputCapacity": 8,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Quando Amazon FSx completa l'elaborazione dell'azione con successo, lo stato cambia in`COMPLETED`. La nuova capacità di throughput è quindi disponibile per il file system e viene visualizzata nel`ThroughputCapacity`proprietà. Questo è mostrato nel seguente estratto di risposta di a`describe-file-systems`Comando CLI.

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Se la modifica della capacità di trasmissione fallisce, lo stato passa a`FAILED`, e`FailureDetails`la proprietà fornisce informazioni sull'errore. Per informazioni sulla risoluzione dei problemi relativi alle azioni non riuscite, vedereGli aggiornamenti della capacità di storage o di throughput falliscono.

Tagging delle risorse Amazon FSx

Per semplificare la gestione dei file system e altre risorse Amazon FSx, puoi assegnare metadati personalizzati a ciascuna risorsa sotto forma di tag. I tag consentono di categorizzare le tue risorse AWS in modi diversi, ad esempio, per scopo, proprietario o ambiente. Questa caratteristicaè molto utile quando hai tante risorse dello stesso tipo in quanto puoi rapidamente individuare una risorsa specifica in base ai tag assegnati. Questo argomento descrive i tag e mostra come crearli.

Argomenti

Nozioni di base sui tag

Un tag è un'etichetta che assegni a una risorsa AWS. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili.

I tag consentono di categorizzare le tue risorse AWS in modi diversi, ad esempio, per scopo, proprietario o ambiente. Ad esempio, puoi definire un set di tag per i file system Amazon FSx del tuo account e monitorare così ogni proprietario dell'istanza e il livello dello stack.

Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Tramite un set di chiavi di tag coerente la gestione delle risorse risulta notevolmente semplificata. Puoi cercare e filtrare le risorse in base ai tag aggiunti. Per ulteriori informazioni su come implementare una strategia efficace di applicazione di tag alle risorse, consulta il Whitepaper AWS denominato Best practice per l'applicazione di tag.

I tag non hanno alcun significato semantico per Amazon FSx e vengono interpretati rigorosamente come una stringa di caratteri. Inoltre, i tag non vengono assegnati automaticamente alle risorse. Puoi modificare chiavi e valori di tag e rimuovere tag da una risorsa in qualsiasi momento. Puoi impostare il valore di un tag su una stringa vuota, ma non su null. Se aggiungi un tag con la stessa chiave di un tag esistente a una risorsa specifica, il nuovo valore sovrascrive quello precedente. Se elimini una risorsa, verranno eliminati anche tutti i tag associati alla risorsa.

Se utilizzi l'API Amazon FSx,AWSCLI o unAWSSDK, puoi utilizzare`TagResource`Azione API per applicare tag alle risorse esistenti. Inoltre, alcune operazioni per la creazione di risorse ti consentono

di specificare tag per una risorsa durante la sua creazione. Se i tag non possono essere applicati durante la creazione della risorsa, eseguiamo il rollback del processo di creazione della risorsa. Ciò fa sì che le risorse vengano create con i tag oppure che non vengano create affatto, nonché che nessuna risorsa sia mai sprovvista di tag. Il tagging delle risorse in fase di creazione ti permette di evitare di eseguire script di tagging personalizzati dopo la creazione delle risorse. Per ulteriori informazioni sull'abilitazione agli utenti affinché possano aggiungere tag alle risorse durante la creazione, vedere Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.

Tagging delle risorse

Puoi assegnare tag alle risorse Amazon FSx esistenti nel tuo account. Se utilizzi la console Amazon FSx, puoi applicare tag alle risorse utilizzando la scheda Tags (Tag) nella schermata delle risorse pertinente. Quando crei risorse, puoi applicare la chiave Nome con un valore e puoi applicare i tag di tua scelta quando crei un nuovo file system. La console può organizzare le risorse in base al relativo tag Nome ma questo tag non ha un significato semantico per il servizio Amazon FSx.

Puoi applicare autorizzazioni basate su tag a livello di risorsa nelle policy IAM alle operazioni dell'API Amazon FSx che supportano il l'assegnazione di tag in fase di creazione per implementare un controllo granulare sugli utenti e sui gruppi che aggiungono tag alle risorse in fase di creazione. Le risorse vengono adeguatamente protette a partire dal momento della creazione, ovvero i tag vengono applicati subito alle risorse. Pertanto qualsiasi autorizzazione basata su tag a livello di risorsa che controlla l'uso delle risorse risulta immediatamente valida. Le risorse possono essere monitorate e segnalate con maggiore precisione. Puoi applicare l'uso del tagging alle nuove risorse e controllare quali chiavi e valori di tag sono impostati per le risorse.

Puoi inoltre applicare autorizzazioni a livello di risorsa alla`TagResource`e`UntagResource`Le operazioni dell'API Amazon FSx nelle policy IAM per controllare quali chiavi e valori di tag sono impostati sulle risorse esistenti.

Per ulteriori informazioni sul tagging delle risorse per la fatturazione, consulta Utilizzo di tag per l'allocazione dei costi nella Guida per l'utente di AWS Billing.

Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per risorsa: 50

- Per ciascuna risorsa, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.
- La lunghezza massima della chiave è 128 caratteri Unicode in formato UTF-8
- La lunghezza massima del valore è 256 caratteri Unicode in formato UTF-8
- I caratteri consentiti per i tag Amazon FSx sono: lettere, numeri e spazi rappresentabili in formato UTF-8 e i seguenti caratteri: + - =. _:/@.
- Per chiavi e valori di tag viene fatta la distinzione tra maiuscole e minuscole.
- Il prefisso `aws:` è riservato per l'uso di AWS. Se il tag ha una chiave di tag con questo prefisso, non puoi modificare o eliminare la chiave o il valore de tag. I tag con il prefisso `aws:` non vengono conteggiati per il limite del numero di tag per risorsa.

Non puoi eliminare una risorsa solo sulla base dei relativi tag ma devi specificare l'identificatore della risorsa. Ad esempio, per eliminare un file system che hai taggato con una chiave di tag denominata`DeleteMe`, devi utilizzare`DeleteFileSystem`azione con l'identificatore delle risorse del file system, come fs-1234567890abcdef0.

Quando si aggiungono tag a risorse pubbliche o condivise, i tag assegnati sono disponibili solo perAccount AWS; nessun altroAccount AWSavrà accesso a tali tag. Per il controllo degli accessi basato su tag alle risorse condivise, ciascunaAccount AWSdeve assegnare il proprio set di tag per controllare l'accesso alla risorsa.

Autorizzazioni e tag

Per ulteriori informazioni sulle autorizzazioni necessarie per assegnare tag alle risorse Amazon FSx in fase di 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 risorse Amazon FSx nelle policy IAM, consultaUtilizzo dei tag per controllare l'accesso alle risorse Amazon FSx.

Utilizzo delle finestre di manutenzione di Amazon FSx

Amazon FSx for Windows File Server esegue l'applicazione di patch di routine per il software Microsoft Windows Server che gestisce. La finestra di manutenzione consente di controllare il giorno e l'ora della settimana in cui vengono applicate le patch del software. La finestra di manutenzione viene scelta durante la creazione del file system. Se non hai preferenze di orario, viene assegnata una finestra predefinita di 30 minuti.

FSx for Windows File Server consente di modificare la finestra di manutenzione per adattarla al carico di lavoro e ai requisiti operativi. È possibile spostare la finestra di manutenzione con la frequenza necessaria, a condizione che sia programmata una finestra di manutenzione almeno una volta ogni 14 giorni. Se viene rilasciata una patch e non è stata pianificata una finestra di manutenzione entro 14 giorni, FSx for Windows File Server procede alla manutenzione del file system per garantirne la sicurezza e l'affidabilità.

Mentre l'applicazione delle patch è in corso, aspettatevi che i file system Single-AZ non siano disponibili, in genere per meno di 20 minuti. I file system Multi-AZ rimangono disponibili e consentono di eseguire automaticamente il failover e il failback tra il file server preferito e il file server di standby. Per ulteriori informazioni, consulta Processo di failover per FSx for Windows File Server. Poiché l'applicazione di patch per i file system Multi-AZ comporta failover e failback, tutto il traffico verso il file system durante questo periodo deve essere sincronizzato tra il file server preferito e il file server di standby. Per ridurre i tempi di applicazione delle patch, ti consigliamo di pianificare la finestra di manutenzione durante i periodi di inattività, quando il carico sul file system è minimo.

> **Note**
>
> Per garantire l'integrità dei dati durante le attività di manutenzione, Amazon FSx for Windows File Server completa tutte le operazioni di scrittura in sospeso sui volumi di storage sottostanti che ospitano il file system prima dell'inizio della manutenzione.

Puoi usare la Console di gestione Amazon FSx,AWS CLI,AWSAPI o una delleAWSSDK per modificare la finestra di manutenzione dei file system.

Per modificare la finestra di manutenzione settimanale (console)

1. Apri la console Amazon FSx all'indirizzohttps://console.aws.amazon.com/fsx/.
2. ScegliSistemi di filenella colonna di navigazione a sinistra.
3. Scegli il file system per il quale desideri modificare la finestra di manutenzione settimanale. Viene visualizzata la pagina dei dettagli del file system.
4. ScegliAmministrazioneper visualizzare l'amministrazione del file systemImpostazionipannello.
5. ScegliAggiornamentoper visualizzareCambia finestra di manutenzionefinestra.
6. Inserisci il nuovo giorno e la nuova ora in cui desideri che inizi la finestra di manutenzione settimanale.

7. Scegliere Save (Salva) per salvare le modifiche. La nuova ora di inizio della manutenzione viene visualizzata nelImpostazioni di amministrazionepannello.

Per modificare la finestra di manutenzione settimanale utilizzandoupdate-file-systemComando CLI, vediProcedura passo per passo Aggiornare un file system esistente.

Best practice per l'amministrazione dei file system Amazon FSx

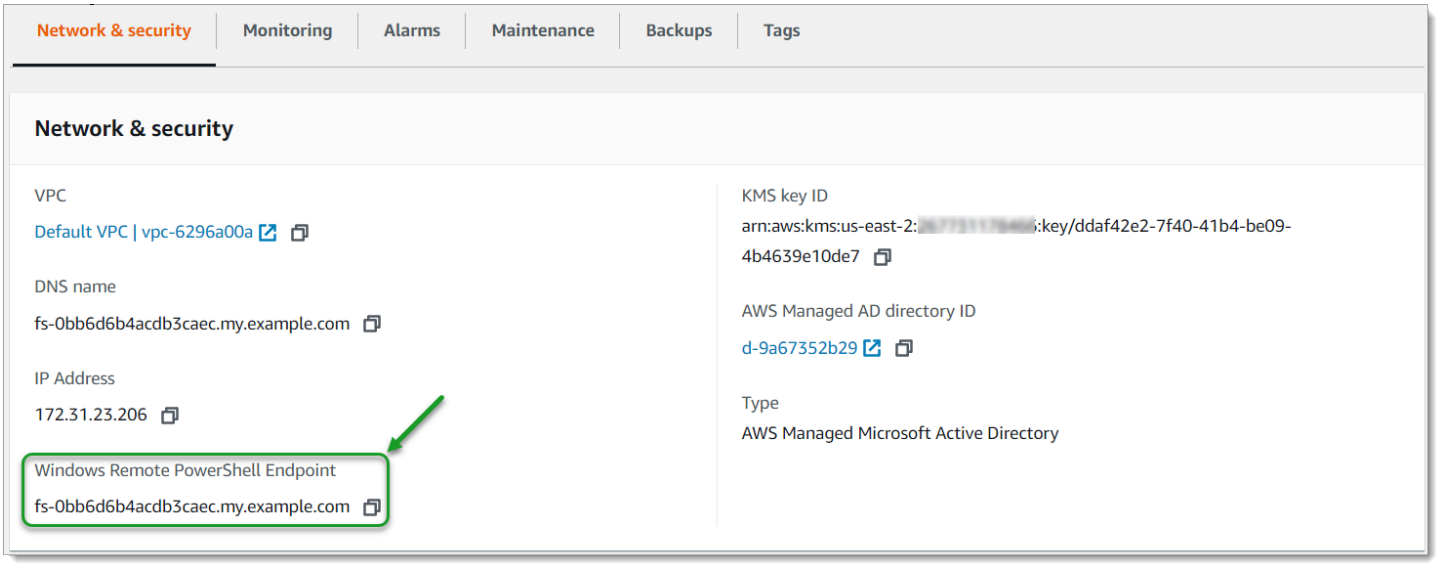
Amazon FSx offre diverse funzionalità che possono aiutarti a implementare le migliori pratiche per l'amministrazione dei tuoi file system, tra cui:

- ottimizzazione del consumo di storage
- consentire agli utenti finali di ripristinare file e cartelle nelle versioni precedenti
- applicazione della crittografia per tutti i client connessi

Utilizza la seguente CLI di Amazon FSx per la gestione remota sui PowerShell comandi per implementare rapidamente queste best practice sui tuoi file system.

Per eseguire questi comandi, devi conoscere il Windows Remote PowerShell Endpoint per il tuo file system. Per trovare questo endpoint, procedi nel seguente modo:

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Scegli il tuo file system. Nella scheda Rete e sicurezza, individua Windows Remote PowerShell Endpoint, come illustrato di seguito.



Per ulteriori informazioni, consulta Amministrazione dei file system e Utilizzo dell'interfaccia a riga di comando di Amazon FSx per PowerShell.

Argomenti

- Attività di configurazione amministrativa una tantum
- Attività amministrative continue per monitorare il file system

Attività di configurazione amministrativa una tantum

Di seguito sono elencate le attività che è possibile configurare rapidamente una sola volta per il file system.

Gestione del consumo di storage

Utilizza i seguenti comandi per gestire il consumo di storage del file system.

- Per attivare la deduplicazione dei dati con la pianificazione predefinita, esegui il comando seguente.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FsxDedup }
```

  Facoltativamente, utilizzate il seguente comando per attivare la deduplicazione dei dati sui file subito dopo la creazione di un file, senza richiedere alcuna età minima per i file.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FSxDedupConfiguration -MinimumFileAgeDays 0 }
```

Per ulteriori informazioni, consulta Deduplicazione dei dati.

- Utilizzate il comando seguente per attivare le quote di archiviazione degli utenti in modalità «Track», che serve solo a scopo di reporting e non a scopo di imposizione.

```
$QuotaLimit = Quota limit in bytes
$QuotaWarningLimit = Quota warning threshold in bytes
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FSxUserQuotas -Track -DefaultLimit
 $Using:QuotaLimit -DefaultWarningLimit $Using:QuotaWarningLimit }
```

Per ulteriori informazioni, consulta Quote di archiviazione.

Attivazione delle copie shadow per consentire agli utenti finali di ripristinare file e cartelle nelle versioni precedenti

Attiva le copie shadow con la pianificazione predefinita (nei giorni feriali 7:00 e 12:00), come segue.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowStorage -Default }

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowCopySchedule -Default -Confirm:$False}
```

Per ulteriori informazioni, consulta Configurazione delle copie shadow per utilizzare l'archiviazione e la pianificazione predefinite.

Applicazione della crittografia in transito

Il comando seguente impone la crittografia per i client che si connettono al file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxSmbServerConfiguration -EncryptData $True -
RejectUnencryptedAccess $True -Confirm:$False}
```

È possibile chiudere tutte le sessioni aperte e forzare i client attualmente connessi a riconnettersi utilizzando la crittografia.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbSession -Confirm:$False}
```

Per ulteriori informazioni, consulta Gestione della crittografia in transito e Sessioni utente e file aperti.

Attività amministrative continue per monitorare il file system

Le seguenti attività continue consentono di monitorare l'utilizzo del disco del file system, le quote degli utenti e i file aperti.

Monitoraggio dello stato della deduplicazione

Monitora lo stato della deduplicazione, incluso il tasso di risparmio ottenuto sul file system, come segue.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FsxRemoteAdmin -ScriptBlock { Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate
```

Monitoraggio del consumo di storage a livello di utente

Ottieni un rapporto sulle attuali quote di spazio di archiviazione degli utenti, incluso quanto spazio stanno consumando e se stanno violando il limite e la soglia di avviso.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxUserQuotaEntries }
```

Monitoraggio e chiusura dei file aperti

Gestisci i file aperti cercando i file lasciati aperti e chiudendoli. Usa il seguente comando per verificare la presenza di file aperti.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxSmbOpenFile}
```

Utilizzate il seguente comando per chiudere i file aperti.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbOpenFile -Confirm:$false}
```

Raggruppamento di più file system con namespace DFS

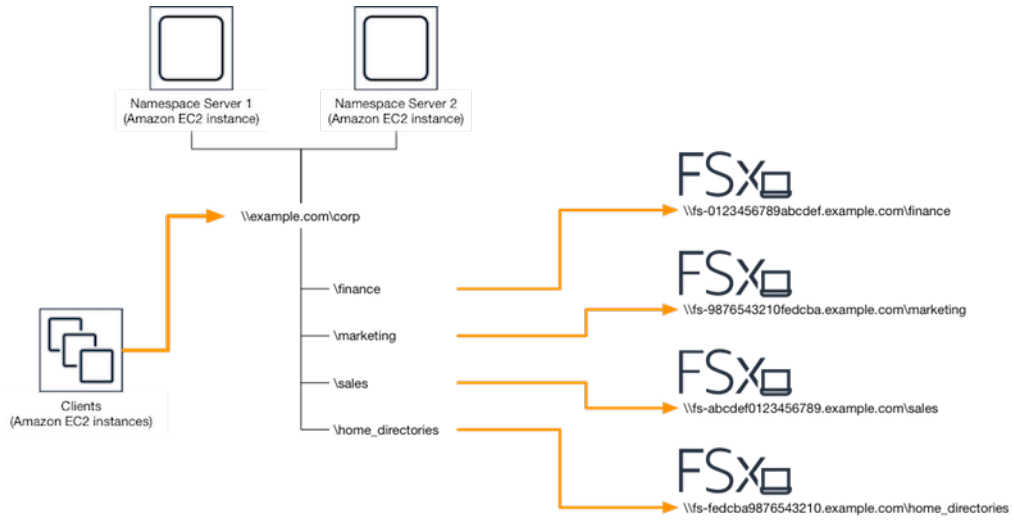
Amazon FSx for Windows File Server supporta l'uso dei namespace DFS (Distributed File System) di Microsoft. Puoi utilizzare i namespace DFS per raggruppare le condivisioni di file su più file system in un'unica struttura di cartelle comune (uno spazio dei nomi) da utilizzare per accedere all'intero set di dati di file. I namespace DFS possono aiutarti a organizzare e unificare l'accesso alle tue condivisioni di file su più file system. I namespace DFS possono anche aiutare a scalare lo storage dei dati di file oltre quello supportato da ciascun file system (64 TB) per set di dati di file di grandi dimensioni, fino a centinaia di petabyte.

Configurazione dei namespace DFS per il raggruppamento di più file system

È possibile utilizzare i namespace DFS per raggruppare più file system in un unico spazio dei nomi. Nell'esempio che segue, lo spazio dei nomi basato sul dominio (example.com\ corp) viene creato su due server dello spazio dei nomi, consolidando le condivisioni di file archiviate su più file system Amazon FSx (finance, marketing, sales, home_directories). Ciò consente agli utenti di accedere alle condivisioni di file utilizzando uno spazio dei nomi comune. Ciò premesso, non è necessario specificare i nomi DNS del file system per ciascuno dei file system che ospitano le condivisioni di file.

> **Note**
>
> Amazon FSx non può essere aggiunto alla radice del percorso di condivisione DFS.

Questi passaggi ti guidano nella creazione di un singolo namespace (example.com\ corp) su due server di namespace. Puoi anche configurare quattro condivisioni di file nello spazio dei nomi, ognuna delle quali reindirizza in modo trasparente gli utenti alle condivisioni ospitate su file system Amazon FSx separati.



Per raggruppare più file system in un namespace DFS comune

1. Se non disponi già di server DFS Namespace in esecuzione, puoi avviare un paio di server DFS Namespace ad alta disponibilità utilizzando il modello Setup-DFSN-Servers.template. AWS CloudFormation Per ulteriori informazioni sulla creazione di uno stack, consulta la sezione Creazione di uno stack sulla console nella Guida per l'utente. AWS CloudFormation AWS CloudFormation AWS CloudFormation
2. Connect a uno dei server DFS Namespace avviati nel passaggio precedente come utente del gruppo AWS Delegated Administrators. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
3. Accedi alla console di gestione DFS aprendo. Apri il menu Start ed esegui dfsmgmt.msc. Si apre lo strumento GUI di gestione DFS.
4. Scegli Azione, quindi Nuovo spazio dei nomi, digita il nome del computer del primo server DFS Namespace che hai avviato per Server e scegli Avanti.
5. Per Nome, digita lo spazio dei nomi che stai creando (ad esempio, corp).
6. Scegli Modifica impostazioni e imposta le autorizzazioni appropriate in base alle tue esigenze. Seleziona Successivo.
7. Lasciate selezionata l'opzione predefinita dello spazio dei nomi basato sul dominio, lasciate selezionata l'opzione Abilita la modalità Windows Server 2008 e scegliete Avanti.

> **Note**
>
> La modalità Windows Server 2008 è l'ultima opzione disponibile per i namespace.

8. Controlla le impostazioni del namespace e scegli Crea.
9. Con lo spazio dei nomi appena creato selezionato in Namespace nella barra di navigazione, scegli Azione, quindi Aggiungi server dello spazio dei nomi.
10. Digita il nome del computer del secondo server DFS Namespace che hai avviato per il server Namespace.
11. Scegliete Modifica impostazioni, impostate le autorizzazioni appropriate in base ai vostri requisiti e scegliete OK.
12. Apri il menu contestuale (fai clic con il pulsante destro del mouse) per lo spazio dei nomi che hai appena creato, scegli Nuova cartella, digita il nome della cartella (ad **`finance`** esempio, Nome) e scegli OK.
13. Digitate il nome DNS della condivisione di file a cui desiderate far puntare la cartella DFS Namespace in formato UNC (ad esempio,**`\\fs-0123456789abcdef0.example.com\finance`**) per Path to folder target e scegliete OK.
14. Se la condivisione non esiste:
    a. Scegli Sì per crearla.
    b. Nella finestra di dialogo Crea condivisione, scegli Sfoglia.
    c. Scegliete una cartella esistente o create una nuova cartella in D$ e scegliete OK.
    d. Imposta le autorizzazioni di condivisione appropriate e scegli OK.
15. Nella finestra di dialogo Nuova cartella, scegliete OK. La nuova cartella verrà creata nello spazio dei nomi.
16. Ripeti gli ultimi quattro passaggi per le altre cartelle che desideri condividere con lo stesso namespace.

Monitoraggio di FSx per Windows File Server

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon FSx e delle tue AWS soluzioni. È necessario raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un errore multipunto, se si verifica. Tuttavia, prima di iniziare a monitorare Amazon FSx, è necessario creare un piano di monitoraggio che includa le risposte alle seguenti domande:

- Quali sono gli obiettivi del monitoraggio?
- Di quali risorse si intende eseguire il monitoraggio?
- Con quale frequenza sarà eseguito il monitoraggio di queste risorse?
- Quali strumenti di monitoraggio verranno utilizzati?
- Chi eseguirà i processi di monitoraggio?
- Chi deve ricevere una notifica quando si verifica un problema?

Per ulteriori informazioni sulla registrazione e il monitoraggio in FSx for Windows File Server, vedere i seguenti argomenti.

Argomenti

Strumenti di monitoraggio

AWS fornisce diversi strumenti che puoi utilizzare per monitorare Amazon FSx. Puoi configurare alcuni di questi strumenti in modo che eseguano il monitoraggio al posto tuo, mentre altri richiedono un intervento manuale. Si consiglia di automatizzare il più possibile i processi di monitoraggio.

Strumenti di monitoraggio automatici

Puoi utilizzare i seguenti strumenti di monitoraggio automatizzato per guardare Amazon FSx e segnalare quando qualcosa non va:

- Amazon CloudWatch Alarms: monitora una singola metrica in un periodo di tempo specificato ed esegui una o più azioni in base al valore della metrica rispetto a una determinata soglia in diversi periodi di tempo. L'azione è una notifica inviata a un argomento di Amazon Simple Notification Service (Amazon SNS) o a una policy di Amazon EC2 Auto Scaling. CloudWatch gli allarmi non richiamano azioni semplicemente perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi. Per ulteriori informazioni, consulta Monitoraggio delle metriche con Amazon CloudWatch.
- Amazon CloudWatch Logs: monitora, archivia e accedi ai tuoi file di registro da AWS CloudTrail o altre fonti. Per ulteriori informazioni, consulta What Is Amazon CloudWatch Logs? nella Amazon CloudWatch Logs User Guide.
- AWS CloudTrail Monitoraggio dei log: condividi file di log tra account, monitora i file di CloudTrail log in tempo reale inviandoli a CloudWatch Logs, scrivi applicazioni di elaborazione dei log in Java e verifica che i file di log non siano cambiati dopo la consegna da parte di. CloudTrail Per ulteriori informazioni, consulta Lavorare con i file di CloudTrail registro nella Guida per l'AWS CloudTrail utente.

Strumenti di monitoraggio manuali

Un'altra parte importante del monitoraggio di Amazon FSx consiste nel monitorare manualmente gli elementi che gli CloudWatch allarmi di Amazon non coprono. Amazon FSx e altre dashboard AWS della console forniscono una at-a-glance visione dello stato del tuo ambiente. CloudWatch AWS

I dashboard di monitoraggio e prestazioni della console Amazon FSx mostrano:

- CloudWatch Avvisi e allarmi attuali di FSx for Windows File Server
- Grafici che mostrano un riepilogo dell'attività del file system
- Grafici della capacità e dell'utilizzo dello storage del file system
- Grafici delle prestazioni dei file server e dei volumi di storage
- CloudWatch allarmi

La CloudWatch home page mostra:

- Stato e allarmi attuali
- Grafici degli allarmi e delle risorse
- Stato di integrità dei servizi

Inoltre, è possibile utilizzare CloudWatch per effettuare le seguenti operazioni:

- Crea dashboard personalizzate per monitorare i servizi che utilizzi.
- Crea grafici dei dati dei parametri per la risoluzione di problemi e il rilevamento di tendenze.
- Cerca e sfoglia tutte le metriche AWS delle tue risorse.
- Crea e modifica gli allarmi per ricevere le notifiche dei problemi.

Per ulteriori informazioni sul dashboard di monitoraggio e prestazioni di Amazon FSx, consulta. Come utilizzare le metriche di FSx for Windows File Server

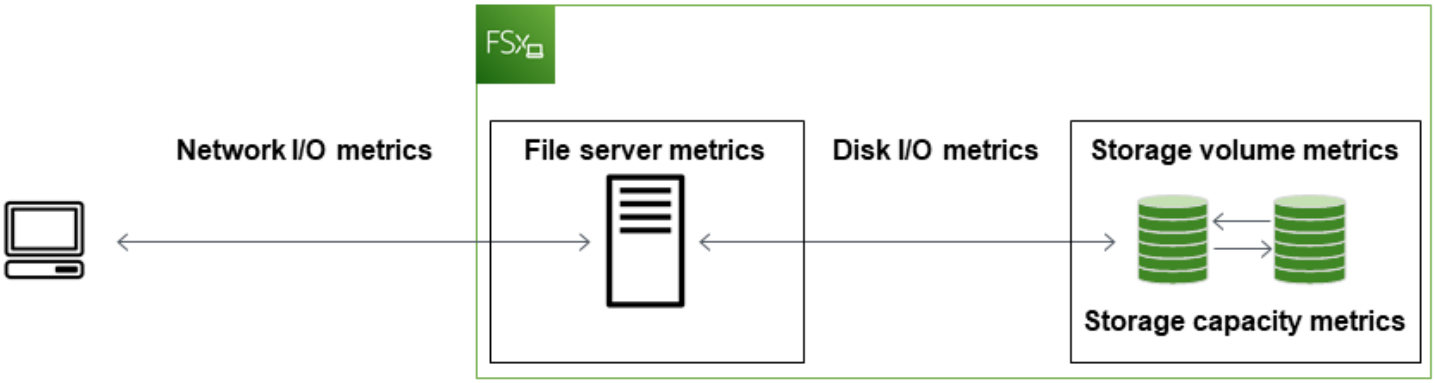
Monitoraggio delle metriche con Amazon CloudWatch

Puoi monitorare i file system FSx for Windows File Server utilizzando CloudWatch Amazon, che raccoglie ed elabora i dati grezzi da FSx for Windows File Server in metriche leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, in modo da poter accedere alle informazioni storiche e acquisire prospettive sulle prestazioni dell'applicazione Web o del file system.

FSx for Windows File Server CloudWatch pubblica metriche nei seguenti domini:

- Le metriche di I/O di rete misurano l'attività tra i client che accedono al file system e al file server.
- Le metriche dei file server misurano l'utilizzo del throughput di rete, la CPU e la memoria del file server, la velocità effettiva del disco del file server e l'utilizzo degli IOPS.
- Le metriche di I/O del disco misurano l'attività tra il file server e i volumi di storage.
- Le metriche del volume di archiviazione misurano l'utilizzo della velocità effettiva del disco per i volumi di archiviazione HDD e l'utilizzo degli IOPS per i volumi di archiviazione SSD.
- I parametri della capacità di storage misurano l'utilizzo dello storage, compresi i risparmi di storage dovuti alla deduplicazione dei dati.

Il diagramma seguente illustra un file system FSx for Windows File Server, i relativi componenti e i domini metrici.



Per impostazione predefinita, Amazon FSx for Windows File Server invia dati metrici CloudWatch a periodi di 1 minuto, con le seguenti eccezioni che vengono emesse a intervalli di 5 minuti:

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

Per ulteriori informazioni su CloudWatch, consulta What is Amazon CloudWatch? nella Amazon CloudWatch User Guide.

Le metriche potrebbero non essere pubblicate per i sistemi di file Single-AZ durante la manutenzione dei file system o la sostituzione dei componenti dell'infrastruttura e per i file system Multi-AZ durante il failover e il failback tra i file server primari e secondari.

Alcune CloudWatch metriche di Amazon FSx sono riportate come byte non elaborati. I byte non sono arrotondati a un multiplo decimale o binario dell'unità.

Argomenti

Parametri e dimensioni

FSx for Windows File Server pubblica le seguenti metriche nel `AWS/FSx` namespace di Amazon CloudWatch per tutti i file system:

- `DataReadBytes`
- `DataWriteBytes`
- `DataReadOperations`
- `DataWriteOperations`
- `MetadataOperations`
- `FreeStorageCapacity`

FSx for Windows File Server pubblica le metriche descritte di seguito nello `AWS/FSx` spazio dei nomi di CloudWatch Amazon per i file system configurati con una capacità di throughput di almeno 32 MBps.

Argomenti

Metriche di I/O di rete FSx per Windows

Il `AWS/FSx` namespace include le seguenti metriche di I/O di rete.

Parametro	Descrizione
`DataReadBytes`	Il numero di byte per le operazioni di lettura per i client che accedono al file system. Unità: byte Statistiche valide: `Sum`
`DataWriteBytes`	Il numero di byte per le operazioni di scrittura per i client che accedono al file system. Unità: byte

Parametro	Descrizione
	Statistiche valide: `Sum`
`DataReadOperations`	Il numero di operazioni di lettura per i client che accedono al file system. Unità: numero Statistiche valide: `Sum`
`DataWriteOperations`	Il numero di operazioni di scrittura per i client che accedono al file system. Unità: numero Statistiche valide: `Sum`
`MetadataOperations`	Il numero di operazioni sui metadati per i client che accedono al file system. Unità: numero Statistiche valide: `Sum`
`ClientConnections`	Il numero di connessioni attive tra i client e il file server. Unità: numero

Metriche dei file server FSx per Windows

Il `AWS/FSx` namespace include le seguenti metriche del file server.

Parametro	Descrizione
`NetworkThroughputUtilization`	Il throughput di rete per i client che accedono al file system, come percentuale del limite fornito. Unità: percentuale
`CPUUtilization`	La percentuale di utilizzo delle risorse CPU del file server.

Parametro	Descrizione
	Unità: percentuale
`MemoryUtilization`	La percentuale di utilizzo delle risorse di memoria del file server. Unità: percentuale
`FileServerDiskThroughputUtilization`	La velocità effettiva del disco tra il file server e i relativi volumi di archiviazione, come percentuale del limite assegnato determinato dalla capacità di throughput. Unità: percentuale
`FileServerDiskThroughputBalance`	La percentuale di crediti burst disponibili per la velocità effettiva del disco tra il file server e i relativi volumi di archiviazione. Valido per i file system dotati di una capacità di throughput pari o inferiore a 256 MBps. Unità: percentuale
`FileServerDiskIopsUtilization`	Gli IOPS del disco tra il file server e i volumi di storage, come percentuale del limite fornito determinato dalla capacità di throughput. Unità: percentuale
`FileServerDiskIopsBalance`	La percentuale di crediti burst disponibili per gli IOPS del disco tra il file server e i relativi volumi di storage. Valido per i file system dotati di una capacità di throughput pari o inferiore a 256 MBps. Unità: percentuale

Metriche di I/O su disco FSx per Windows

Lo spazio dei `AWS/FSx` nomi include le seguenti metriche di I/O del disco.

Parametro	Descrizione
`DiskReadBytes`	Il numero di byte per le operazioni di lettura che accedono ai volumi di archiviazione. Unità: byte Statistiche valide: somma
`DiskWriteBytes`	Il numero di byte per le operazioni di scrittura che accedono ai volumi di archiviazione. Unità: byte Statistiche valide: somma
`DiskReadOperations`	Il numero di operazioni di lettura per il file server che accede ai volumi di storage. Unità: numero Statistiche valide: `Sum`
`DiskWriteOperations`	Il numero di operazioni di scrittura per il file server che accede ai volumi di storage. Unità: numero Statistiche valide: `Sum`

Metriche del volume di archiviazione FSx per Windows

Il `AWS/FSx` namespace include le seguenti metriche del volume di archiviazione.

Parametro	Descrizione
`DiskThroughputUtilization`	(Solo HDD) La velocità effettiva del disco tra il file server e i relativi volumi di archiviazione, come percentuale del limite fornito determinato dai volumi di archiviazione.

Parametro	Descrizione
	Unità: percentuale
`DiskThroughputBalance`	(Solo HDD) La percentuale di crediti burst disponibili per la velocità effettiva del disco per i volumi di archiviazione. Unità: percentuale
`DiskIopsUtilization`	(Solo SSD) Gli IOPS del disco tra il server di file e i volumi di storage, come percentuale del limite di IOPS assegnato determinato dai volumi di storage. Unità: percentuale

Metriche della capacità di archiviazione FSx per Windows

Il `AWS/FSx` namespace include i seguenti parametri della capacità di archiviazione.

Parametro	Descrizione
`FreeStorageCapacity`	La quantità di capacità di archiviazione disponibile. Unità: byte Statistiche valide: `Average`, `Minimum`
`StorageCapacityUtilization`	Capacità di archiviazione fisica utilizzata come percentua le della capacità di archiviazione totale. Unità: percentuale
`DeduplicationSavedStorage`	La quantità di spazio di archiviazione risparmiata dalla deduplicazione dei dati, se abilitata. Unità: byte

Dimensioni FSx per Windows

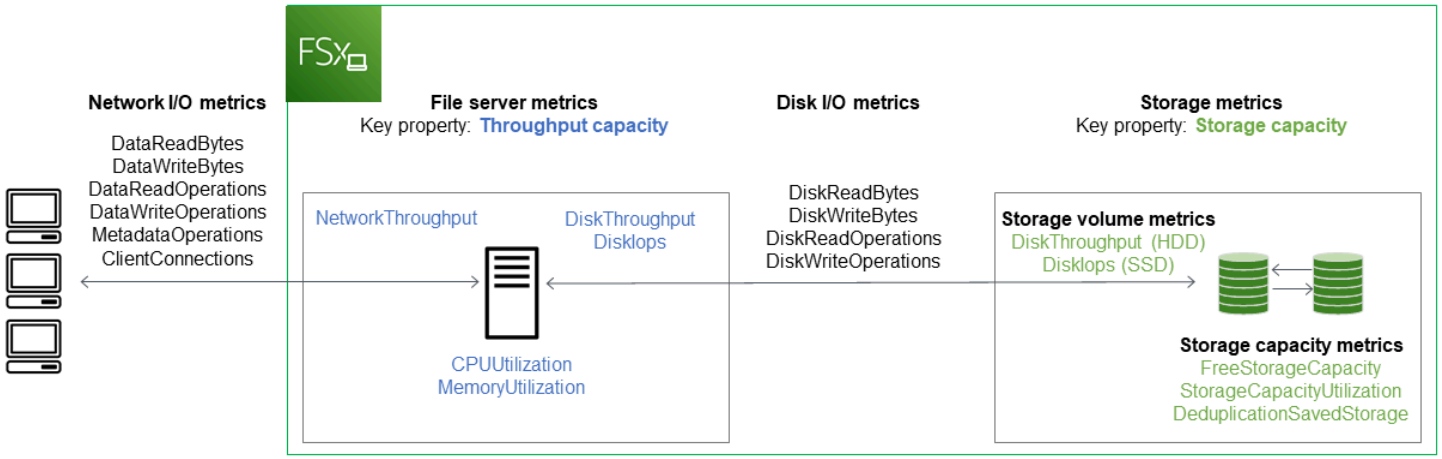
Le metriche di FSx for Windows File Server utilizzano `FSx` lo spazio dei nomi e forniscono metriche per una singola dimensione,. `FileSystemId` È possibile trovare l'ID di un file system utilizzando il comando o il describe-file-systems AWS CLI comando API. DescribeFileSystems Un ID del file system assume la forma di *`fs-0123456789abcdef0`*.

Come utilizzare le metriche di FSx for Windows File Server

Esistono due componenti architetturali principali di ogni file system Amazon FSx:

- Il file server che fornisce i dati ai client che accedono al file system.
- I volumi di storage che ospitano i dati nel file system.

FSx for Windows File Server riporta metriche CloudWatch che tengono traccia delle prestazioni e dell'utilizzo delle risorse per il file server e i volumi di storage del file system. Il diagramma seguente illustra un file system Amazon FSx con i suoi componenti architettonici e i CloudWatch parametri di prestazioni e risorse disponibili per il monitoraggio. La proprietà chiave mostrata per un set di parametri è la proprietà del file system che determina la capacità di tali parametri. La regolazione di tale proprietà modifica le prestazioni del file system per quel set di metriche.



Utilizza il pannello Monitoraggio e prestazioni nella console Amazon FSx per visualizzare i parametri di FSx for Windows File CloudWatch Server descritti nella tabella seguente.

Pannello di monitoraggio e prestazioni	Come posso...	Grafico	Parametri rilevanti
Riepilogo	... determinare gli IOPS totali del mio file system?	IOPS totali	SUM (`DataReadOperations + DataWriteOperations +MetadataOperations`) /Periodo (in secondi)
	... determinare la velocità effettiva totale del mio file system?	Throughput totale	SUM (`DataReadBytes +DataWriteBytes`) /Periodo (in secondi)
	... determinare la quantità di capacità di storage disponibile sul mio file system?	Capacità di archiviazione disponibile	`FreeStorageCapacity`
	... determinare il numero di connessioni stabilite tra i client e il file server?	Connessioni client	`ClientConnections`
Storage	... determinare la quantità di spazio fisico su disco utilizzato come percentuale della capacità di archiviazione totale del file system?	Utilizzo della capacità di archiviazione	`StorageCapacityUtilization`
	... determinare la quantità di spazio fisico su disco risparmiata dalla deduplicazione dei dati?	Archiviazione salvata	`DeduplicationSavedStorage`

Pannello di monitoraggio e prestazioni	Come posso...	Grafico	Parametri rilevanti
		dalla deduplicazione dei dati	
Prestazioni: file server	... determinare il throughput di rete per i client che accedono al file system, come percentuale del throughput assegnato al file system?	Utilizzo del throughput di rete	`NetworkThroughputUtilization`
	... determinare la velocità effettiva del disco tra il file server e i relativi volumi di storage, come percentuale del limite fornito determinato dalla capacità di throughput?	Utilizzo della velocità effettiva del disco	`FileServerDiskThroughputUtilization`
	... determinare la percentuale di crediti burst disponibili per la velocità effettiva del disco tra il file server e i relativi volumi di storage?	Throughput del disco (burst balance)	`FileServerDiskThroughputBalance`
	... determinare la quantità di IOPS del disco tra il file server e i volumi di storage, come percentuale del limite assegnato determinato dalla capacità di throughput?	Utilizzo degli IOPS del disco	`FileServerDiskIopsUtilization`

Pannello di monitoraggio e prestazioni	Come posso...	Grafico	Parametri rilevanti
	... determinare la percentuale di crediti burst disponibili per gli IOPS del disco tra il file server e i volumi di storage?	Bilanciamento del burst IOPS del disco	`FileServerDiskIopsBalance`
	... determinare la percentuale di utilizzo della CPU del file server?	Utilizzo CPU	`CPUUtilization`
	... determinare la percentuale di utilizzo della memoria del file server?	Utilizzo della memoria	`MemoryUtilization`
Prestazioni: volumi di archiviazione	... determinare la velocità effettiva per le operazioni che accedono ai volumi di storage, come percentuale del limite previsto determinato dalla capacità di storage dell'HDD?	Utilizzo della velocità effettiva del disco (HDD)	`DiskThroughputUtilization`
	... determinare la percentuale di crediti burst disponibili per la velocità effettiva per le operazioni che accedono ai volumi di storage degli HDD?	Throughput burst balance (HDD) del disco	`DiskThroughputBalance`
	... determinare gli IOPS per le operazioni che accedono ai volumi di storage, come percentuale del limite previsto determinato dalla capacità di archiviazione SSD?	Utilizzo degli IOPS del disco (SSD)	`DiskIopsUtilization`

> **Note**
>
> Si consiglia di mantenere un utilizzo medio della capacità di throughput inferiore al 50% per garantire una capacità di throughput sufficiente in caso di picchi imprevisti del carico di lavoro e per qualsiasi operazione di storage Windows in background (come sincronizzazione dello storage, deduplicazione o copie shadow).

Avvertenze e consigli sulle prestazioni

FSx for Windows fornisce avvisi sulle prestazioni per i file system configurati con una capacità di throughput di almeno 32 MBps. Amazon FSx visualizza un avviso per una serie di CloudWatch parametri ogni volta che uno di questi parametri ha raggiunto o superato una soglia predeterminata per più punti dati consecutivi. Questi avvisi forniscono consigli pratici che puoi utilizzare per ottimizzare le prestazioni del tuo file system.

Gli avvisi sono accessibili in diverse aree del pannello di controllo Monitoraggio e prestazioni. Tutti gli avvisi sulle prestazioni di Amazon FSx attivi o recenti e tutti gli CloudWatch allarmi configurati per il file system che si trovano in uno stato ALARM vengono visualizzati nel pannello Monitoraggio e prestazioni nella sezione Riepilogo. L'avviso appare anche nella sezione del pannello di controllo in cui viene visualizzato il grafico metrico.

Puoi creare CloudWatch allarmi per qualsiasi metrica di Amazon FSx. Per ulteriori informazioni, consulta Creazione di CloudWatch allarmi 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.

Se è presente un avviso per questa metrica	Esegui questa operazione
Throughput di rete: utilizzo	Aumentare la capacità di throughput
File server > Disk IOPS: utilizzo	

Se è presente un avviso per questa metrica	Esegui questa operazione
File server > Throughput del disco: utilizzo	
File server > IOPS del disco: burst balance	
File server > Velocità effettiva del disco: bilanciamento del burst	
Utilizzo della capacità di storage	Aumentare la capacità di archiviazione
Volume di archiviazione > Velocità effettiva e utilizzo del disco (HDD)	Aumenta la capacità di archiviazione o passa al tipo di storage SDD
Volume di archiviazione > Velocità effettiva del disco — burst balance (HDD)	
Volume di archiviazione > IOPS del disco: utilizzo (SSD)	Aumentare gli IOPS SSD

> **Note**
>
> Alcuni eventi del file system possono consumare le risorse prestazionali di I/O del disco e potenzialmente attivare avvisi sulle prestazioni. Per esempio:
>
> - La fase di ottimizzazione della scalabilità della capacità di archiviazione può generare un aumento della velocità effettiva del disco, come descritto in Aumento della capacità di storage e delle prestazioni del file system
> - Per i file system Multi-AZ, eventi quali la scalabilità della capacità di throughput, la sostituzione dell'hardware o l'interruzione della zona di disponibilità determinano eventi automatici di failover e failback. Tutte le modifiche ai dati che si verificano durante questo periodo devono essere sincronizzate tra i file server primari e secondari e Windows Server esegue un processo di sincronizzazione dei dati che può consumare risorse di I/O del disco. Per ulteriori informazioni, consulta Gestione della capacità di throughput.

Per ulteriori informazioni sulle prestazioni del file system, vedere. Prestazioni di FSx for Windows File Server

Accesso ai parametri di FSx for Windows File Server

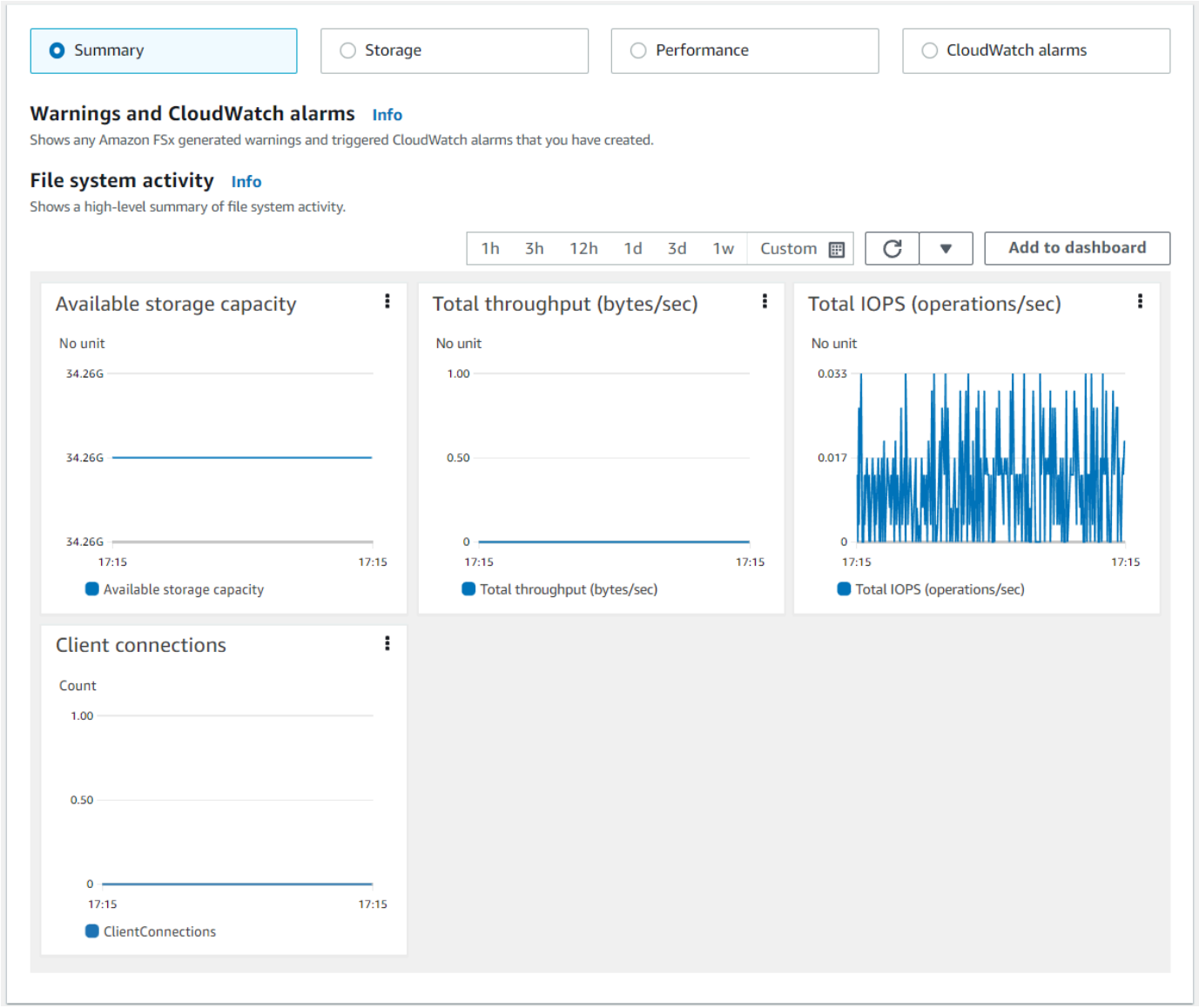
Puoi visualizzare i parametri di Amazon FSx CloudWatch nei seguenti modi.

- La console Amazon FSx.
- La CloudWatch console.
- La CloudWatch CLI (interfaccia a riga di comando).
- L' CloudWatch API.

Le seguenti procedure descrivono come accedere alle metriche del file system utilizzando questi vari strumenti.

Per visualizzare i parametri del file system utilizzando la console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Per visualizzare la pagina dei dettagli del file system, scegli File system nel pannello di navigazione.
3. Scegli il file system di cui desideri visualizzare le metriche.
4. Per visualizzare i grafici delle metriche del file system, scegli Monitoraggio e prestazioni nel secondo pannello.

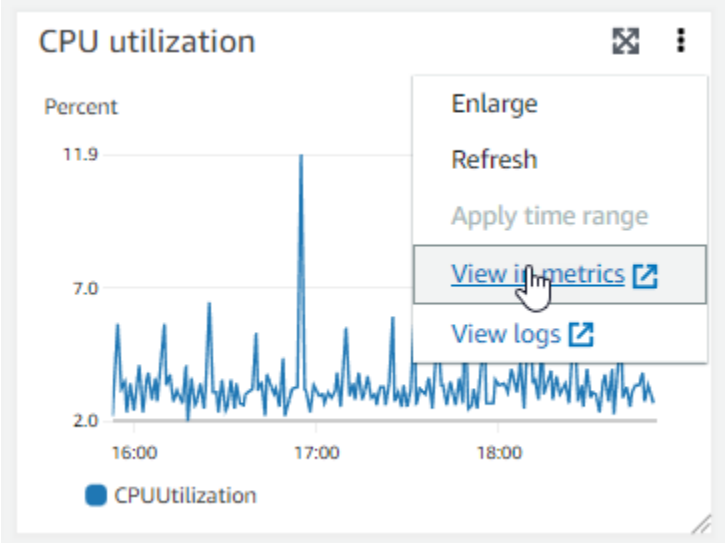


- Le metriche di riepilogo vengono visualizzate per impostazione predefinita e mostrano eventuali avvisi e CloudWatch allarmi attivi insieme alle metriche di attività del file system.
- Scegli Archiviazione per visualizzare la capacità di archiviazione e le metriche di utilizzo.
- Scegli Performance per visualizzare i parametri relativi alle prestazioni dei file server e dello storage
- Scegli gli CloudWatch allarmi per visualizzare i grafici di tutti gli allarmi configurati per il file system.

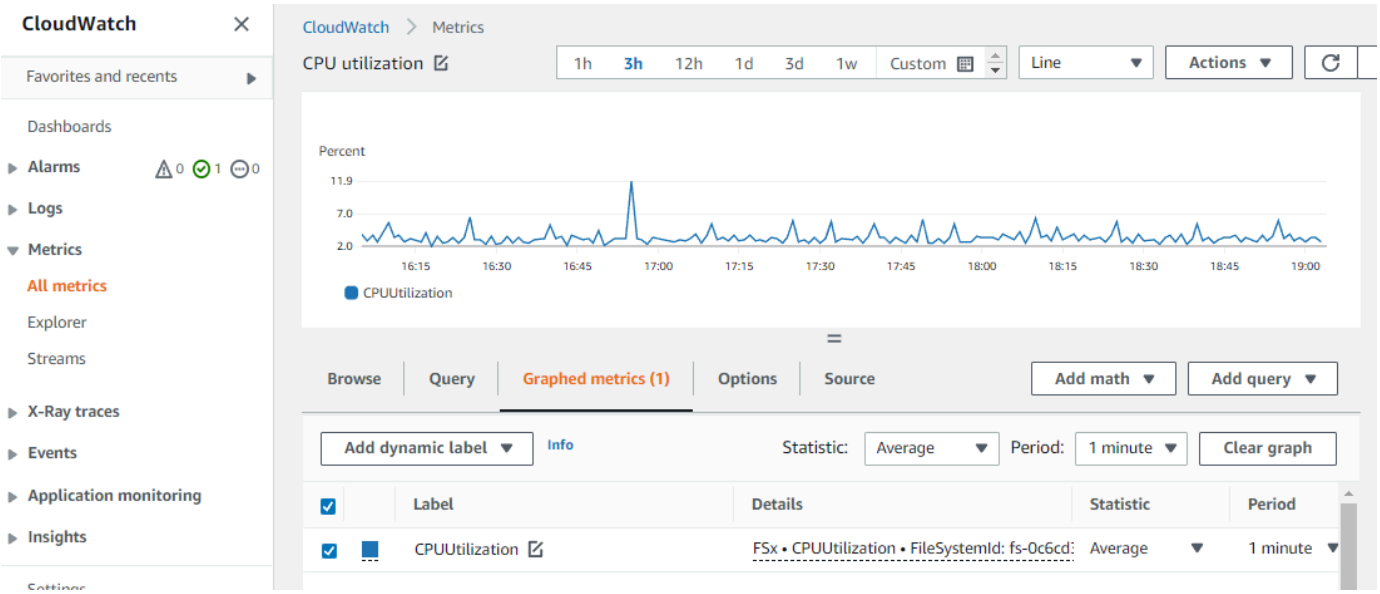
Per ulteriori informazioni, consulta Come utilizzare le metriche di FSx for Windows File Server

Per visualizzare le metriche nella console CloudWatch

1. Per visualizzare una metrica del file system nella pagina Metriche della CloudWatch console Amazon, accedi alla metrica nel pannello Monitoraggio e prestazioni della console Amazon FSx.
2. Scegli Visualizza nelle metriche dal menu delle azioni in alto a destra del grafico delle metriche, come mostrato nell'immagine seguente.



Si apre la pagina Metriche nella CloudWatch console, che mostra il grafico metrico, come mostrato nell'immagine seguente.



Per aggiungere metriche a una dashboard CloudWatch

1. Per aggiungere un set di parametri del file system FSx for Windows a un pannello di controllo nella CloudWatch console, scegli il set di parametri (Riepilogo, Storage o Performance) nel pannello Monitoraggio e prestazioni della console Amazon FSx.
2. Scegli Aggiungi alla dashboard nella parte superiore destra del pannello per aprire la console. CloudWatch
3. Seleziona una CloudWatch dashboard esistente dall'elenco o crea una nuova dashboard. Per ulteriori informazioni, consulta Using Amazon CloudWatch dashboard nella Amazon CloudWatch User Guide.

Per accedere alle metriche da AWS CLI

- Utilizza il comando `list-metrics` con il namespace `--namespace "AWS/FSx"`. Per ulteriori informazioni, consulta la sezione relativa alle informazioni di riferimento ai comandi di AWS CLI.

Utilizzando l'API CloudWatch

Per accedere alle metriche dall'API CloudWatch

- Chiama `GetMetricStatistics`. Per ulteriori informazioni, consulta Amazon CloudWatch API Reference.

Creazione di CloudWatch allarmi per monitorare Amazon FSx

Puoi creare un CloudWatch allarme che invia un messaggio Amazon SNS quando l'allarme cambia stato. Un allarme controlla un singolo parametro in un periodo di tempo specificato ed esegue una o più operazioni in base al valore del parametro relativo a una determinata soglia in una serie 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 semplicemente perché si trovano in uno stato particolare; lo stato deve essere cambiato e mantenuto per un determinato numero di periodi. Puoi creare un allarme dalla console Amazon FSx o dalla CloudWatch console.

Le seguenti procedure descrivono come creare allarmi per Amazon FSx utilizzando la console e l' AWS CLI API.

Per impostare allarmi utilizzando la console Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Dal pannello di navigazione, scegli File system, quindi scegli il file system per cui desideri creare l'allarme.
3. Scegli il menu Azioni e scegli Visualizza dettagli.
4. Nella pagina di riepilogo, scegli Monitoraggio e prestazioni.
5. Scegli CloudWatch allarmi.
6. Scegli Crea CloudWatch allarme. Sarai reindirizzato alla console CloudWatch.
7. Scegli Seleziona metriche e scegli Avanti.
8. Nella sezione Metriche, scegli FSX.
9. Scegli Metriche del file system, 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 e scegli Avanti.

> **Note**
>
> Le metriche potrebbero non essere pubblicate durante la manutenzione del file system per i file system Single-AZ o durante il failover e il failback da o verso i server primari o secondari per i file system Multi-AZ. 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 SNS quando lo stato di allarme attiva l'azione, scegli uno stato di allarme per Ogni volta che lo stato di allarme è.

    Per selezionare un argomento SNS, scegli un argomento SNS esistente. Se selezioni Crea argomento, puoi impostare il nome e gli indirizzi e-mail per un nuovo elenco di sottoscrizioni e-mail. Questo elenco viene salvato e visualizzato nel campo per allarmi futuri. Seleziona Successivo.

> **Note**
>
> Se usi Crea argomento per creare un nuovo argomento Amazon SNS, gli indirizzi e-mail devono essere verificati prima di poter ricevere le notifiche. Le e-mail sono inviate solo quando viene attivato lo stato di allarme. Se lo stato cambia prima della verifica degli indirizzi e-mail, questi non riceveranno una notifica.

12. Inserisci i valori Name, Description e Whenever per la metrica e 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. Accedi AWS Management Console e apri la CloudWatch console all'indirizzo https://console.aws.amazon.com/cloudwatch/.
2. Scegli Create Alarm per avviare la Create Alarm Wizard.
3. Scegli FSx Metrics e scorri i parametri di Amazon FSx per individuare il parametro su cui desideri inserire un allarme. Per visualizzare solo i parametri di Amazon FSx in questa finestra di dialogo, cerca l'ID del file system del tuo file system. Seleziona il parametro per il quale si intende creare un allarme e scegli Avanti.
4. Compila i valori Name (Nome), Description (Descrizione) e Whenever (Qualsiasi momento) per il parametro.
5. Se desideri CloudWatch inviarti un'e-mail quando viene raggiunto lo stato di allarme, per Ogni volta che si verifica questo allarme, scegli State is ALARM. Per Invia notifica a:, scegliere un argomento SNS esistente. Se selezioni Crea argomento, puoi impostare il nome e gli indirizzi e-mail per un nuovo elenco di sottoscrizioni e-mail. Questo elenco viene salvato e visualizzato nel campo per allarmi futuri.

> **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 viene attivato lo stato di allarme. Se lo stato cambia prima della verifica degli indirizzi e-mail, questi non riceveranno una notifica.

6. A questo punto, l'area di anteprima dell'allarme ti dà la possibilità di vedere in anteprima l'avviso che stai per creare. Scegli Crea allarme.

Per impostare una sveglia utilizzando il AWS CLI

- Chiamare `put-metric-alarm`. Per ulteriori informazioni, consulta il Riferimento ai comandi AWS CLI.

Per impostare un allarme utilizzando l' CloudWatch API

- Chiama `PutMetricAlarm`. Per ulteriori informazioni, consulta Amazon CloudWatch API Reference.

Registrazione di chiamate API Amazon FSx for Windows File Server File Server File Server conAWS CloudTrail

Amazon FSx for Windows File Server è integrato conAWS CloudTrail, un servizio che fornisce un record delle operazioni eseguite da un utente, un ruolo o unAWSservizio in Amazon FSx. CloudTrail acquisisce tutte le chiamate API per Amazon FSx come eventi. Le chiamate acquisite includono le chiamate dalla console Amazon FSx e le chiamate di codice alle operazioni API Amazon FSx. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi su un bucket Amazon S3, inclusi gli eventi per Amazon FSx. Se non configuri un trail, è comunque possibile visualizzare gli eventi più recenti in CloudTrail Console inCronologia eventi. Utilizzo delle informazioni raccolte da CloudTrail, puoi determinare la richiesta effettuata ad Amazon FSx, l'indirizzo IP da cui è stata eseguita la richiesta, l'autore della richiesta, il momento in cui è stata eseguita la richiesta, l'autore della richiesta, l'autore della richiesta, il momento in cui è stata eseguita

Per ulteriori informazioni su CloudTrail, consulta.AWS CloudTrailGuida per l’utente di.

Informazioni Amazon FSx in CloudTrail

CloudTrail è abilitato sul tuoAccount AWSquando crei l'account. Quando si verifica un'attività in Amazon FSx, tale attività viene registrata in un CloudTrail evento insieme ad altriAWSEventi del servizio inCronologia eventi. Puoi visualizzare, cercare e scaricare gli eventi recenti nell'Account AWS. Per ulteriori informazioni, consulta la paginaVisualizzazione di eventi con CloudTrail Cronologia eventi.

Per una registrazione continuativa di attività ed eventi nel tuoAccount AWS, inclusi gli eventi per Amazon FSx, crea un trail. UNpistaabilita CloudTrail per distribuire i file di log in un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le regioni nella partizione AWS e distribuisce i file di registro nel bucket Amazon S3 specificato. Inoltre, puoi configurarne altriAWSservizi per analizzare con maggiore dettaglio e usare i dati raccolti in CloudTrail registri. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un percorso
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione CloudTrail file di log da più regioneRicezione CloudTrail file di log da più account

Tutte le operazioni Amazon FSx sono registrate da CloudTrail e sono documentati nelGuida di riferimento all'API FSx. Ad esempio, le chiamate al`CreateFileSystem`,`CreateBackup`e`TagResource`le azioni generano voci nel CloudTrail file di log.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci del file di log Amazon FSx

Un trail è una configurazione che consente la distribuzione di eventi come i file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di log possono contenere una o più voci di log. Un evento rappresenta una singola richiesta da un'origine e include informazioni sull'operazione richiesta, data e ora dell'operazione, parametri della richiesta e così via. CloudTrail i file di log non sono una traccia di pila ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in base a un ordine specifico.

Il seguente esempio mostra un CloudTrail voce di registro che dimostra la`TagResource`operazione quando un tag per un file system viene creato dalla console.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

Il seguente esempio mostra un CloudTrail voce di registro che dimostra la`UntagResource`azione 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"
}
```

Prestazioni di FSx for Windows File Server

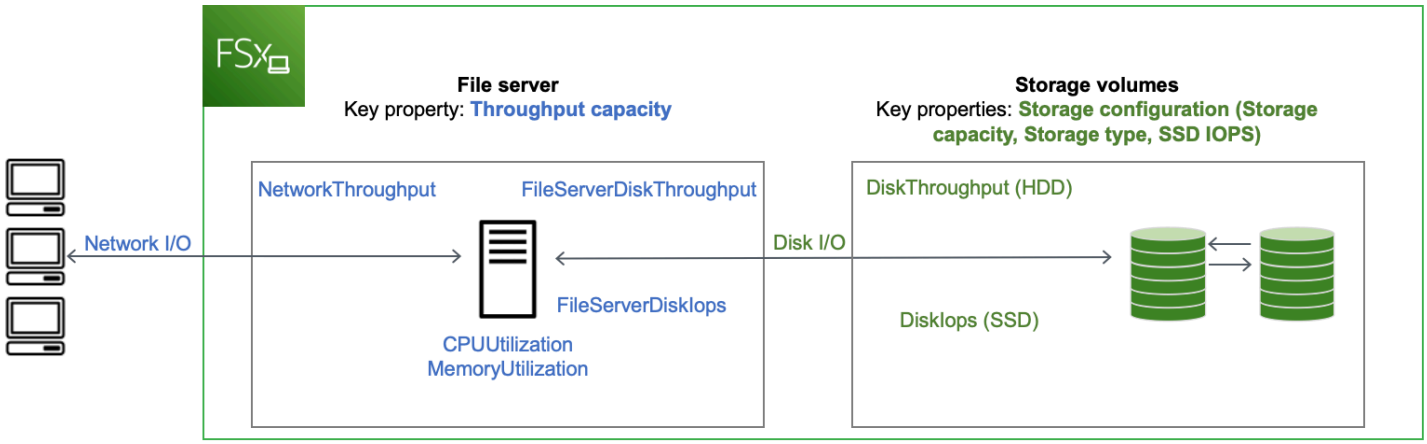
FSx for Windows File Server offre opzioni di configurazione del file system per soddisfare una varietà di esigenze di prestazioni. Di seguito è riportata una panoramica delle prestazioni del file system Amazon FSx, con una discussione sulle opzioni di configurazione delle prestazioni disponibili e utili suggerimenti sulle prestazioni.

Argomenti

Prestazioni del file system

Ogni file system FSx for Windows File Server è costituito da un file server Windows con cui i client comunicano e da un set di volumi di storage, o dischi, collegati al file server. Ogni file server utilizza una cache veloce in memoria per migliorare le prestazioni dei dati a cui si accede con maggiore frequenza.

Il diagramma seguente illustra come si accede ai dati da un file system FSx for Windows File Server.



Quando un client accede ai dati archiviati nella cache in memoria, i dati vengono forniti direttamente al client richiedente come I/O di rete. Il file server non ha bisogno di leggerli o scriverli sul disco. Le prestazioni di questo accesso ai dati sono determinate dai limiti di I/O di rete e dalla dimensione della cache in memoria.

Quando un client accede a dati non presenti nella cache, il file server li legge o li scrive sul disco come I/O del disco. I dati vengono quindi serviti dal file server al client come I/O di rete. Le prestazioni di questo accesso ai dati sono determinate dai limiti di I/O della rete e dai limiti di I/O del disco.

Le prestazioni di I/O di rete e la cache in memoria del file server sono determinate dalla capacità di trasmissione del file system. Le prestazioni di I/O del disco sono determinate da una combinazione di capacità di throughput e configurazione di storage. Le prestazioni massime di I/O del disco, costituite dalla velocità effettiva del disco e dai livelli di IOPS del disco, che il file system è in grado di raggiungere sono le seguenti:

- Il livello di prestazioni di I/O del disco fornito dal file server, in base alla capacità di throughput selezionata per il file system.
- Il livello di prestazioni di I/O del disco fornito dalla configurazione di storage (capacità di storage, tipo di storage e livello di IOPS SSD selezionato per il file system).

Considerazioni aggiuntive sulle prestazioni

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

Latenza

I file server FSx for Windows File Server utilizzano una cache veloce in memoria per ottenere latenze costanti inferiori al millisecondo per i dati ad accesso attivo. Per i dati che non si trovano nella cache in memoria, ovvero per le operazioni sui file che devono essere gestite eseguendo I/O sui volumi di storage sottostanti, Amazon FSx fornisce latenze di operazioni di file inferiori al millisecondo con storage su unità a stato solido (SSD) e latenze a una cifra di millisecondi con storage su disco rigido (HDD).

Throughput e IOPS

I file system Amazon FSx forniscono fino a 2 GB/s e 80.000 IOPS in tutti i paesi in cui è disponibile Regioni AWS Amazon FSx e 12 GB/s di throughput e 400.000 IOPS negli Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti orientali (Ohio), Europa (Irlanda), Asia Pacifico (Tokyo) e Asia Pacifico (Singapore). La quantità specifica di throughput e IOPS che il carico di lavoro può generare sul file system dipende dalla capacità di throughput, dalla capacità di archiviazione e dal tipo di storage del file system, oltre alla natura del carico di lavoro, inclusa la dimensione del working set attivo.

Prestazioni con un solo client

Con Amazon FSx, puoi raggiungere tutti i livelli di throughput e IOPS del tuo file system da un singolo client che vi accede. Amazon FSx supporta il multicanale SMB. Questa funzionalità consente di fornire un throughput fino a più GB/s e centinaia di migliaia di IOPS per un singolo client che accede al file system. SMB Multichannel utilizza più connessioni di rete tra client e server contemporaneamente per aggregare la larghezza di banda della rete per il massimo utilizzo. Sebbene esista un limite teorico al numero di connessioni SMB supportate da Windows, questo limite è di milioni e praticamente è possibile avere un numero illimitato di connessioni SMB.

Prestazioni impennate

I carichi di lavoro basati su file sono in genere caratterizzati da picchi di traffico, caratterizzati da periodi brevi e intensi di I/O elevati, con lunghi periodi di inattività tra i burst. Per supportare carichi di lavoro con picchi di lavoro, oltre alle velocità di base che un file system può supportare 24 ore su 24, 7 giorni su 7, Amazon FSx offre la possibilità di raggiungere velocità più elevate per periodi di tempo sia per le operazioni di I/O di rete che di I/O su disco. Amazon FSx utilizza un meccanismo di crediti I/O per allocare throughput e IOPS in base all'utilizzo medio: i file system accumulano crediti quando il

loro throughput e l'utilizzo di IOPS sono inferiori ai limiti di base e possono utilizzare questi crediti per eseguire operazioni di I/O.

Impatto della capacità di throughput sulle prestazioni

La capacità di throughput determina le prestazioni del file system nelle seguenti categorie:

- I/O di rete: la velocità alla quale il file server può fornire i dati dei file ai client che vi accedono.
- CPU e memoria del file server: risorse disponibili per servire i dati dei file ed eseguire attività in background come la deduplicazione dei dati e le copie shadow.
- I/O su disco: la velocità alla quale il file server è in grado di supportare l'I/O tra il file server e i volumi di storage.

Le tabelle seguenti forniscono dettagli sui livelli massimi di I/O di rete (throughput e IOPS) e I/O su disco (throughput e IOPS) che è possibile ottenere con ogni configurazione di capacità di throughput fornita e la quantità di memoria disponibile per la memorizzazione nella cache e il supporto di attività in background come la deduplicazione dei dati e le copie shadow. Sebbene sia possibile selezionare livelli di capacità di throughput inferiori a 32 megabyte al secondo (MBps) quando si utilizza l'API o la CLI di Amazon FSx, tieni presente che questi livelli sono pensati per carichi di lavoro di test e sviluppo, non per carichi di lavoro di produzione.

> **Note**
>
> Tieni presente che i livelli di capacità di throughput pari o superiori a 4.608 MBps sono supportati solo nelle seguenti regioni: Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti orientali (Ohio), Europa (Irlanda), Asia Pacifico (Tokyo) e Asia Pacifico (Singapore).

I/O e memoria di rete

Capacità di throughput FSx (megabyte al secondo)	Throughput di rete (megabyte al secondo)		IOPS di rete	Memoria (GB)
	Linea di base	Burst (per pochi minuti al giorno)		
32	32	600	Migliaia	4
64	64	600	Decine di migliaia	8
128	150	1.250		8
256	300	1.250	Centinaia di migliaia	16
512	600	1.250		32
1,024	1.500	–		72
2.048	3.125	–		144
4.608	9.375	–	Milioni	192
6.144	12.500	–		256
9.216	18.750	–		384
12.288	21.250	–		512

I/O del disco

Capacità di throughput FSx (megabyte al secondo)	Velocità effettiva del disco (megabyte al secondo)		IOPS del disco	
	Linea di base	Burst (per 30 minuti al giorno)	Linea di base	Burst (per 30 minuti al giorno)
32	32	260	2K	12 K
64	64	350	4K	16 K
128	128	600	6 K	20 K
256	256	600	10K	20 K
512	512	–	20 K	–
1,024	1,024	–	40K	–
2.048	2.048	–	80 K	–
4.608	4.608	–	150 K	–
6.144	6.144	–	200 K	–
9.216	9.216 [1]	–	300 K [1]	–
12.288	12.288 [1]	–	400 K [1]	–

Note

[1] Se si dispone di un file system Multi-AZ con una capacità di throughput di 9.216 o 12.288 MBps, le prestazioni saranno limitate a 9.000 MBps e 262.500 IOPS per il solo traffico di scrittura. Altrimenti, per il traffico di lettura su tutti i file system Multi-AZ, il traffico di lettura e scrittura su tutti i file system Single-AZ e tutti gli altri livelli di capacità di throughput, il file system supporterà i limiti di prestazioni indicati nella tabella.

Scelta del giusto livello di capacità di throughput

Quando crei un file system utilizzando la console di gestione di Amazon Web Services, Amazon FSx seleziona automaticamente il livello di capacità di throughput consigliato per il tuo file system in base alla quantità di capacità di storage configurata. Sebbene la capacità di throughput consigliata dovrebbe essere sufficiente per la maggior parte dei carichi di lavoro, hai la possibilità di ignorare il consiglio e selezionare una quantità specifica di capacità di throughput per soddisfare le esigenze dell'applicazione. Ad esempio, se il carico di lavoro richiede l'indirizzamento di 1 GBps di traffico verso il file system, è necessario selezionare una capacità di throughput di almeno 1.024 MBps.

Per decidere il livello di velocità effettiva da configurare, è inoltre necessario considerare le funzionalità che si intende abilitare sul file system. Ad esempio, l'attivazione delle Shadow Copies può richiedere l'aumento della capacità di throughput fino a tre volte il carico di lavoro previsto per garantire che il file server possa mantenere le copie shadow con la capacità di prestazioni di I/O disponibile. Se si abilita la deduplicazione dei dati, è necessario determinare la quantità di memoria associata alla capacità di throughput del file system e assicurarsi che tale quantità di memoria sia sufficiente per le dimensioni dei dati.

È possibile aumentare o ridurre la quantità di capacità di throughput in qualsiasi momento dopo la creazione. Per ulteriori informazioni, consulta Gestione della capacità di throughput.

Puoi monitorare l'utilizzo da parte del carico di lavoro delle risorse prestazionali dei file server e ottenere consigli sulla capacità di throughput da selezionare visualizzando la scheda Monitoraggio e prestazioni > Prestazioni della console Amazon FSx. Ti consigliamo di eseguire il test in un ambiente di preproduzione per garantire che la configurazione selezionata soddisfi i requisiti prestazionali del tuo carico di lavoro. Per i file system Multi-AZ, consigliamo inoltre di testare l'impatto del processo di failover che si verifica durante la manutenzione del file system, le modifiche alla capacità di throughput e l'interruzione non pianificata del servizio sul carico di lavoro, oltre a garantire una capacità di throughput sufficiente per prevenire l'impatto sulle prestazioni durante questi eventi. Per ulteriori informazioni, consulta Accesso ai parametri di FSx for Windows File Server.

Impatto della configurazione dello storage sulle prestazioni

La capacità di storage, il tipo di storage e il livello di IOPS dell'SSD influiscono tutti sulle prestazioni di I/O su disco del file system. Puoi configurare queste risorse per fornire i livelli di prestazioni desiderati per il tuo carico di lavoro.

Puoi aumentare la capacità di archiviazione e scalare gli IOPS SSD in qualsiasi momento. Per ulteriori informazioni, consulta Gestione della capacità di archiviazione e Gestione degli IOPS SSD. Puoi anche aggiornare il file system dal tipo di archiviazione HDD al tipo di archiviazione SSD. Per ulteriori informazioni, consulta Gestione del tipo di storage.

Il file system fornisce i seguenti livelli predefiniti di velocità effettiva del disco e IOPS:

Storage Type (Tipo di storage)	Velocità effettiva del disco (MBps per TiB di storage)	IOPS su disco (IOPS per TiB di storage)
SSD	750	3.000*
HDD	12 linee di base; 80 burst (fino a un massimo di 1 GB/s per file system)	12 linee di base; 80 raffiche

> **Note**
>
> *Per i file system con tipo di storage SSD, è possibile fornire IOPS aggiuntivi fino a un rapporto massimo di 500 IOPS per GiB di storage e 400.000 IOPS per file system.

Prestazioni HDD burst

Per i volumi di storage su disco rigido, Amazon FSx utilizza un modello burst bucket per le prestazioni. Le dimensioni del volume determinano il throughput di base del volume, ossia la velocità a cui il volume accumula i crediti del throughput. Le dimensioni del volume determinano il throughput ottimale del volume, ossia la velocità a cui è possibile spendere crediti quando sono disponibili. I volumi più grandi hanno baseline elevata e un throughput ottimale. Maggiore è il numero di crediti di cui dispone il volume, più a lungo può guidare I/O a livello ottimale.

Il throughput disponibile di un volume di storage HDD è espresso dalla seguente formula:

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

Per un volume HDD da 1 TiB, il burst throughput è limitato a 80 MIB/s, il bucket si riempie di crediti a 12 MIB/s e può contenere fino a 1 TiB di crediti.

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 configurato con 2 TiB di capacità di storage su disco rigido e 32 MBps di capacità di throughput presenta i seguenti livelli di throughput:

- Throughput di rete: 32 MBps di base e 600 MBps di burst (vedere la tabella sulla capacità di throughput)
- Throughput del disco: 24 MBps di base e 160 MBps di burst, che è il valore più basso tra:
  - i livelli di throughput del disco di 32 MBps di base e 260 MBps di burst supportati dal file server, in base alla capacità di throughput del file system
  - i livelli di throughput del disco di 24 MBps di base (12 MBps per TB * 2 TiB) e 160 MBps burst (80 MBps per TiB* 2 TiB) supportati dai volumi di storage, in base al tipo e alla capacità di storage

Il carico di lavoro che accede al file system sarà quindi in grado di gestire un throughput di base fino a 32 MBps e un throughput burst fino a 600 MBps per le operazioni sui file eseguite sui dati ad accesso attivo memorizzati nella cache in memoria del file server e fino a 24 MBps di velocità di base e 160 MBps per le operazioni sui file che devono arrivare fino al disco, ad esempio a causa di errori di cache.

Misurazione delle prestazioni mediante metriche CloudWatch

Puoi usare Amazon CloudWatch per misurare e monitorare il throughput e gli IOPS del tuo file system. Per ulteriori informazioni, consulta Monitoraggio delle metriche con Amazon CloudWatch.

Risoluzione dei problemi di prestazioni

Per assistenza nella risoluzione dei problemi di prestazioni più comuni, vedereRisoluzione dei problemi di prestazioni del file system.

Procedure dettagliate su Amazon FSx

Di seguito, puoi trovare una serie di procedure dettagliate orientate alle attività che ti guidano attraverso vari processi.

Argomenti

Procedura guidata 1: Prerequisiti per iniziare

Prima di poter completare l'esercizio introduttivo, devi già avere un'istanza Amazon EC2 basata su Microsoft Windows unita al tuoAWS Directory Servicedirectory. È inoltre necessario aver effettuato l'accesso all'istanza tramite Windows Remote Desktop Protocol come utente amministratore della directory. Le procedure guidate seguenti illustrano come eseguire queste azioni prerequisite necessarie.

Argomenti

Fase 1: Configurazione di Active Directory

Con Amazon FSx, puoi gestire lo storage file completamente gestito per carichi di lavoro basati su Windows. Allo stesso modo,AWS Directory Servicefornisce directory completamente gestite da utilizzare nella distribuzione del carico di lavoro. Se hai un dominio AD aziendale esistente in esecuzioneAWSin un cloud privato virtuale (VPC) che utilizza istanze EC2, è possibile abilitare

l'autenticazione basata sull'utente e il controllo degli accessi. Lo fai stabilendo una relazione di fiducia tra ilAWSMicrosoft AD gestito e il dominio aziendale. Per l'autenticazione Windows in Amazon FSx, è necessario solo un trust di foresta direzionale unidirezionale, doveAWSla foresta gestita si fida della foresta di domini aziendali.

Il dominio aziendale assume il ruolo di dominio attendibile eAWS Directory Serviceil dominio gestito assume il ruolo del dominio fiduciario. Le richieste di autenticazione convalidate viaggiano tra i domini in una sola direzione, consentendo agli account del dominio aziendale di autenticarsi in base alle risorse condivise nel dominio gestito. In questo caso, Amazon FSx interagisce solo con il dominio gestito. Il dominio gestito trasmette quindi le richieste di autenticazione al dominio aziendale.

> **Note**
>
> Puoi anche utilizzare un tipo di trust esterno con Amazon FSx per domini attendibili.

Il gruppo di sicurezza di Active Directory deve abilitare l'accesso in entrata dal gruppo di sicurezza del file system Amazon FSx.

Per creare unAWSServizi directory per Microsoft AD

- Se non ne hai ancora uno, usa ilAWS Directory Serviceper creare ilAWSDirectory Microsoft AD Managed. Per ulteriori informazioni, consultaCreazione delAWSDirectory Microsoft AD gestitanellaAWS Directory ServiceGuida di amministrazione.

  > **Important**
  >
  > Ricorda la password che assegni al tuo utente amministratore; ne hai bisogno più avanti in questo esercizio introduttivo. Se si dimentica la password, è necessario ripetere i passaggi di questo esercizio con il nuovoAWS Directory Servicedirectory e utente amministratore.

- Se disponi di un AD esistente, crea una relazione di trust tra ilAWSMicrosoft AD gestito e il tuo AD esistente. Per ulteriori informazioni, consulta Quando creare una relazione di trust nella Guida di amministrazione di AWS Directory Service.

Fase 2: Avvia un'istanza Windows nella console Amazon EC2

Puoi avviare un'istanza Windows utilizzando laAWS Management Consolecome descritto nella seguente procedura. Ciò consente di avviare rapidamente la prima istanza, in modo da non coprire

tutte le possibili opzioni. Per ulteriori informazioni sulle opzioni avanzate, consulta l'argomento relativo all'avvio di un'istanza.

Per avviare un'istanza

1. Aprire la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Dal pannello di controllo della console, scegliere Launch Instance (Avvia istanza).
3. Nella pagina Choose an Amazon Machine Image (AMI) (Scegli Amazon Machine Image (AMI)) è visualizzato un elenco delle configurazioni di base denominato Amazon Machine Images (AMIs) (Amazon Machine Image (AMI)), che possono fungere da modelli per l'istanza. Selezionare l'AMI per Windows Server 2016 Base o Windows Server 2012 R2 Base. Queste AMI sono contrassegnate dalla dicitura "Free tier eligible" (Idoneo per il piano gratuito).
4. Nella pagina Choose an Instance Type (Scegli un tipo di istanza), è possibile selezionare la configurazione hardware per l'istanza. Selezionare il tipo `t2.micro`, ovvero l'opzione selezionata per impostazione di default. Questo tipo di istanza è idoneo per il piano gratuito.
5. Scegliere Review and Launch (Analizza e avvia) per consentire alla procedura guidata di completare automaticamente le altre impostazioni di configurazione.
6. SulRivedi l'avvio dell'istanzapagina, sottoSecurity Groups (Gruppi di sicurezza), viene visualizzato un gruppo di sicurezza che la procedura guidata ha creato e selezionato per te. Puoi utilizzare questo gruppo di sicurezza o scegliere il gruppo di sicurezza creato durante la configurazione utilizzando la procedura seguente:

   a. Scegliere Edit security groups (Modifica gruppi di sicurezza).
   b. Nella pagina Configure Security Group (Configura gruppi di sicurezza), assicurarsi che l'opzione Select an existing security group (Seleziona un gruppo di sicurezza esistente) sia selezionata.
   c. Selezionare il gruppo di sicurezza dall'elenco dei gruppi di sicurezza esistenti, quindi scegliere Review and Launch (Analizza e avvia).
7. Nella pagina Review Instance Launch (Verifica avvio istanza), scegliere Launch (Avvia).
8. Quando viene richiesto di immettere una coppia di chiavi, selezionare Choose an existing key pair (Scegli una coppia di chiavi esistente), quindi scegliere la coppia di chiavi creata durante la configurazione.

   In alternativa, è possibile creare una nuova coppia di chiavi. Selezionare Create a new key pair (Crea una nuova coppia di chiavi), immettere un nome per la coppia, quindi scegliere Download Key Pair (Scarica la coppia di chiavi). Questo è l'unico momento in cui salvare il file della chiave

privata. Assicurarsi di scaricarlo. Salvare il file della chiave privata in un luogo sicuro. Dovrai fornire il nome della coppia di chiavi quando avvii un'istanza e la chiave privata corrispondente ogni volta che ti connetti all'istanza.

> **Warning**
>
> Non selezionare l'opzione Proceed without a key pair (Procedi senza una coppia di chiavi). Se l'istanza viene avviata senza una coppia di chiavi, non sarà possibile connettersi a essa.

Al termine, selezionare la casella di controllo di conferma, quindi scegliere Launch Instances (Avvia istanze).

9. Una pagina di conferma indicherà che l'istanza si sta avviando. Scegliere View Instances (Visualizza istanze) per chiudere la pagina di conferma e tornare alla console.
10. Nella schermata Instances (Istanze), è possibile visualizzare lo stato dell'avvio. L'avvio di un'istanza richiede pochi minuti. Quando avvii un'istanza, il suo stato iniziale è `pending`. Dopo aver avviato l'istanza, il relativo stato cambia in `running` e l'istanza riceve un nome DNS pubblico. Se la colonna Public DNS (IPv4) (DNS pubblico (IPv4)) è nascosta, scegliere Show/Hide Columns (Mostra/nascondi colonne) (icona a forma di ingranaggio) nell'angolo superiore destro della pagina, quindi selezionare Public DNS (IPv4) (DNS pubblico (IPv4)).)
11. Possono essere necessari alcuni minuti affinché l'istanza sia pronta e sia possibile connettervisi. Controllare che l'istanza abbia superato i controlli relativi allo stato. È possibile visualizzare queste informazioni nella colonna Status Checks (Verifiche dello stato).

> **Important**
>
> Annotare l'ID del gruppo di sicurezza creato all'avvio di questa istanza. In quanto sarà necessario per la creazione del file system Amazon FSx.

Ora che l'istanza è stata avviata, puoi connetterti all'istanza.

Fase 3: Connessione all'istanza

Per connettersi a un'istanza di Windows, è necessario recuperare la password iniziale dell'amministratore e specificarla quando ci si connette all'istanza tramite Desktop remoto.

Il nome dell'account amministratore dipende dalla lingua del sistema operativo. Per esempio, per l'inglese è Administrator, per il francese è Administrateur e per il portoghese è Administrador. Per ulteriori informazioni, consulta Nomi localizzati dell'account amministratore in Windows nel Wiki Microsoft TechNet.

Se l'istanza è stata aggiunta a un dominio, è possibile connettersi all'istanza utilizzando le credenziali di dominio definite inAWS Directory Service. Nella schermata di accesso Desktop remoto, non utilizzare il nome del computer locale e la password generata. Utilizzate invece il nome utente completo per l'amministratore e la password per questo account. Un esempio è **`corp.example.com\Admin`**.

La licenza per il sistema operativo Windows Server consente due connessioni remote simultanee per scopi amministrativi. Il costo della licenza per Windows Server è incluso nel costo della tua istanza Windows. Se hai bisogno di più di due connessioni remote simultanee, devi acquistare una licenza di Remote Desktop Services (RDS). Se tenti di stabilire una terza connessione, si verifica un errore. Per ulteriori informazioni, consultaConfigurazione del numero di connessioni remote simultanee consentite per una connessione.

Per connetterti alla tua istanza Windows utilizzando un client RDP

1. Nella console Amazon EC2, selezionare l'istanza, quindi scegliere Connect (Connetti).
2. NellaConnessione all'istanzafinestra di dialogo, scegliereOttieni passwordDopo l'avvio dell'istanza è necessario attendere alcuni minuti prima che la password sia disponibile.
3. Scegliere Browse (Sfoglia) e selezionare il file della chiave privata creato al momento dell'avvio dell'istanza. Selezionare il file e scegliere Open (Apri) per copiare l'intero contenuto del file nel campo Contents (Contenuto).
4. Selezionare Decrypt Password (Decifra password). La console visualizza la password di default dell'amministratore per l'istanza nellaConnessione all'istanzafinestra di dialogo, che sostituisce il collegamento aOttieni passwordmostrato in precedenza con la password effettiva.
5. Prendi nota della password amministratore predefinita oppure copiala negli Appunti. Questa password ti servirà per connetterti all'istanza.
6. Seleziona Download remote desktop file (Scarica file per desktop remoto). Il browser mostrerà un messaggio che ti chiede se desideri aprire o salvare il file .rdp. Entrambe le opzioni vanno bene. Al termine dell'operazione, puoi scegliereChiudiper respingere ilConnessione all'istanzafinestra di dialogo.

- Se hai aperto il file .rdp, visualizzerai la finestra di dialogo Remote Desktop Connection (Connessione Remote Desktop).
- Se hai salvato il file .rdp, puoi navigare nella directory dei download e aprire il file .rdp per visualizzare la finestra di dialogo.

7. Potresti visualizzare un avviso che ti informa che non è nota l'identità di chi ha pubblicato la connessione remota. Puoi continuare a connetterti alla tua istanza.
8. Quando richiesto, accedere all'istanza utilizzando l'account amministratore per il sistema operativo e la password che hai registrato o copiato in precedenza. Se la connessione Desktop remoto dispone già di un account amministratore configurato, potrebbe essere necessario scegliere l'opzione Usa un altro account e digitare il nome utente e la password manualmente.

   > **Note**
   >
   > A volte copiare e incollare i contenuti può danneggiare i dati. Se si verifica un errore di password non corretta quando effettui l'accesso, prova a digitare la password manualmente.

9. Data la natura dei certificati autofirmati, è possibile che venga visualizzato un avviso relativo all'impossibilità di autenticare il certificato di sicurezza. Procedere come descritto di seguito per verificare l'identità del computer remoto oppure scegliere Yes (Sì) o Continue (Continua) per continuare se si ritiene attendibile il certificato.

   a. Se stai utilizzando la Connessione Remote Desktop da un PC Windows, scegliere View certificate (Visualizza certificato). Se stai utilizzando Microsoft Remote Desktop su un computer Mac, scegliere Show certificate (Mostra certificato).
   b. Scegliere la scheda Dettagli, scorrere verso il basso fino alla voce Identificazione personale su un PC Windows oppure alla voce Impronte digitali SHA1 su un computer Mac. Questo è l'identificatore univoco per il certificato di sicurezza del computer remoto.
   c. Nella console Amazon EC2, selezionare l'istanza, scegliere Actions (Operazioni), quindi Get system log (Ottieni il registro di sistema).
   d. Nell'output del logo di sistema, trova la voce `RDPCERTIFICATE-THUMBPRINT`. Se questo valore corrisponde all'identificazione personale o all'impronta del certificato, l'identità del computer remoto è stata verificata.
   e. Se stai utilizzando Remote Desktop Connection da un PC Windows, tornare alla finestra di dialogo Certificato e scegliere OK. Se stai utilizzando Remote Desktop Connection da

un computer Mac, tornare alla finestra di dialogo Verify Certificate (Verifica certificato) e scegliere Continue (Continua).

f. [Windows] Scegliere Yes (Sì) nella finestra Connessione Remote Desktop per connetterti alla tua istanza.

Ora che sei connesso alla tua istanza, puoi unirti all'istanza alla tuaAWS Directory Servicedirectory.

Fase 4: Unisciti alla tua istanza alla tuaAWS Directory Servicedirectory

Nella procedura seguente viene illustrato come aggiungere manualmente un'istanza Amazon EC2 Windows esistente alAWS Directory Servicedirectory.

Per aggiungere un'istanza Windows alAWS Directory Servicedirectory

1. Connettiti all'istanza utilizzando qualsiasi client Remote Desktop Protocol.
2. Apri la finestra di dialogo delle proprietà TCP/IPv4 sull'istanza.

   a. Apri Network Connections (Connessioni di rete).

   > **Tip**
   >
   > Puoi aprire le Network Connections (Connessioni di rete) direttamente eseguendo quanto segue da un prompt del comando sull'istanza.
   >
   > ```
   > %SystemRoot%\system32\control.exe ncpa.cpl
   > ```

   b. Aprire il menu contestuale (clic con il pulsante destro del mouse) per qualsiasi connessione di rete abilitata e scegliereProprietà.

   c. Nella finestra di dialogo delle proprietà di connessione, apri (doppio clic) Internet Protocol Version 4 (Protocollo Internet versione 4).
3. (Opzionale) SelezionaUtilizzare i seguenti indirizzi server DNS, cambia ilPreferred DNS server (Server DNS preferito)eAlternate DNS server (Server DNS alternativo)indirizzi agli indirizzi IP delAWS Directory Service—fornito server DNS e scegliereOK.
4. Apertura dellaProprietà di sistemafinestra di dialogo per l'istanza, scegliere ilNome computertab e scegliModifica.

> **Tip**
>
> Puoi aprire la finestra di dialogo System Properties (Proprietà di sistema) direttamente eseguendo quanto segue da un prompt del comando sull'istanza.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. NellaMembro dibox, scegliDominio, inserisci il nome completo delAWS Directory Servicedirectory e scegliOK.
6. Quando viene richiesto di specificare il nome e la password per l'amministratore di dominio, inserire il nome utente e la password dell'account Admin.

> **Note**
>
> Puoi inserire il nome completo del tuo dominio o il NetBios name, seguiti da una barra rovesciata (\), quindi dal nome utente, in questo caso,Amministratore. Ad esempio, corp.example.com\Admin o corp\Admin.

7. Dopo aver ricevuto il messaggio che ti invita al dominio, riavvia l'istanza perché le modifiche diventino effettive.
8. Riconnettiti all'istanza tramite RDP e accedi all'istanza utilizzando il nome utente e la password perAWS Directory ServiceUtente amministratore della directory.

Ora che la tua istanza è stata aggiunta al dominio, sei pronto a creare il file system Amazon FSx. È quindi possibile continuare a completare le altre attività nell'esercizio iniziale. Per ulteriori informazioni, consultare Guida introduttiva ad Amazon FSx for Windows File Server.

Procedura guidata 2: Creare un file system da un backup

Con Amazon FSx, puoi creare un file system da un backup. In tal caso, è possibile modificare uno dei seguenti elementi per adattarsi meglio al caso d'uso del file system appena creato:

- Storage Type (Tipo di storage)
- Capacità di velocità effettiva
- VPC

- Zona di disponibilità
- Sottorete
- Gruppi di sicurezza VPC
- Configurazione di Active Directory
- AWS KMSChiave di crittografia
- Ora di inizio del backup automatico giornaliero
- Finestra di manutenzione settimanale

La procedura seguente ti guiderà attraverso il processo di creazione di un nuovo file system da un backup. Per creare questo file system, è necessario disporre di un backup esistente. Per ulteriori informazioni, consultaUtilizzo dei backup

Per creare un file system da un backup esistente

1. Aprire la console Amazon FSx all'indirizzohttps://console.aws.amazon.com/fsx/.
2. Dalla lista di navigazione a destra, scegliBackup.
3. Dalla tabella del dashboard, scegliere il backup che si desidera utilizzare per creare un nuovo file system.

   > **Note**
   >
   > È possibile ripristinare il backup solo su un file system con la stessa capacità di archiviazione dell'originale. È possibile aumentare la capacità di storage del file system ripristinato dopo la sua disponibilità. Per ulteriori informazioni, consulta la pagina Gestione della capacità di archiviazione .

4. Scegli Restore backup (Ripristina backup). Questo inizierà la procedura guidata di creazione del file system.
5. Scegli le impostazioni che desideri modificare per questo nuovo file system. Il tipo di storage è impostato suSSDper impostazione predefinita, ma è possibile cambiarlaHDDalle condizioni seguenti:

   - Il tipo di implementazione del file system èMulti-AZoSingle-AZ 2.
   - La capacità di storage è di almeno 2.000 GiB.

6. ScegliereRiepilogo recensioniper rivedere le impostazioni prima di creare il file system.

7. Scegliere Create file system (Crea file system).

Ora hai creato correttamente il nuovo file system da un backup esistente.

Procedura passo per passo Aggiornare un file system esistente

Ci sono tre elementi che è possibile aggiornare con le procedure in questa procedura dettagliata. Tutti gli altri elementi del file system che è possibile aggiornare, è possibile farlo dalla console. Queste procedure presuppongono che tu abbia ilAWS CLIinstallato e configurato nel computer locale. Per ulteriori informazioni, consultaInstallaeConfiguranellaAWS Command Line InterfaceGuida per l'utente di.

- AutomaticBackupRetentionDays— il numero di giorni in cui si desidera mantenere i backup automatici per il file system.
- DailyAutomaticBackupStartTime— l'ora del giorno in UTC (Coordinated Universal Time) in cui si desidera che si avvii la finestra di backup automatico giornaliero. La finestra è di 30 minuti a partire dall'ora specificata. Questa finestra non può sovrapporsi con la finestra di backup della manutenzione settimanale.
- WeeklyMaintenanceStartTime— l'ora della settimana in cui si desidera che la finestra di manutenzione inizi. Il giorno 1 è lunedì, 2 è martedì e così via. La finestra è di 30 minuti a partire dall'ora specificata. Questa finestra non può sovrapporsi con la finestra di backup automatico giornaliera.

Le procedure seguenti illustrano come aggiornare il file system con ilAWS CLI.

Per aggiornare quanto tempo vengono conservati i backup automatici per il file system

1. Aprire un prompt dei comandi o un terminale nel computer.
2. Eseguire il comando seguente, sostituendo l'ID del file system con l'ID del file system e il numero di giorni per i quali si desidera conservare i backup automatici.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration AutomaticBackupRetentionDays=30
```

Per aggiornare la finestra di backup giornaliera del file system

1. Aprire un prompt dei comandi o un terminale nel computer.
2. Eseguire il comando seguente, sostituendo l'ID del file system con l'ID del file system e l'ora con cui si desidera iniziare la finestra.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration DailyAutomaticBackupStartTime=01:00
```

Per aggiornare la finestra di manutenzione settimanale del file system

1. Aprire un prompt dei comandi o un terminale nel computer.
2. Eseguire il comando seguente, sostituendo l'ID del file system con l'ID del file system e la data e l'ora con cui si desidera iniziare la finestra.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

Procedura dettagliata 4: utilizzo di Amazon FSx con Amazon AppStream 2.0

Supportando il protocollo Server Message Block (SMB), Amazon FSx for Windows File Server supporta l'accesso al file system da istanze Amazon EC2AWS, VMware Cloud on WorkSpaces, Amazon e Amazon AppStream 2.0. AppStream 2.0 è un servizio di streaming di applicazioni completamente gestito. Gestisci centralmente le tue applicazioni desktop su AppStream 2.0 e le distribuisci in modo sicuro a un browser su qualsiasi computer. Per ulteriori informazioni sulla AppStream versione 2.0, consulta la Amazon AppStream 2.0 Administration Guide. Per istruzioni su come semplificare la gestione delle immagini e delle flotte Amazon AppStream 2.0, consulta il post delAWS blog Creazione automatica di immagini Windows AppStream 2.0 personalizzate.

Usa questa procedura dettagliata come guida su come utilizzare Amazon FSx con AppStream 2.0 per due casi d'uso: fornire uno storage personale persistente a ciascun utente e fornire una cartella condivisa tra gli utenti per accedere a file comuni.

Fornire spazio di archiviazione personale persistente a ciascun utente

Puoi utilizzare Amazon FSx per fornire a ogni utente della tua organizzazione un'unità di archiviazione unica all'interno di sessioni di streaming AppStream 2.0. Un utente avrà le autorizzazioni per accedere solo alla propria cartella. L'unità viene montata automaticamente all'inizio di una sessione di streaming e i file aggiunti o aggiornati sull'unità vengono mantenuti automaticamente tra le sessioni di streaming.

Per completare questa operazione è necessario eseguire tre procedure.

Per creare cartelle home per utenti di dominio utilizzando Amazon FSx

1. Creare un file system Amazon FSx. Per ulteriori informazioni, consulta Guida introduttiva ad Amazon FSx for Windows File Server.
2. Una volta che il file system è disponibile, crea una cartella per ogni utente del dominio AppStream 2.0 all'interno del file system Amazon FSx. L'esempio seguente utilizza il nome utente di dominio dell'utente come nome della cartella corrispondente. In questo modo è possibile creare facilmente il nome UNC della condivisione di file da mappare facilmente utilizzando la variabile di ambiente Windows`%username%`.
3. Condividi ognuna di queste cartelle come cartella condivisa. Per ulteriori informazioni, consulta Gestione delle condivisioni di file su file system FSx for Windows File Server.

Per avviare un generatore di immagini AppStream 2.0 aggiunto al dominio

1. Accedi alla console AppStream 2.0: https://console.aws.amazon.com/appstream2
2. Scegliete Directory Configs dal menu di navigazione e create un oggetto Directory Config. Per ulteriori informazioni, consulta Utilizzo di Active Directory con AppStream 2.0 nella Guida all'amministrazione di Amazon AppStream 2.0.
3. Scegli Images, Image Builder e avvia un nuovo generatore di immagini.
4. Scegli l'oggetto di configurazione della directory creato in precedenza nella procedura guidata di avvio di immagini per l'aggiunta di uno sviluppatore di immagini al dominio Active Directory.
5. Avvia uno sviluppatore di immagini nello stesso file system Amazon FSx nello stesso file system VPC FSx nello stesso file system Amazon FSx nello stesso file system Amazon FSx. Assicurati di associare il generatore di immagini alla stessaAWS Managed Microsoft AD directory a cui è collegato il tuo file system Amazon FSx. I gruppi di sicurezza VPC associati al generatore di immagini devono consentire l'accesso al file system Amazon FSx.

6. Una volta che il generatore di immagini è disponibile, connettiti al generatore di immagini e accedi utilizzando il tuo account di amministratore di dominio.
7. Installa le tue applicazioni.

Per collegare le condivisioni di file Amazon FSx alla AppStream versione 2.0

1. Nel generatore di immagini, create uno script batch con il seguente comando e memorizzatelo in una posizione di file nota (ad esempio: C:\Scripts\map -fs.bat). L'esempio seguente utilizza S: come lettera di unità per mappare la cartella condivisa sul file system Amazon FSx. In questo script usi il nome DNS del tuo file system Amazon FSx o un alias DNS associato al file system, che puoi ottenere dalla vista dei dettagli del file system nella console Amazon FSx.

   Se si utilizza il nome DNS del file system:

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\users\%username%
   ```

   Se stai utilizzando un alias DNS associato al file system:

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\users\%username%
   ```
2. Apri un PowerShell prompt ed eseguigpedit.msc.
3. Da Configurazione utente scegli Impostazioni Windows e quindi Accedi.
4. Accedete allo script batch creato nella prima fase di questa procedura e selezionatelo.
5. In Configurazione computer, scegli Modelli amministrativi di Windows, Sistema e quindi Criteri di gruppo.
6. Scegli la politica Configura il ritardo dello script di accesso. Abilita la politica e riduci il ritardo a0. Questa impostazione aiuta a garantire che lo script di accesso dell'utente venga eseguito immediatamente quando l'utente avvia una sessione di streaming.
7. Crea la tua immagine e assegnala a una flotta AppStream 2.0. Assicurati di aggiungere anche la flotta AppStream 2.0 allo stesso dominio Active Directory che hai usato per il generatore di immagini. Avvia la flotta nello stesso file system utilizzato da VPC FSx utilizzando lo stesso file system Amazon FSx utilizzato da. I gruppi di sicurezza VPC associati al parco veicoli devono fornire l'accesso al file system Amazon FSx.

8. Avvia una sessione di streaming utilizzando SAML SSO. Per connetterti a un parco veicoli che fa parte di Active Directory, configura la federazione Single Sign-on utilizzando un provider SAML. Per ulteriori informazioni, consulta Accesso Single Sign-on a AppStream 2.0 utilizzando SAML 2.0 nella Guida all'amministrazione di Amazon AppStream 2.0.
9. La tua condivisione di file Amazon FSx è mappata sulla lettera S: drive all'interno della sessione di streaming.

Fornire una cartella condivisa tra gli utenti

Puoi utilizzare Amazon FSx per fornire una cartella condivisa a utenti e compiti della tua organizzazione. Una cartella condivisa può essere utilizzata per conservare file comuni (ad esempio file demo, esempi di codice, manuali di istruzioni, ecc.) necessari a tutti gli utenti.

Per completare questa operazione è necessario eseguire tre procedure.

Per creare una cartella condivisa utilizzando Amazon FSx

1. Creare un file system Amazon FSx. Per ulteriori informazioni, consulta Guida introduttiva ad Amazon FSx for Windows File Server.
2. Ogni file system Amazon FSx include per impostazione predefinita una cartella condivisa a cui puoi accedere utilizzando l'indirizzo\\ *File-system-DNS-name*\ share o\\ *fqdn-DNS-alias*\ share se utilizzi alias DNS. È possibile utilizzare la condivisione predefinita o creare una cartella condivisa diversa. Per ulteriori informazioni, consulta Gestione delle condivisioni di file su file system FSx for Windows File Server.

Per avviare un generatore di immagini AppStream 2.0

1. Dalla console AppStream 2.0, avvia un nuovo generatore di immagini o connettiti a un generatore di immagini esistente. Avvia il generatore di immagini nello stesso VPC utilizzato dal tuo file system Amazon FSx. I gruppi di sicurezza VPC associati al generatore di immagini devono consentire l'accesso al file system Amazon FSx.
2. Una volta che il generatore di immagini è disponibile, connettiti al generatore di immagini come utente amministratore.
3. Installa o aggiorna le tue applicazioni come amministratore.

Per collegare la cartella condivisa alla AppStream versione 2.0

1. Crea uno script batch, come descritto nella procedura precedente, per montare automaticamente la cartella condivisa ogni volta che un utente avvia una sessione di streaming. Per completare lo script, sono necessari il nome DNS del file system o un alias DNS associato al file system (che puoi ottenere dalla vista dei dettagli del file system nella console Amazon FSx) e le credenziali per accedere alla cartella condivisa.

   Se si utilizza il nome DNS del file system:

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\share /user:username password
   ```

   Se stai utilizzando un alias DNS associato al file system:

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\share /user:username password
   ```

2. Crea una policy di gruppo per eseguire questo script batch ad ogni accesso dell'utente. Puoi seguire le stesse istruzioni descritte nella sezione precedente.
3. Crea la tua immagine e assegnala alla tua flotta.
4. Avvia una sessione di streaming. Ora dovresti vedere la cartella condivisa mappata automaticamente alla lettera dell'unità.

Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system

FSx for Windows File Server fornisce un nome DNS (Domain Name System) predefinito per ogni file system che è possibile utilizzare per accedere ai dati sul file system. È inoltre possibile accedere ai file system utilizzando un alias DNS di propria scelta. Con gli alias DNS, puoi continuare a utilizzare i nomi DNS esistenti per accedere ai dati archiviati su Amazon FSx durante la migrazione dello storage del file system da locale ad Amazon FSx, senza dover aggiornare strumenti o applicazioni. Puoi associare fino a 50 alias DNS a un file system contemporaneamente.

Per accedere ai tuoi file system Amazon FSx utilizzando alias DNS, devi eseguire i tre passaggi seguenti:

1. Associa gli alias DNS al tuo file system Amazon FSx.
2. Configura i nomi principali dei servizi (SPN) per l'oggetto computer del tuo file system. (È necessario per ottenere l'autenticazione Kerberos quando si accede al file system utilizzando alias DNS).
3. Aggiorna o crea un record DNS CNAME per il file system e l'alias DNS.

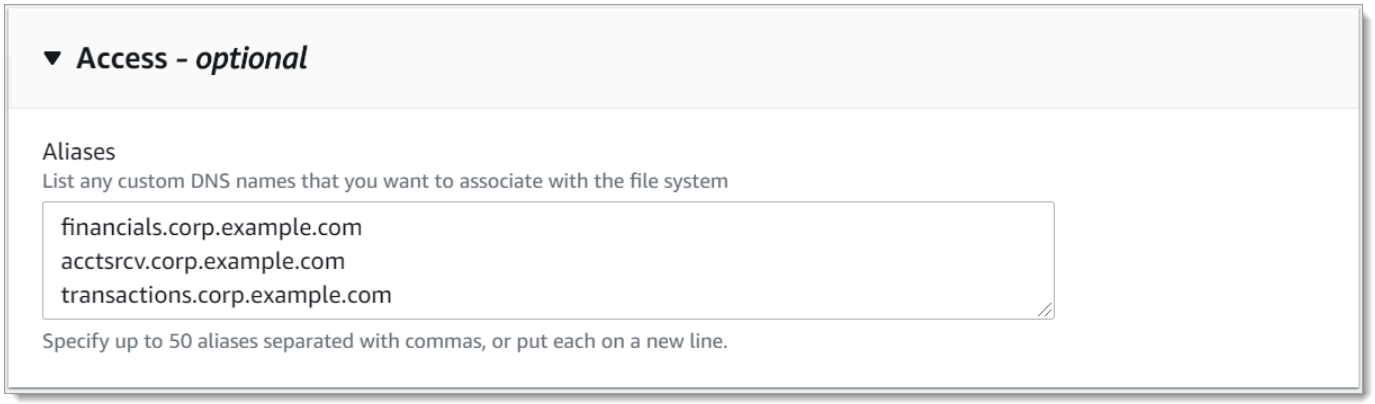
Argomenti

Fase 1: Associare gli alias DNS al file system Amazon FSx

Puoi associare gli alias DNS ai file system FSx for Windows File Server esistenti, quando crei nuovi file system e quando crei un nuovo file system da un backup utilizzando la console, la CLI e l'API di Amazon FSx. Se stai creando un alias con un nome di dominio diverso, inserisci il nome completo, incluso il dominio principale, per associare un alias.

Questa procedura descrive come associare gli alias DNS durante la creazione di un nuovo file system utilizzando la console Amazon FSx. Per informazioni sull'associazione degli alias DNS ai file system esistenti e dettagli sull'utilizzo della CLI e dell'API, consulta. Gestione degli alias DNS

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Segui la procedura per creare un nuovo file system come descritto nella Crea il tuo file system sezione Guida introduttiva.
3. Nella sezione Accesso - opzionale della procedura guidata per la creazione del file system, inserite gli alias DNS che desiderate associare al file system.



Utilizza le seguenti linee guida per specificare gli alias DNS:

- Deve essere formattato come nome di dominio completo (FQDN), ad esempio. *hostname.domain* `accounting.example.com`
- Può contenere caratteri alfanumerici e trattini (-).
- Non può iniziare o terminare con un trattino (-).
- Può iniziare con un numerico.

Per i nomi alias DNS, Amazon FSx archivia i caratteri alfabetici come lettere minuscole (a-z), indipendentemente dal modo in cui li specifichi: come lettere maiuscole, minuscole o lettere corrispondenti in codici di escape.

4. Per le preferenze di manutenzione, apportate le modifiche desiderate.
5. Nella sezione Tag, facoltativa, aggiungi i tag di cui hai bisogno, quindi scegli Avanti.
6. Rivedi la configurazione del file system riportata nella pagina Crea file system. Scegli Crea file system per creare il file system.

   Quando il nuovo file system diventa disponibile, continua con il passaggio 2.

Passaggio 2: Configurazione dei nomi principali di servizio (SPN) per Kerberos

Ti consigliamo di utilizzare l'autenticazione e la crittografia basate su Kerberos in transito con Amazon FSx. Kerberos fornisce l'autenticazione più sicura per i client che accedono al file system.

Per abilitare l'autenticazione Kerberos per i client che accedono ad Amazon FSx utilizzando un alias DNS, devi aggiungere nomi principali di servizio (SPN) che corrispondono all'alias DNS sull'oggetto

computer Active Directory del tuo file system Amazon FSx. Un SPN può essere associato solo a un singolo oggetto informatico Active Directory alla volta. Se disponi di SPN esistenti per il nome DNS configurato per l'oggetto computer Active Directory del file system originale, devi prima eliminarli.

Sono necessari due SPN per l'autenticazione Kerberos:

```
HOST/alias
HOST/alias.domain
```

Se l'alias è`finance.domain.com`, i due SPN richiesti sono i seguenti:

```
HOST/finance
HOST/finance.domain.com
```

> **Note**
>
> Dovrai eliminare tutti gli SPN HOST esistenti che corrispondono all'alias DNS sull'oggetto computer Active Directory prima di creare nuovi SPN HOST per l'oggetto computer Active Directory (AD) del tuo file system Amazon FSx. I tentativi di impostare gli SPN per il file system Amazon FSx falliranno se nell'AD esiste un SPN per l'alias DNS.

Le seguenti procedure descrivono come eseguire le seguenti operazioni:

- Trova tutti gli alias DNS SPN esistenti nell'oggetto computer Active Directory del file system originale.
- Elimina gli SPN esistenti trovati, se presenti.
- Crea nuovi alias DNS SPN per l'oggetto computer Active Directory del tuo file system Amazon FSx.

Per installare il modulo Active Directory richiesto PowerShell

1. Accedi a un'istanza Windows aggiunta all'Active Directory a cui è unito il tuo file system Amazon FSx.
2. Apri PowerShell come amministratore.
3. Installa il modulo PowerShell Active Directory utilizzando il seguente comando.

   ```
   Install-WindowsFeature RSAT-AD-PowerShell
   ```

Per trovare ed eliminare gli alias DNS esistenti, SPN sull'oggetto computer Active Directory del file system originale

1. Trova tutti gli SPN esistenti utilizzando i seguenti comandi. Sostituiscilo *alias_fqdn* con l'alias DNS associato al file system nel passaggio 1.

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. Eliminare gli SPN HOST esistenti restituiti nel passaggio precedente utilizzando lo script di esempio seguente.

   - Sostituiscilo *alias_fqdn* con l'alias DNS completo associato al file system nel passaggio 1.
   - Sostituire *file_system_DNS_name* con il nome DNS del file system originale.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. Ripeti i passaggi precedenti per ogni alias DNS associato al file system nel passaggio 1.

Per impostare gli SPN sull'oggetto computer Active Directory del tuo file system Amazon FSx

1. Imposta nuovi SPN per il tuo file system Amazon FSx eseguendo i seguenti comandi.

   - Sostituisci *file_system_DNS_name* con il nome DNS assegnato da Amazon FSx al file system.

     Per trovare il nome DNS del tuo file system sulla console Amazon FSx, scegli File system, scegli il tuo file system, quindi scegli il pannello Rete e sicurezza nella pagina dei dettagli del file system.

Puoi anche ottenere il nome DNS nella risposta dell'operazione DescribeFileSystems API.

- Sostituiscilo *alias_fqdn* con l'alias DNS completo associato al file system nel passaggio 1.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

##Use one of the following commands, not both:
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
##Or
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> L'impostazione di un SPN per il file system Amazon FSx avrà esito negativo se nell'AD per l'oggetto computer del file system originale esiste un SPN per l'alias DNS. Per informazioni su come trovare ed eliminare gli SPN esistenti, consulta. Per trovare ed eliminare gli alias DNS esistenti, SPN sull'oggetto computer Active Directory del file system originale

2. Verifica che i nuovi SPN siano configurati per l'alias DNS utilizzando lo script di esempio seguente. Assicurati che la risposta includa due HOST SPN `HOST/`*alias* e`HOST/`*alias_fqdn*, come descritto in precedenza in questa procedura.

   Sostituisci *file_system_DNS_name* con il nome DNS assegnato da Amazon FSx al tuo file system. Per trovare il nome DNS del tuo file system sulla console Amazon FSx, scegli File system, scegli il tuo file system, quindi scegli il pannello Rete e sicurezza nella pagina dei dettagli del file system.

   Puoi anche ottenere il nome DNS nella risposta dell'operazione DescribeFileSystems API.

```
## Verify SPNs on FSx file system AD computer object
$FileSystemDnsName = "file_system_dns_name"
```

```
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${FSxAdComputer}.Name
```

3. Ripeti i passaggi precedenti per ogni alias DNS associato al file system nel passaggio 1.

Per informazioni su come imporre ai client di utilizzare l'autenticazione e la crittografia Kerberos durante la connessione al file system Amazon FSx, consulta. Applicazione dell'autenticazione Kerberos tramite GPO

Passaggio 3: Aggiornare o creare un record DNS CNAME per il file system

Dopo aver configurato correttamente gli SPN per il tuo file system, puoi passare ad Amazon FSx sostituendo ogni record DNS risolto nel file system originale con un record DNS che si risolve nel nome DNS predefinito del file system Amazon FSx.

I moduli `dnsserver` e `activedirectory` Windows sono necessari per eseguire i comandi presentati in questa sezione.

Per installare i PowerShell cmdlet richiesti

1. Accedi a un'istanza Windows aggiunta ad Active Directory a cui fa parte il tuo file system Amazon FSx come utente membro di un gruppo con autorizzazioni di amministrazione DNS (AWSAWS Delegated Domain Name System Administrators in AWS Managed Active Directory e Domain Admins o un altro gruppo a cui hai delegato le autorizzazioni di amministrazione DNS nella tua Active Directory autogestita).

   Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
2. Apri PowerShell come amministratore.
3. Il modulo PowerShell DNS Server è necessario per eseguire le istruzioni di questa procedura. Installarlo utilizzando il seguente comando.

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

Per aggiornare o creare un nome DNS personalizzato per il file system Amazon FSx

1. Connect alla tua istanza Amazon EC2 come utente membro di un gruppo con autorizzazioni di amministrazione DNS (AWS Delegated Domain Name System Administrators in AWS Managed Active Directory e Domain Admins o un altro gruppo a cui hai delegato le autorizzazioni di amministrazione DNS nella tua Active Directory autogestita).

   Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.

2. Al prompt dei comandi, esegui lo script seguente. Questo script migra qualsiasi record DNS CNAME esistente sul file system Amazon FSx. Se non ne viene trovato nessuno, crea un nuovo record DNS CNAME per l'alias DNS *alias_fqdn* che si risolve nel nome DNS predefinito per il file system Amazon FSx.

   Per eseguire lo script:

   - Sostituiscilo *alias_fqdn* con l'alias DNS associato al file system.
   - Sostituisci *file_system_DNS_name* con il nome DNS che Amazon FSx ha assegnato al file system.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name) | Select -First 1
foreach ($computer in $DnsServerComputerName)
{
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName $computer -
HostNameAlias $FSxDnsName -ZoneName $ZoneName
}
```

3. Ripeti il passaggio precedente per ogni alias DNS associato al file system nel passaggio 1.

Ora hai aggiunto un valore DNS CNAME per il tuo file system Amazon FSx con l'alias DNS. Ora puoi usare l'alias DNS per accedere ai tuoi dati.

> **Note**
>
> Quando si aggiorna un record DNS CNAME in modo che punti a un file system Amazon FSx precedentemente indirizzato a un altro file system, i client potrebbero non essere in grado di connettersi al file system per un breve periodo di tempo. Quando la cache DNS del client si aggiorna, dovrebbero essere in grado di connettersi utilizzando l'alias DNS. Per ulteriori informazioni, consulta Impossibile accedere al file system utilizzando un alias DNS.

Applicazione dell'autenticazione Kerberos tramite GPO

È possibile applicare l'autenticazione Kerberos quando si accede al file system impostando i seguenti Group Policy Object (GPO) in Active Directory:

- Limita NTLM: traffico NTLM in uscita verso server remoti: utilizza questa impostazione dei criteri per negare o controllare il traffico NTLM in uscita da un computer a qualsiasi server remoto che esegue il sistema operativo Windows.
- Limita NTLM: aggiungi eccezioni del server remoto per l'autenticazione NTLM: utilizza questa impostazione dei criteri per creare un elenco di eccezioni di server remoti su cui i dispositivi client possono utilizzare l'autenticazione NTLM se è configurata l'impostazione del criterio Sicurezza di rete: Limita il traffico NTLM: traffico NTLM in uscita ai server remoti.

1. Accedi a un'istanza Windows aggiunta ad Active Directory a cui è collegato il tuo file system Amazon FSx come amministratore. Se stai configurando un Active Directory autogestito, applica questi passaggi direttamente ad Active Directory.
2. Scegliete Start, scegliete Strumenti di amministrazione, quindi scegliete Gestione delle politiche di gruppo.
3. Scegliete Oggetti di policy di gruppo.
4. Se il tuo oggetto Group Policy non esiste già, crealo.
5. Individua la politica esistente Network Security: Limit NTLM: Outgoing NTLM traffic to remote servers. (Se non esiste alcuna politica esistente, crea una nuova politica.) Nella scheda Impostazioni di sicurezza locali, apri il menu contestuale (fai clic con il pulsante destro del mouse) e scegli Proprietà.
6. Scegli Nega tutto.
7. Scegli Applica per salvare l'impostazione di sicurezza.

8. Per impostare eccezioni per le connessioni NTLM a server remoti specifici per il client, individua l'opzione Sicurezza di rete: Limita NTLM: Aggiungi eccezioni al server remoto.

   Apri il menu contestuale (fai clic con il pulsante destro del mouse) e scegli Proprietà nella scheda Impostazioni di sicurezza locale.

9. Immettete i nomi di tutti i server da aggiungere all'elenco delle eccezioni.
10. Scegli Applica per salvare l'impostazione di sicurezza.

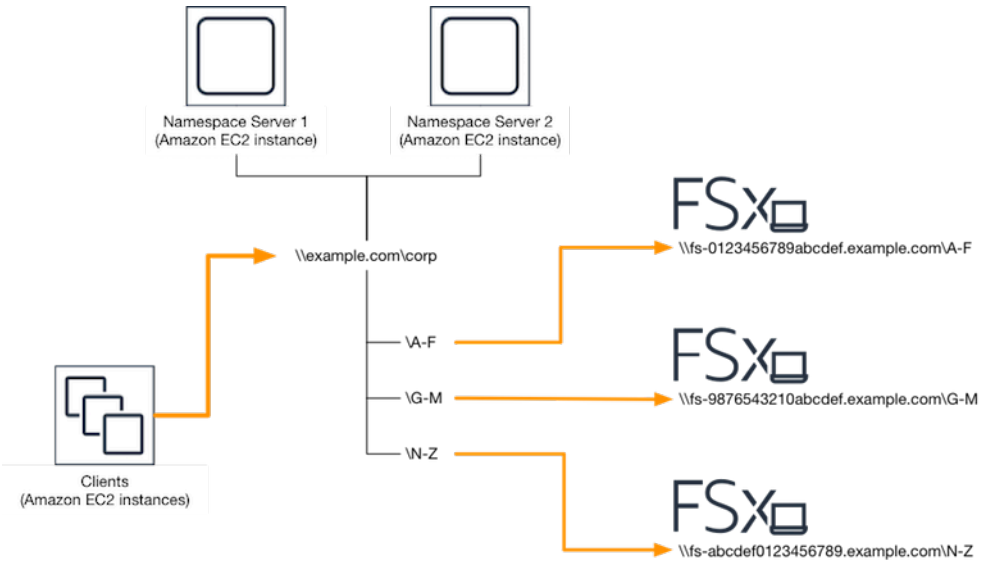
Procedura dettagliata 6: Ridimensionamento delle prestazioni con gli shard

Amazon FSx for Windows File Server supporta l'uso del Microsoft Distributed File System (DFS). Utilizzando DFS Namespaces, puoi scalare le prestazioni (sia in lettura che in scrittura) per gestire carichi di lavoro a uso intensivo di I/O distribuendo i dati dei file su più file system Amazon FSx. Allo stesso tempo, puoi comunque presentare alle tue applicazioni una vista unificata sotto un namespace comune. Questa soluzione prevede la suddivisione dei dati dei file in set di dati o frammenti più piccoli e la loro memorizzazione su file system diversi. Le applicazioni che accedono ai dati da più istanze possono raggiungere livelli di prestazioni elevati leggendo e scrivendo su questi shard in parallelo.

È possibile utilizzare questa soluzione quando il carico di lavoro richiede un accesso in lettura/scrittura distribuito in modo uniforme ai dati dei file (ad esempio, se ogni sottoinsieme di istanze di calcolo accede a una parte diversa dei dati del file).

Configurazione dei namespace DFS per prestazioni di scalabilità orizzontale

La seguente procedura ti guida nella creazione di una soluzione DFS su Amazon FSx per prestazioni scalabili. In questo esempio, i dati archiviati nel namespace aziendale vengono suddivisi *`alfabeticamente.`* I file di dati 'A-F', 'G-M' e 'N-Z' sono tutti archiviati su diverse condivisioni di file. In base al tipo di dati, alla dimensione di I/O e al modello di accesso I/O, è necessario decidere come condividere al meglio i dati tra più condivisioni di file. Scegliete una convenzione di sharding che distribuisca l'I/O in modo uniforme su tutte le condivisioni di file che intendete utilizzare. Tieni presente che ogni namespace supporta fino a 50.000 condivisioni di file e centinaia di petabyte di capacità di storage in totale.



Per configurare i namespace DFS per prestazioni di scalabilità orizzontale

1. Se non disponi già di server DFS Namespace in esecuzione, puoi avviare un paio di server DFS Namespace ad alta disponibilità utilizzando il modello Setup-DFSN-Servers.template. AWS CloudFormation Per ulteriori informazioni sulla creazione di uno stack, consulta la sezione Creazione di uno stack sulla console nella Guida per l'utente. AWS CloudFormation AWS CloudFormation AWS CloudFormation
2. Connect a uno dei server DFS Namespace avviati nel passaggio precedente come utente del gruppo AWS Delegated Administrators. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
3. Accedi alla console di gestione DFS. Apri il menu Start ed esegui dfsmgmt.msc. Si apre lo strumento DFS Management GUI.
4. Scegli Azione, quindi Nuovo spazio dei nomi, digita il nome del computer del primo server DFS Namespace che hai avviato per Server e scegli Avanti.
5. Per Nome, digita lo spazio dei nomi che stai creando (ad esempio, corp).
6. Scegli Modifica impostazioni e imposta le autorizzazioni appropriate in base alle tue esigenze. Seleziona Successivo.
7. Lasciate selezionata l'opzione predefinita dello spazio dei nomi basato sul dominio, lasciate selezionata l'opzione Abilita la modalità Windows Server 2008 e scegliete Avanti.

> **Note**
>
> La modalità Windows Server 2008 è l'ultima opzione disponibile per i namespace.

8. Controlla le impostazioni del namespace e scegli Crea.
9. Con lo spazio dei nomi appena creato selezionato in Namespace nella barra di navigazione, scegli Azione, quindi Aggiungi server dello spazio dei nomi.
10. Digita il nome del computer del secondo server DFS Namespace che hai avviato per il server Namespace.
11. Scegliete Modifica impostazioni, impostate le autorizzazioni appropriate in base ai vostri requisiti e scegliete OK.
12. Apri il menu contestuale (fai clic con il pulsante destro del mouse) per lo spazio dei nomi appena creato, scegli Nuova cartella, inserisci il nome della cartella per il primo shard (ad esempio, **`A-F`** per Nome) e scegli Aggiungi.
13. Digita il nome DNS della condivisione di file che ospita questo shard in formato UNC (ad esempio,**`\\fs-0123456789abcdef0.example.com\A-F`**) per Path to folder target e scegli OK.
14. Se la condivisione non esiste:
    a. Scegli Sì per crearla.
    b. Nella finestra di dialogo Crea condivisione, scegli Sfoglia.
    c. Scegliete una cartella esistente o create una nuova cartella in D$ e scegliete OK.
    d. Imposta le autorizzazioni di condivisione appropriate e scegli OK.
15. Ora che la destinazione della cartella è stata aggiunta allo shard, scegliete OK.
16. Ripeti gli ultimi quattro passaggi per gli altri shard che desideri aggiungere allo stesso namespace.

Procedura guidata 7: Copia di un backup in un altroRegione AWS

Con Amazon FSx, puoi copiare un backup esistente all'interno dello stessoAccount AWSa un altroRegione AWS(copia di backup su più regioni) o allo stesso modoRegione AWS(copia di backup nella regione).

La procedura seguente ti guiderà attraverso il processo di creazione di una copia di un backup all'interno della stessaAccount AWS. Prima di poter creare questa copia di backup, è necessario disporre di un backup esistente. Per ulteriori informazioni, consulta la pagina Utilizzo dei backup .

Copia di un backup esistente all'interno dello stessoAccount AWS(tra regioni o in regione)

1. Apri la console Amazon FSx all'indirizzohttps://console.aws.amazon.com/fsx/.
2. Nel pannello di navigazione, scegliere Backups (Backup).
3. NellaBackup, scegliere il backup da copiare.
4. Scegli Copy backup (Copia backup). Così facendo apre ilCopia di backupmago.
5. NellaRegione di destinazionelista, scegli una destinazioneRegione AWSper copiare il backup in. La destinazione può essere in un'altraRegione AWSo all'interno dello stessoRegione AWS.
6. (Facoltativo) SelezionaCopia di tagper copiare i tag dal backup di origine al backup di destinazione. Se selezioniCopia di tage aggiungi anche tag al passaggio 8, tutti i tag vengono uniti.
7. PerCrittografia, scegli ilAWS KMSchiave di crittografia per crittografare il backup copiato.
8. PerTags - opzionale, immettere una chiave e un valore per aggiungere tag per il backup copiato. Se aggiungi tag qui e anche selezionatoCopia di tagal passaggio 6, tutti i tag vengono uniti.
9. Scegli Copy backup (Copia backup).

Ora hai copiato con successo un backup all'interno dello stessoAccount AWSa un altroRegione AWSo all'interno dello stessoRegione AWS.

Sicurezza in Amazon FSx

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Amazon Web Services Cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei programmi di conformitàAWS. Per informazioni sui programmi di conformità applicabili ad Amazon FSx for Windows File Server, AWS consulta Services in Scope by Compliance Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon FSx for Windows File Server. I seguenti argomenti mostrano come configurare Amazon FSx per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon FSx for Windows File Server.

Argomenti

Crittografia dei dati in Amazon FSx

Amazon FSx for Windows File Server supporta due forme di crittografia per i file system, la crittografia dei dati in transito e la crittografia a riposo. La crittografia dei dati in transito è supportata su condivisioni di file mappate su un'istanza di calcolo che supporta il protocollo SMB 3.0 o successivo. La crittografia dei dati inattivi viene abilitata automaticamente durante la creazione di un file system Amazon FSx. Amazon FSx crittografa automaticamente i dati in transito utilizzando la crittografia SMB quando accedi al file system senza la necessità di modificare le applicazioni.

Quando usare la crittografia

Se la propria azienda è soggetto a politiche aziendali o normative che richiedono la crittografia dei dati e dei metadati memorizzati su disco, consigliamo di creare un file system crittografato montando il file system utilizzando la crittografia dei dati in transito.

Per ulteriori informazioni sulla crittografia con Amazon FSx for Windows File Server, consulta questi argomenti correlati:

- Crea il tuo file system Amazon FSx for Windows File Server
- Azioni, risorse e chiavi di condizione per Amazon FSx nella IAM User Guide

Argomenti

Crittografia dei dati inattivi

Tutti i file system Amazon FSx sono crittografati quando sono inattivi con chiavi gestite tramite AWS Key Management Service ()AWS KMS. I dati vengono crittografati automaticamente prima di essere scritti nel file system e decrittografati automaticamente durante la lettura. Questi processi sono gestiti in modo trasparente da Amazon FSx, quindi non è necessario modificare le applicazioni.

Amazon FSx utilizza un algoritmo di crittografia AES-256 standard di settore per crittografare dati e metadati Amazon FSx a riposo. Per ulteriori informazioni, consulta Elementi di base di crittografia nella Guida per sviluppatori di AWS Key Management Service .

> **Note**
>
> L'infrastruttura di gestione delle AWS chiavi utilizza algoritmi crittografici approvati dal Federal Information Processing Standards (FIPS) 140-2. L'infrastruttura è compatibile con le raccomandazioni National Institute of Standards and Technology (NIST) 800-57.

Come utilizza Amazon FSx AWS KMS

Amazon FSx si integra con AWS KMS per la gestione delle chiavi. Amazon FSx utilizza an AWS KMS key per crittografare il file system. Scegli la chiave KMS utilizzata per crittografare e decrittografare i file system (dati e metadati). Puoi abilitare, disabilitare o revocare le concessioni su questa chiave KMS. Questa chiave KMS può essere di uno dei due tipi seguenti:

- Chiave gestita da AWS— Questa è la chiave KMS predefinita ed è gratuita.
- Chiave gestita dal cliente – Questa è la chiave KMS più flessibile da usare, perché è possibile configurare le policy della chiave e i permessi per più utenti o servizi. Per ulteriori informazioni sulla creazione di chiavi gestite dai clienti, consulta Creating keys nella AWS Key Management Service Developer Guide.

Se utilizzi una chiave gestita dal cliente come chiave KMS per la crittografia e la decrittografia dei dati dei file, puoi abilitare la rotazione delle chiavi. Quando si abilita la rotazione delle chiavi, AWS KMS fa ruotare automaticamente la chiave una volta all'anno. Inoltre, con una chiave gestita dal cliente, puoi scegliere quando disabilitare, riattivare, eliminare o revocare l'accesso alla tua chiave KMS in qualsiasi momento. Per ulteriori informazioni, consulta Rotating AWS KMS keys nella Developer Guide. AWS Key Management Service

La crittografia e la decrittografia dei file system inattivi vengono gestite in modo trasparente. Tuttavia, Account AWS gli ID specifici di Amazon FSx vengono visualizzati nei AWS CloudTrail log relativi alle azioni. AWS KMS

Politiche chiave di Amazon FSx per AWS KMS

Le policy chiave sono lo strumento principale per controllare l'accesso alle chiavi KMS. Per ulteriori informazioni sulle politiche chiave, consulta Using key policy AWS KMS nella AWS Key Management Service Developer Guide.L'elenco seguente descrive tutte le autorizzazioni AWS KMS correlate supportate da Amazon FSx per i file system crittografati a riposo:

- kms:Encrypt - (Facoltativa) Crittografa testo normale in testo criptato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms:Decrypt - (Obbligatoria) Decifra il testo criptato. Il testo cifrato è un testo normale che è stato precedentemente crittografato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: ReEncrypt — (Facoltativo) Crittografa i dati sul lato server con una nuova chiave KMS, senza esporre il testo in chiaro dei dati sul lato client. I dati sono prima decifrati e quindi nuovamente crittografati. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: GenerateData KeyWithout Plaintext — (Obbligatorio) Restituisce una chiave di crittografia dei dati crittografata con una chiave KMS. Questa autorizzazione è inclusa nella politica delle chiavi predefinita in kms: Key*. GenerateData
- kms: CreateGrant — (Obbligatorio) Aggiunge una concessione a una chiave per specificare chi può utilizzare la chiave e in quali condizioni. I grant sono meccanismi di autorizzazioni alternative alle policy sulle chiavi. Per ulteriori informazioni sulle sovvenzioni, consulta Using grants nella Developer Guide.AWS Key Management Service Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: DescribeKey — (Obbligatorio) Fornisce informazioni dettagliate sulla chiave KMS specificata. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: ListAliases — (Facoltativo) Elenca tutti gli alias chiave dell'account. Quando usi la console per creare un file system crittografato, questa autorizzazione compila l'elenco delle chiavi KMS. Consigliamo di usare questa autorizzazione per garantire la migliore esperienza utente. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

Crittografia in transito

La crittografia dei dati in transito è supportata sulle condivisioni di file mappate su un'istanza di calcolo che supporta il protocollo SMB 3.0 o versioni successive. Ciò include tutte le versioni di Windows a partire da Windows Server 2012 e Windows 8 e tutti i client Linux con client Samba versione 4.2 o successiva. Amazon FSx for Windows File Server crittografa automaticamente i dati in transito utilizzando la crittografia SMB quando accedi al file system senza la necessità di modificare le applicazioni.

La crittografia SMB utilizza AES-128-GCM o AES-128-CCM (con la variante GCM scelta se il client supporta SMB 3.1.1) come algoritmo di crittografia e fornisce inoltre l'integrità dei dati con la firma tramite chiavi di sessione Kerberos SMB. L'uso di AES-128-GCM porta a prestazioni migliori, ad esempio, fino a 2 volte superiori quando si copiano file di grandi dimensioni su connessioni SMB crittografate.

Per soddisfare i requisiti di conformità per la crittografia continua data-in-transit, è possibile limitare l'accesso al file system in modo da consentire l'accesso solo ai client che supportano la crittografia SMB. È inoltre possibile abilitare o disabilitare la crittografia in transito per ogni condivisione di file o per l'intero file system. Ciò consente di disporre di una combinazione di condivisioni di file crittografate e non crittografate sullo stesso file system. Per ulteriori informazioni encryption-in-transit sulla gestione del file system, consultaGestione della crittografia in transito.

Controllo degli accessi a livello di file e cartella tramite ACL di Windows

Amazon FSx for Windows File Server supporta l'autenticazione basata sull'identità tramite il protocollo Server Message Block (SMB) tramite Microsoft Active Directory. Active Directory è il servizio di directory di Microsoft che consente di archiviare informazioni sugli oggetti presenti in rete e di semplificare la ricerca e l'utilizzo di tali informazioni da parte di amministratori e utenti. Questi oggetti includono in genere risorse condivise come file server e account di utenti e computer di rete. Per ulteriori informazioni sul supporto di Active Directory in Amazon FSx, consulta. Utilizzo di Microsoft Active Directory in FSx for Windows File Server

Le istanze di calcolo aggiunte al dominio possono accedere alle condivisioni di file Amazon FSx utilizzando le credenziali di Active Directory. Utilizzi elenchi di controllo degli accessi (ACL) standard di Windows per un controllo granulare degli accessi a livello di file e cartelle. I file system Amazon FSx verificano automaticamente le credenziali degli utenti che accedono ai dati del file system per applicare questi ACL di Windows.

Ogni file system Amazon FSx è dotato di una condivisione di file Windows predefinita denominata. `share` Gli ACL di Windows per questa cartella condivisa sono configurati per consentire l'accesso in lettura/scrittura agli utenti del dominio. Consentono inoltre il pieno controllo al gruppo di amministratori delegati di Active Directory, incaricato di eseguire azioni amministrative sui file system. Se state integrando il vostro file system con AWS Managed Microsoft AD, questo gruppo è costituito da AWS Delegated FSx Administrators. Se stai integrando il tuo file system con la configurazione autogestita di Microsoft AD, questo gruppo può essere Domain Admins. Oppure può essere un gruppo di amministratori delegati personalizzato specificato durante la creazione del file system. Per modificare gli ACL, puoi mappare la condivisione come utente membro del gruppo di amministratori delegati.

> **Warning**
>
> Amazon FSx richiede che l'utente SYSTEM disponga delle autorizzazioni ACL NTFS Full control su tutte le cartelle all'interno del file system. Non modificare le autorizzazioni NTFS ACL per questo utente sulle tue cartelle. In questo modo si può rendere inaccessibile la condivisione di file e impedire l'utilizzo dei backup del file system.

Collegamenti correlati

- Che cos'è il AWS Directory Service? nella Guida all' AWS Directory Service amministrazione.
- Crea la tua directory AWS Managed Microsoft AD nella AWS Directory Service Administration Guide.
- Quando creare una relazione di fiducia nella Guida all'AWS Directory Service amministrazione.
- Procedura guidata 1: Prerequisiti per iniziare.

Controllo degli accessi ai file system con Amazon VPC

È possibile accedere al file system Amazon FSx tramite un'interfaccia di rete elastica. Questa interfaccia di rete risiede nel cloud privato virtuale (VPC) basato sul servizio Amazon Virtual Private Cloud (Amazon VPC) che associ al tuo file system. Ti connetti al tuo file system Amazon FSx tramite il nome DNS (Domain Name Service). Il nome DNS viene mappato all'indirizzo IP privato dell'interfaccia di rete elastica del file system nel tuo VPC. Solo le risorse all'interno del VPC associato, le risorse collegate al VPC associato tramite AWS Direct Connect o VPN o le risorse all'interno di VPC peerizzati possono accedere all'interfaccia di rete del file system. 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.

FSx for Windows File Server supporta la condivisione VPC, che consente di visualizzare, creare, modificare ed eliminare risorse in una sottorete condivisa in un VPC di proprietà di un altro account. AWS Per ulteriori informazioni, consulta Utilizzo dei VPC condivisi nella Guida per l'utente di Amazon VPC.

Gruppi di sicurezza Amazon VPC

Per controllare ulteriormente il traffico di rete che attraversa le interfacce di rete elastiche del file system all'interno del VPC, utilizza i gruppi di sicurezza per limitare l'accesso ai file system. Un gruppo di sicurezza è un firewall a stato che controlla il traffico da e verso le interfacce di rete associate. In questo caso, la risorsa associata sono le interfacce di rete del file system.

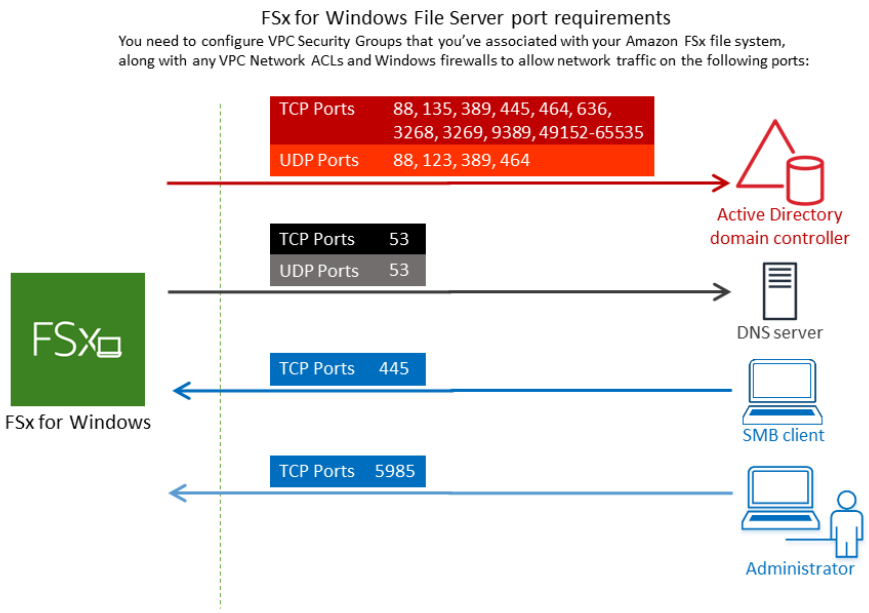
Per utilizzare un gruppo di sicurezza per controllare l'accesso al file system Amazon FSx, aggiungi regole in entrata e in uscita. Le regole in entrata controllano il traffico in entrata e le regole in uscita controllano il traffico in uscita dal tuo file system. Assicurati di avere le regole del traffico di rete corrette nel tuo gruppo di sicurezza per mappare la condivisione di file del tuo file system Amazon FSx su una cartella sull'istanza di calcolo supportata.

Per ulteriori informazioni sulle regole dei gruppi di sicurezza, consulta le regole del gruppo di sicurezza nella Guida per l'utente di Amazon EC2.

Per creare un gruppo di sicurezza per Amazon FSx

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2.
2. Fare clic su Security Groups (Gruppi di sicurezza) nel pannello di navigazione.
3. Scegliere Create Security Group (Crea un gruppo di sicurezza).
4. Specificare un nome e una descrizione per il gruppo di sicurezza.
5. Per VPC, scegli Amazon VPC associato al tuo file system per creare il gruppo di sicurezza all'interno di quel VPC.
6. Aggiungi le seguenti regole per consentire il traffico di rete in uscita sulle seguenti porte:

    a. Per i gruppi di sicurezza VPC, il gruppo di sicurezza predefinito per il tuo Amazon VPC predefinito è già aggiunto al file system nella console. Assicurati che il gruppo di sicurezza e gli ACL di rete VPC per le sottoreti in cui stai creando il file system FSx consentano il traffico sulle porte e nelle direzioni mostrate nel diagramma seguente.



Nella tabella seguente è indicato il ruolo di ciascuna porta.

Protocollo	Porte	Ruolo
TCP/UDP	53	Domain Name System (DNS)
TCP/UDP	88	Autenticazione Kerberos
TCP/UDP	464	Modifica/reimpostazione della password
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)
UDP	123	Network Time Protocol (NTP)
TCP	135	Distributed Computing Environment/End Point Mapper (DCE/EPMAP)
TCP	445	Condivisione di file SMB di Servizi directory
TCP	636	Lightweight Directory Access Protocol su TLS/SSL (LDAPS)

Protocollo	Porte	Ruolo
TCP	3268	Catalogo globale Microsoft
TCP	3269	Microsoft Global Catalog tramite SSL
TCP	5985	WinRM 2.0 (gestione remota di Microsoft Windows)
TCP	9389	Servizi Web Microsoft AD DS, PowerShell
TCP	49152 - 65535	Porte effimere per RPC

> **Important**
>
> L'autorizzazione del traffico in uscita sulla porta TCP 9389 è necessaria per le implementazioni di file system Single-AZ 2 e Multi-AZ.

b. Assicurati che queste regole del traffico siano rispecchiate anche sui firewall che si applicano a ciascuno dei controller di dominio AD, server DNS, client FSx e amministratori FSx.

> **Important**
>
> Sebbene i gruppi di sicurezza Amazon VPC richiedano l'apertura delle porte solo nella direzione di avvio del traffico di rete, la maggior parte dei firewall Windows e degli ACL di rete VPC richiedono che le porte siano aperte in entrambe le direzioni.

> **Note**
>
> Se hai definito siti Active Directory, devi assicurarti che le sottoreti nel VPC associato al tuo file system Amazon FSx siano definite in un sito Active Directory e che non esistano conflitti tra le sottoreti del tuo VPC e le sottoreti negli altri siti. È possibile visualizzare e modificare queste impostazioni utilizzando lo snap-in MMC di Active Directory Sites and Services.

> **Note**
>
> In alcuni casi, è possibile che le regole del gruppo di AWS Managed Microsoft AD sicurezza siano state modificate rispetto alle impostazioni predefinite. In tal caso, assicurati che questo gruppo di sicurezza disponga delle regole in entrata necessarie per consentire il traffico proveniente dal tuo file system Amazon FSx. Per ulteriori informazioni sulle regole in entrata richieste, consulta AWS Managed Microsoft AD Prerequisiti nella Guida all'amministrazione.AWS Directory Service

Ora che hai creato il tuo gruppo di sicurezza, puoi associarlo alle interfacce di rete elastiche del tuo file system Amazon FSx.

Per associare un gruppo di sicurezza al tuo file system Amazon FSx

1. Apri la console Amazon FSx all'indirizzo https://console.aws.amazon.com/fsx/.
2. Nella dashboard, scegli il tuo file system per visualizzarne i dettagli.
3. Scegli la scheda Rete e sicurezza e scegli le interfacce di rete del tuo file system, ad esempio ENI-01234567890123456. Per i file system Single-AZ, vedrai un'unica interfaccia di rete. Per i file system Multi-AZ, vedrete un'interfaccia di rete nella sottorete Preferred e una nella sottorete Standby.
4. Per ogni interfaccia di rete, scegli l'interfaccia di rete e in Azioni, scegli Cambia gruppi di sicurezza.
5. Nella finestra di dialogo Modifica gruppi di sicurezza, scegli i gruppi di sicurezza da utilizzare e scegli Salva.

Impedisci l'accesso a un file system

Per impedire temporaneamente l'accesso di rete al file system da parte di tutti i client, è possibile rimuovere tutti i gruppi di sicurezza associati alle elastic network interface del file system e sostituirli con un gruppo privo di regole in entrata/in uscita.

ACL di rete Amazon VPC

Un'altra opzione per proteggere l'accesso al file system all'interno del VPC consiste nello stabilire elenchi di controllo degli accessi alla rete (ACL di rete). Gli ACL di rete sono separati dai gruppi di

sicurezza, ma hanno funzionalità simili per aggiungere un ulteriore livello di sicurezza alle risorse del tuo VPC. Per ulteriori informazioni sugli ACL di rete, consulta gli ACL di rete nella Amazon VPC User Guide.

Identity and Access Management per Amazon FSx for Windows File Server

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Amazon FSx. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon FSx.

Utente del servizio: se utilizzi il servizio Amazon FSx per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Amazon FSx per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La

comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Amazon FSx, consulta. Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon FSx for Windows File Server

Amministratore del servizio: se sei responsabile delle risorse Amazon FSx della tua azienda, probabilmente hai pieno accesso ad Amazon FSx. È tuo compito determinare a quali funzionalità e risorse di Amazon FSx devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon FSx, consulta. Come funziona Amazon FSx for Windows File Server con IAM

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso ad Amazon FSx. Per visualizzare esempi di policy basate sull'identità di Amazon FSx che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Amazon FSx for Windows File Server

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWSaccesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conserva le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le

chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato Amministratori IAM e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.

- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM assunto da un servizio per eseguire operazioni per conto dell'utente. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori

informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono incorporate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo

Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.

- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon FSx for Windows File Server 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 Windows File Server

Funzionalità IAM	Supporto FSx
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì

Funzionalità IAM	Supporto FSx
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Sessioni di accesso diretto	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come FSx e AWS altri servizi funzionano con la maggior parte delle funzionalità IAM, AWS consulta i servizi che funzionano con IAM nella IAM User Guide.

Policy basate sull'identità per FSx

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate sull'identità per FSx

Per visualizzare esempi di policy basate sull'identità di Amazon FSx, consulta. Esempi di policy basate sull'identità per Amazon FSx for Windows File Server

Policy basate sulle risorse all'interno di FSx

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile allegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è allegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per FSx

Supporta le azioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a una policy. Le azioni politiche in genere hanno lo stesso nome dell'operazione

AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di azioni FSx, consulta Actions defined by Amazon FSx for Windows File Server nel Service Authorization Reference.

Le azioni politiche in FSx utilizzano il seguente prefisso prima dell'azione:

```
fsx
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Per visualizzare esempi di policy basate sull'identità di Amazon FSx, consulta. Esempi di policy basate sull'identità per Amazon FSx for Windows File Server

Risorse politiche per FSx

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse FSx e dei relativi ARN, consulta Resources defined by Amazon FSx for Windows File Server nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon FSx for Windows File Server.

Per visualizzare esempi di policy basate sull'identità di Amazon FSx, consulta. Esempi di policy basate sull'identità per Amazon FSx for Windows File Server

Chiavi relative alle condizioni delle policy per FSx

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco di chiavi di condizione FSx, consulta Chiavi di condizione per Amazon FSx for Windows File Server nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta Azioni definite da Amazon FSx for Windows File Server.

Per visualizzare esempi di policy basate sull'identità di Amazon FSx, consulta. Esempi di policy basate sull'identità per Amazon FSx for Windows File Server

ACL in FSx

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con FSx

Supporta ABAC (tag nelle policy)	Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`* o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente 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.

Utilizzo di credenziali temporanee con FSx

Supporta le credenziali temporanee	Sì

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Sessioni di accesso diretto per FSx

Supporta sessioni di accesso diretto (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra azione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le operazioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per FSx

Supporta i ruoli di servizio	No

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità FSx. Modificate i ruoli di servizio solo quando FSx fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per FSx

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per dettagli sulla creazione o la gestione di ruoli collegati ai servizi Amazon FSx, consulta. Utilizzo di ruoli collegati ai servizi per Amazon FSx

Esempi di policy basate sull'identità per Amazon FSx for Windows File Server

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare risorse Amazon FSx. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da FSx, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon FSx for Windows File Server nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console FSx
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le policy basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon FSx nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.

- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente 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, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto 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 console FSx

Per accedere alla console Amazon FSx for Windows File Server, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Amazon FSx presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime di console per gli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la console FSx, allega anche la policy `AmazonFSxConsoleReadOnlyAccess` AWS gestita FSx alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

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 allegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. AWS CLI AWS

```
{
```

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

AWS politiche gestite per Amazon FSx

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 Consigliamo

pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AmazonF SxServiceRolePolicy

Consente ad Amazon FSx di gestire AWS le risorse per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

AWS politica gestita: AmazonF SxDeleteServiceLinkedRoleAccess

Non è possibile collegare `AmazonFSxDeleteServiceLinkedRoleAccess`alle entità IAM. Questa politica è collegata a un servizio e utilizzata solo con il ruolo collegato al servizio per quel servizio. Non è possibile collegare, scollegare, modificare o eliminare questa policy. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

Questa politica concede autorizzazioni amministrative che consentono ad Amazon FSx di eliminare il relativo Service Linked Role per l'accesso ad Amazon S3, utilizzato solo da Amazon FSx for Lustre.

Dettagli dell'autorizzazione

Questa policy include le autorizzazioni `iam` per consentire ad Amazon FSx di visualizzare, eliminare e visualizzare lo stato di eliminazione per gli accessi FSx Service Linked Roles for Amazon S3.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonF SxDeleteServiceLinkedRoleAccess nella Managed Policy Reference Guide. AWS

AWS politica gestita: AmazonF SxFullAccess

Puoi collegare AmazonF alle tue entità IAMSxFullAccess . Amazon FSx associa questa politica anche a un ruolo di servizio che consente ad Amazon FSx di eseguire azioni per tuo conto.

Fornisce accesso completo ad Amazon FSx e accesso ai servizi correlati AWS .

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai responsabili l'accesso completo per eseguire tutte le azioni di Amazon FSx, ad eccezione di. `BypassSnaplockEnterpriseRetention`
- `ds`— Consente ai responsabili di visualizzare le informazioni sulle directory. AWS Directory Service
- `ec2`
  - Consente ai mandanti di creare tag nelle condizioni specificate.
  - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
- `iam`— Consente ai principi di creare un ruolo collegato al servizio Amazon FSx per conto dell'utente. Ciò è necessario affinché Amazon FSx possa gestire AWS le risorse per conto dell'utente.
- `logs`— Consente ai responsabili di creare gruppi di log, flussi di log e scrivere eventi nei flussi di log. Ciò è necessario per consentire agli utenti di monitorare l'accesso al file system di FSx for Windows File Server inviando i log di accesso di controllo a Logs. CloudWatch
- `firehose`— Consente ai mandanti di scrivere record su un Amazon Data Firehose. Ciò è necessario per consentire agli utenti di monitorare l'accesso al file system FSx for Windows File Server inviando i log di accesso di controllo a Firehose.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonF SxFullAccess nella Managed Policy Reference Guide. AWS

AWS politica gestita: AmazonF SxConsoleFullAccess

È possibile allegare la policy `AmazonFSxConsoleFullAccess`alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo ad Amazon FSx e l'accesso ai servizi correlati AWS tramite. AWS Management Console

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai responsabili di eseguire tutte le azioni nella console di gestione Amazon FSx, ad eccezione di. `BypassSnaplockEnterpriseRetention`
- `cloudwatch`— Consente ai responsabili di visualizzare CloudWatch allarmi e metriche nella console di gestione Amazon FSx.
- `ds`— Consente ai responsabili di elencare le informazioni su una directory. AWS Directory Service
- `ec2`
  - Consente ai mandanti di creare tag su tabelle di routing, elencare interfacce di rete, tabelle di routing, gruppi di sicurezza, sottoreti e il VPC associato a un file system Amazon FSx.
  - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
- `kms`— Consente ai principali di elencare gli alias per le chiavi. AWS Key Management Service
- `s3`— Consente ai responsabili di elencare alcuni o tutti gli oggetti in un bucket Amazon S3 (fino a 1000).
- `iam`— Concede l'autorizzazione a creare un ruolo collegato al servizio che consente ad Amazon FSx di eseguire azioni per conto dell'utente.

Per visualizzare le autorizzazioni per questa politica, consulta AmazonF SxConsoleFullAccess nella Managed Policy Reference Guide. AWS

AWS politica gestita: AmazonF SxConsoleReadOnlyAccess

È possibile allegare la policy `AmazonFSxConsoleReadOnlyAccess`alle identità IAM.

Questa politica concede autorizzazioni di sola lettura ad Amazon FSx e AWS ai servizi correlati in modo che gli utenti possano visualizzare le informazioni su questi servizi in. AWS Management Console

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai responsabili di visualizzare le informazioni sui file system Amazon FSx, inclusi tutti i tag, nella console di gestione Amazon FSx.
- `cloudwatch`— Consente ai responsabili di visualizzare CloudWatch allarmi e metriche nella console di gestione Amazon FSx.

- `ds`— Consente ai responsabili di visualizzare le informazioni su una AWS Directory Service directory nella console di gestione Amazon FSx.
- `ec2`
  - Consente ai responsabili di visualizzare interfacce di rete, gruppi di sicurezza, sottoreti e il VPC associato a un file system Amazon FSx nella console di gestione Amazon FSx.
  - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
- `kms`— Consente ai mandanti di visualizzare gli alias per le AWS Key Management Service chiavi nella console di gestione Amazon FSx.
- `log`— Consente ai responsabili di descrivere i gruppi di log di Amazon CloudWatch Logs associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano visualizzare la configurazione di controllo dell'accesso ai file esistente per un file system FSx for Windows File Server.
- `firehose`— Consente ai mandanti di descrivere i flussi di distribuzione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano visualizzare la configurazione di controllo dell'accesso ai file esistente per un file system FSx for Windows File Server.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonF SxConsoleReadOnlyAccess nella Managed Policy Reference Guide. AWS

AWS politica gestita: AmazonF SxReadOnlyAccess

È possibile allegare la policy `AmazonFSxReadOnlyAccess`alle identità IAM.

Questa policy concede autorizzazioni amministrative che consentono l'accesso in sola lettura ad Amazon FSx.

- `fsx`— Consente ai responsabili di visualizzare le informazioni sui file system Amazon FSx, inclusi tutti i tag, nella console di gestione Amazon FSx.
- `ec2`— Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.

Per visualizzare le autorizzazioni relative a questa politica, consulta AmazonF SxReadOnlyAccess nella Managed Policy Reference Guide. AWS

Amazon FSx si aggiorna alle AWS policy gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon FSx da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS sulla pagina Amazon FSx. Cronologia dei documenti

Modifica	Descrizione	Data
AmazonF: aggiornamento a una SxServiceRolePolicy politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
AmazonF SxReadOnlyAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
AmazonF SxConsole 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

Modifica	Descrizione	Data
AmazonF SxFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
AmazonF SxConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, `ec2:GetSecurityGroupsForVpc` che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
AmazonF SxFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica dei dati tra regioni e più account per i file system FSx for OpenZFS.	20 dicembre 2023
AmazonF: aggiornamento a una politica esistente SxConsoleFullAccess	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica dei dati tra regioni e più account per i file system FSx for OpenZFS.	20 dicembre 2023

Modifica	Descrizione	Data
AmazonF: aggiornamento a una politica esistente SxFullAccess	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica su richiesta dei volumi per i file system FSx for OpenZFS.	26 novembre 2023
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica su richiesta dei volumi per i file system FSx for OpenZFS.	26 novembre 2023
AmazonF SxFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare, abilitare e disabilitare il supporto VPC condiviso per i file system FSx for ONTAP Multi-AZ.	14 novembre 2023
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare, abilitare e disabilitare il supporto VPC condiviso per i file system FSx for ONTAP Multi-AZ.	14 novembre 2023

Modifica	Descrizione	Data
AmazonF SxFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di gestire le configurazioni di rete per i file system FSx for OpenZFS Multi-AZ.	9 agosto 2023
AWS politica gestita: AmazonF — Aggiornam ento a una politica esistente SxServiceRolePolicy	Amazon FSx ha modificato l'`cloudwatch:PutMetr icData` autorizzazione esistente in modo che Amazon FSx pubblichi CloudWatch i parametri nello spazio dei nomi. `AWS/FSx`	24 luglio 2023
AmazonF SxFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiornat o la policy per rimuovere l'`fsx:*`autorizzazione e aggiungere azioni specifich `efsx`.	13 luglio 2023
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiornat o la policy per rimuovere l'`fsx:*`autorizzazione e aggiungere azioni specifich `efsx`.	13 luglio 2023
AmazonF SxFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di gestire le configurazioni di rete per i file system FSx for OpenZFS Multi-AZ.	31 maggio 2023

Modifica	Descrizione	Data
SxConsoleReadOnlyAccessAmazonF: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare metriche di prestazioni migliorate e azioni consigliate per i file system FSx for Windows File Server nella console Amazon FSx.	21 settembre 2022
AmazonF SxConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare metriche di prestazioni migliorate e azioni consigliate per i file system FSx for Windows File Server nella console Amazon FSx.	21 settembre 2022
AmazonF: politica di tracciamento avviata SxReadOnlyAccess	Questa policy garantisce l'accesso in sola lettura a tutte le risorse Amazon FSx e a tutti i tag ad esse associati.	4 febbraio 2022
AmazonF SxDeleteServiceLinkedRoleAccess — Avviata la politica di tracciamento	Questa politica concede autorizzazioni amministrative che consentono ad Amazon FSx di eliminare il suo Service Linked Role per l'accesso ad Amazon S3.	7 gennaio 2022

Modifica	Descrizione	Data
AmazonF SxServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di gestire le configurazioni di rete per i file system Amazon FSx for ONTAP. NetApp	2 settembre 2021
AmazonF SxFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare tag sulle tabelle di routing EC2 per chiamate con ambito limitato.	2 settembre 2021
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare Amazon FSx per i file system ONTAP Multi-AZ. NetApp	2 settembre 2021
AmazonF SxConsole FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare tag sulle tabelle di routing EC2 per chiamate con ambito limitato.	2 settembre 2021

Modifica	Descrizione	Data
AmazonF SxServiceRolePolicy: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di descrivere e scrivere su Logs i flussi di log. CloudWatch Ciò è necessario per consentire agli utenti di visualizzare i registri di controllo degli accessi ai file per i file system FSx for Windows File Server utilizzando Logs. CloudWatch	8 giugno 2021
AmazonF: aggiornamento a una SxServiceRolePolicy politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di descrivere e scrivere nei flussi di distribuzione di Amazon Data Firehose. Ciò è necessario per consentire agli utenti di visualizzare i log di controllo degli accessi ai file per un file system FSx for Windows File Server utilizzando Amazon Data Firehose.	8 giugno 2021

Modifica	Descrizione	Data
AmazonF: aggiornamento a una SxFullAccess politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere e creare gruppi di CloudWatch log, flussi di log e scrivere eventi nei flussi di log. Ciò è necessario affinché i responsabili possano visualizz are i registri di controllo degli accessi ai file per i file system FSx for Windows File Server utilizzando Logs. CloudWatch	8 giugno 2021
AmazonF SxFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere e scrivere record su Amazon Data Firehose. Ciò è necessario per consentir e agli utenti di visualizzare i log di controllo degli accessi ai file per un file system FSx for Windows File Server utilizzan do Amazon Data Firehose.	8 giugno 2021

Modifica	Descrizione	Data
AmazonF: aggiornamento a una SxConsoleFullAccess 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 CloudWatch Logs esistente durante la configurazione del controllo dell'accesso ai file per un file system FSx for Windows File Server.	8 giugno 2021
AmazonF SxConsole FullAccess: 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 un file system FSx for Windows File Server.	8 giugno 2021

Modifica	Descrizione	Data
AmazonF SxConsole ReadOnlyAccess: 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 visualizzare la configurazione di controllo dell'accesso ai file esistente per un file system FSx for Windows File Server.	8 giugno 2021
AmazonF: aggiornamento a una SxConsoleReadOnlyAccess 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 visualizzare la configurazione di controllo dell'accesso ai file esistente per un file system FSx for Windows File Server.	8 giugno 2021
Amazon FSx ha iniziato a tracciare le modifiche	Amazon FSx ha iniziato a tracciare le modifiche per le sue politiche AWS gestite.	8 giugno 2021

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon FSx for Windows File Server

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 FSx

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `fsx:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `fsx:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue policy devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon FSx.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio anziché creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon FSx. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse FSx

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon FSx supporta queste funzionalità, consulta. Come funziona Amazon FSx for Windows File Server con IAM
- Per sapere come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

Utilizzo dei tag con Amazon FSx

Puoi utilizzare i tag per controllare l'accesso alle risorse Amazon FSx e implementare il controllo degli accessi basato sugli attributi (ABAC). Gli utenti devono essere autorizzati ad applicare tag alle risorse Amazon FSx durante la creazione.

Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione

Alcune azioni dell'API Amazon FSx per la creazione di risorse consentono di specificare i tag quando si crea la risorsa. Puoi utilizzare i tag delle risorse per implementare il controllo degli accessi basato sugli attributi (ABAC). Per ulteriori informazioni, consulta What is ABAC AWS nella IAM User Guide.

Per consentire agli utenti di applicare tag alle risorse durante la creazione, essi devono disporre delle autorizzazioni per utilizzare l'operazione che crea la risorsa, come `fsx:CreateFileSystem` o `fsx:CreateBackup`. Se i tag vengono specificati nell'azione di creazione delle risorse, Amazon esegue autorizzazioni aggiuntive per l'azione `fsx:TagResource` per verificare se gli utenti dispongono delle autorizzazioni per creare tag. Pertanto, gli utenti devono disporre anche delle autorizzazioni esplicite per utilizzare l'operazione `fsx:TagResource`.

L'esempio seguente illustra una politica che consente agli utenti di creare file system e applicare tag ai file system durante la creazione in uno specifico. Account AWS

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

Analogamente, la seguente policy consente agli utenti di creare backup su un file system specifico e di applicare eventuali tag al backup durante la creazione del backup.

```
{
```

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

L'operazione `fsx:TagResource` viene valutata solo se i tag vengono applicati durante l'operazione di creazione di risorse. Pertanto, un utente con le autorizzazioni per la creazione di una risorsa (presupponendo che non siano presenti condizioni di assegnazione di tag) non necessità delle autorizzazioni per utilizzare l'operazione `fsx:TagResource` se nella richiesta non viene specificato alcun tag. Tuttavia, se l'utente tenta di creare una risorsa con tag, la richiesta ha esito negativo se non dispone delle autorizzazioni per utilizzare l'operazione `fsx:TagResource`.

Per ulteriori informazioni sull'etichettatura delle risorse Amazon FSx, consulta. Tagging delle risorse Amazon FSx Per ulteriori informazioni sull'utilizzo dei tag per controllare l'accesso alle risorse FSx, vedere. Utilizzo dei tag per controllare l'accesso alle risorse Amazon FSx

Utilizzo dei tag per controllare l'accesso alle risorse Amazon FSx

Per controllare l'accesso alle risorse e alle azioni di Amazon FSx, puoi utilizzare policy AWS Identity and Access Management (IAM) basate su tag. È possibile fornire il controllo in due modi:

1. Controlla l'accesso alle risorse Amazon FSx in base ai tag presenti su tali risorse.
2. Controllare quali tag possono essere trasferiti in una condizione di richiesta IAM.

Per informazioni su come utilizzare i tag per controllare l'accesso alle AWS risorse, consulta Controlling access using tags nella IAM User Guide. Per ulteriori informazioni sull'etichettatura delle risorse Amazon FSx al momento della creazione, consulta. Concessione dell'autorizzazione

all'applicazione di tag per le risorse durante la creazione Per ulteriori informazioni sull'assegnazione di tag alle risorse, consulta Tagging delle risorse Amazon FSx.

Controllo dell'accesso in base ai tag di una risorsa

Per controllare le azioni che un utente o un ruolo può eseguire su una risorsa Amazon FSx, puoi utilizzare i tag sulla risorsa. Ad esempio, è possibile consentire o negare operazioni API specifiche su una risorsa di gateway di file in base alla coppia chiave-valore del tag sulla risorsa.

Example policy: crea un file system attivo quando fornisci un tag specifico

Questa politica consente all'utente di creare un file system solo quando lo contrassegna con una coppia chiave-valore specifica, in questo esempio`key=Department, value=Finance`.

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

Example policy — Crea backup solo dei file system Amazon FSx con un tag specifico

Questa policy consente agli utenti di creare backup solo dei file system etichettati con la coppia `key=Department, value=Finance` chiave-valore e il backup verrà creato con il tag. `Deparment=Finance`

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
```

```
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }

    ]
}
```

Example policy: crea un file system con un tag specifico dai backup con un tag specifico

Questa politica consente agli utenti di creare file system etichettati con `Department=Finance` solo a partire da backup contrassegnati con. `Department=Finance`

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

```
        }
    ]
}
```

Example policy: elimina i file system con tag specifici

Questa politica consente a un utente di eliminare solo i file system contrassegnati con`Department=Finance`. Se creano un backup finale, deve essere contrassegnato con`Department=Finance`.

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

Utilizzo di ruoli collegati ai servizi per Amazon FSx

Amazon FSx for Windows File Server AWS Identity and Access Management utilizza ruoli collegati ai servizi (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente ad Amazon FSx. I ruoli collegati ai servizi sono predefiniti da Amazon FSx e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per tuo conto. AWS

Un ruolo collegato al servizio semplifica la configurazione di Amazon FSx perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Amazon FSx definisce le autorizzazioni dei suoi ruoli collegati ai servizi e, se non diversamente definito, solo Amazon FSx può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato ai servizi solo dopo aver eliminato le risorse correlate. In questo modo proteggi le tue risorse Amazon FSx perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati ai servizi, consulta la sezione Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruolo associato ai servizi. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Autorizzazioni di ruolo collegate ai servizi per Amazon FSx

Amazon FSx utilizza il ruolo collegato al servizio denominato `AWSServiceRoleForAmazonFSx` — che esegue determinate azioni nel tuo account, come la creazione di interfacce di rete elastiche per i tuoi file system nel tuo VPC.

La politica di autorizzazione dei ruoli consente ad Amazon FSx di completare le seguenti azioni su tutte AWS le risorse applicabili:

Non puoi collegare AmazonF SxServiceRolePolicy alle tue entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente a FSx di gestire AWS le risorse per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon FSx.

Per gli aggiornamenti a questa politica, vedere AmazonF SxServiceRolePolicy

Questa politica concede autorizzazioni amministrative che consentono a FSx di gestire AWS le risorse per conto dell'utente.

Dettagli dell'autorizzazione

Le autorizzazioni dei SxServiceRolePolicy ruoli AmazonF sono definite dalla politica gestita di AmazonF. SxServiceRolePolicy AWS AmazonF dispone SxServiceRolePolicy delle seguenti autorizzazioni:

> **Note**
>
> AmazonF SxServiceRolePolicy è utilizzato da tutti i tipi di file system Amazon FSx; alcune delle autorizzazioni elencate potrebbero non essere applicabili a FSx per Windows.

- `ds`— Consente a FSx di visualizzare, autorizzare e non autorizzare le applicazioni nella directory. AWS Directory Service
- `ec2`— Consente a FSx di effettuare le seguenti operazioni:
  - Visualizza, crea e dissocia le interfacce di rete associate a un file system Amazon FSx.
  - Visualizza uno o più indirizzi IP elastici associati a un file system Amazon FSx.
  - Visualizza VPC, gruppi di sicurezza e sottoreti Amazon associati a un file system Amazon FSx.
  - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
  - Crea un'autorizzazione per un utente AWS autorizzato a eseguire determinate operazioni su un'interfaccia di rete.
- `cloudwatch`— Consente a FSx di pubblicare punti dati metrici nello spazio dei nomi /FSx. CloudWatch AWS
- `route53`— Consente a FSx di associare un Amazon VPC a una zona ospitata privata.
- `logs`— Consente a FSx di descrivere e scrivere su Logs i flussi di CloudWatch log. In questo modo gli utenti possono inviare i log di controllo degli accessi ai file per un file system FSx for Windows File Server a CloudWatch un flusso Logs.
- `firehose`— Consente a FSx di descrivere e scrivere sui flussi di distribuzione di Amazon Data Firehose. In questo modo gli utenti possono pubblicare i log di controllo degli accessi ai file per un file system FSx for Windows File Server su un flusso di distribuzione Amazon Data Firehose.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
```

```
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
```

```
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
```

```
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

Eventuali aggiornamenti a questa politica sono descritti in. Amazon FSx si aggiorna alle AWS policy gestite

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Creazione di un ruolo collegato ai servizi per Amazon FSx

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un file system nella CLI AWS Management Console IAM o nell'API IAM, Amazon FSx crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato ai servizi può apparire nell'account se è stata completata un'operazione in un altro servizio che utilizza le funzionalità supportate dal ruolo. Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato ai servizi, puoi ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un file system, Amazon FSx crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato ai servizi per Amazon FSx

Amazon FSx non consente di modificare il ruolo collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Amazon FSx

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non sarà più presente un'entità non utilizzata che non viene monitorata e gestita attivamente. Tuttavia, è necessario eliminare tutti i file system e i backup prima di poter eliminare manualmente il ruolo collegato al servizio.

> **Note**
>
> Se il servizio Amazon FSx utilizza il ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Usa la console IAM, la CLI IAM oppure l'API IAM per eliminare il ruolo collegato ai servizi . Per ulteriori informazioni, consulta Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Regioni supportate per i ruoli collegati ai servizi Amazon FSx

Amazon FSx supporta l'utilizzo di ruoli collegati al servizio in tutte le regioni in cui il servizio è disponibile. Per ulteriori informazioni, consulta Regioni ed endpoint di AWS.

Convalida della conformità per Amazon FSx for Windows File Server

Per sapere se un Servizio AWS programma rientra nell'ambito di specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono i passaggi per l'implementazione di ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive in che modo le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of

Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).

- Evaluating Resources with Rules nella AWS Config Developer Guide: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio e la conformità alle normative e agli standard di settore.

Amazon FSx for Windows File Server e endpoint VPC di interfaccia

Puoi migliorare la posizione di sicurezza del VPC configurando Amazon FSx in modo che utilizzi un endpoint VPC di interfaccia. Endpoint VPC dell'interfaccia con tecnologiaAWS PrivateLink, una tecnologia che consente di accedere privatamente alle API Amazon FSx senza un gateway Internet, un dispositivo NAT, una connessione VPN oAWS Direct Connectconnessione. Le istanze presenti nel VPC non richiedono indirizzi IP pubblici per comunicare con le API Amazon FSx. Il traffico tra il tuo VPC e Amazon FSx non esce dalAWSnetwork.

Ogni endpoint VPC di interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti. Un'interfaccia di rete fornisce un indirizzo IP privato che funge da punto di ingresso per il traffico verso l'API Amazon FSx.

Considerazioni sugli endpoint VPC dell'interfaccia Amazon FSx

Prima di impostare un endpoint VPC di interfaccia per Amazon FSx, assicurarsi di esaminareProprietà e limitazioni degli endpoint VPC dell'interfacciaAmazon VPC User Guide.

Puoi chiamare qualsiasi operazione API Amazon FSx dal tuo VPC. Ad esempio, è possibile creare un file system FSx for Windows File Server chiamando il file system CreateFileSystem API dal tuo VPC. Per l'elenco completo delle API Amazon FSx, consultaOperazioninella Documentazione di riferimento delle API FSx di Amazon.

Peering VPC

È possibile connettere altri VPC al VPC con endpoint VPC di interfaccia utilizzando Peering VPC. Il peering VPC è una connessione di rete tra due VPC. Puoi creare una connessione peering VPC tra i tuoi VPC oppure con un VPC in un altroAccount AWS. I VPC possono essere anche in due diversiRegioni AWS.

Il traffico tra VPC peered rimane sulla rete AWS e non attraversa la rete Internet pubblica. Una volta eseguito il peering dei vPC, risorse come istanze Amazon Elastic Compute Cloud (Amazon EC2) in entrambi i VPC possono accedere all'API Amazon FSx tramite gli endpoint VPC di interfaccia creati in uno dei VPC.

Creazione di un endpoint VPC di interfaccia per l'API Amazon FSx

Puoi creare un endpoint VPC per l'API Amazon FSx utilizzando la console Amazon VPC oAWS Command Line Interface(AWS CLI). Per ulteriori informazioni, consultaCreazione di un endpoint VPC dell'interfacciaAmazon VPC User Guide.

Per creare un endpoint VPC di interfaccia per Amazon FSx, utilizzare una delle seguenti opzioni:

- **`com.amazonaws.`*`region`*`.fsx`**: crea un endpoint per le operazioni API Amazon FSx.
- **`com.amazonaws.`*`region`*`.fsx-fips`**: crea un endpoint per l'API Amazon FSx conforme aFederal Information Processing Standard (FIPS) 140-2.

Per utilizzare l'opzione DNS privato, è necessario impostare la`enableDnsHostnames`e`enableDnsSupport`attributi del tuo VPC. Per ulteriori informazioni, consultaVisualizzazione e aggiornamento del supporto DNS per il VPCAmazon VPC User Guide.

EscludendoRegioni AWSin Cina, se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API a Amazon FSx con l'endpoint VPC utilizzando il nome DNS predefinito per l'endpoint VPC utilizzando il nome DNS predefinito per l'endpoint,Regione AWS, ad esempio`fsx.us-east-1.amazonaws.com`. Per la Cina (Pechino) e Cina (Ningxia)Regioni AWS, è possibile effettuare richieste API con

l'endpoint VPC utilizzandofsx-api.cn-north-1.amazonaws.com.cnefsx-api.cn-northwest-1.amazonaws.com.cn, rispettivamente.

Per ulteriori informazioni, consultaAccesso a un servizio tramite un endpoint VPC di interfacciaAmazon VPC User Guide.

Creazione di una policy per l'endpoint VPC per Amazon FSx

Per controllare ulteriormente l'accesso all'API Amazon FSx, puoi facoltativamente allegare unAWS Identity and Access Management(IAM) per l'endpoint VPC. La policy specifica quanto segue:

- Il principale che può eseguire operazioni.
- Le operazioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire operazioni.

Per ulteriori informazioni, consultare Controllo degli accessi ai servizi con endpoint VPC in Guida per l'utente di Amazon VPC.

Quote

Di seguito, puoi scoprire le quote quando lavori con Amazon FSx for Windows File Server.

Argomenti

Quote che è possibile incrementare

Di seguito sono riportate le quote per Amazon FSx for Windows File Server per Account AWS ogni file che puoi aumentare. Regione AWS

Risorsa	Predefinito	Descrizione
File system Windows	100	Il numero massimo di file system Amazon FSx per Windows File Server che puoi creare in questo account.
Capacità di velocità effettiva di Windows	10240	La quantità totale di capacità effettiva di trasmissione (in Mbps) consentita per tutti i file system Amazon FSx per Windows in questo account.
Capacità di archiviazione HDD di Windows	524288	La quantità massima di capacità di archiviazione su disco rigido (in GiB) consentit a per tutti i file system Amazon FSx per Windows File Server in questo account.

Risorsa	Predefinito	Descrizione
Capacità di archiviazione SSD di Windows	524288	La quantità massima di capacità di archiviazione SSD (in GiB) consentita per tutti i file system Amazon FSx for Windows File Server in questo account.
IOPS SSD totali di Windows	500.000	La quantità totale di IOPS SSD consentiti per tutti i file system Amazon FSx for Windows File Server in questo account.
Backup di Windows	500	Il numero massimo di backup avviati dall'utente per tutti i file system Amazon FSx per Windows File Server che puoi avere in questo account.

Richiesta di un aumento delle quote

1. Apri la console Service Quotas.
2. Nel pannello di navigazione, scegli Servizi AWS (servizi AWS).
3. Scegli Amazon FSx.
4. Scegli una quota.
5. Scegli Richiedi un aumento della quota e segui le istruzioni per richiedere un aumento della quota.
6. Per visualizzare lo stato della richiesta di quota, scegli Cronologia delle richieste di quota nel riquadro di navigazione della console.

Per ulteriori informazioni, consulta Richiesta di un aumento di quota nella Guida per l'utente per Service Quotas.

Quote di risorse per ogni file system

Di seguito sono riportate le quote sulle risorse di Amazon FSx for Windows File Server per ogni file system in un. Regione AWS

Risorsa	Limite per file system
Numero massimo di tag	50
Periodo massimo di conservazione per i backup automatici	90 giorni
Numero massimo di richieste di copie di backup in corso verso una singola regione di destinazione per account.	5
Capacità di archiviazione minima, file system SSD	32 GiB
Capacità di archiviazione minima, file system HDD	2.000 GiB
Capacità massima di archiviazione, SSD e HDD	64 TiB
IOPS SSD minimi	96
Numero massimo di IOPS SSD	400.000
Capacità di throughput minima	8 MBps
Capacità massima di throughput	12.288 MBps
Numero massimo di condivisioni di file	100.000

Ulteriori considerazioni

In aggiunta, tieni presente quanto segue:

- Puoi utilizzare ogni chiave AWS Key Management Service (AWS KMS) su un massimo di 125 file system Amazon FSx.
- Per un elenco di Regioni AWS dove è possibile creare file system, consulta Amazon FSx Endpoints and Quotas nel. Riferimenti generali di AWS

- Puoi mappare le tue condivisioni di file dalle istanze Amazon EC2 nel tuo cloud privato virtuale (VPC) con i relativi nomi DNS (Domain Name Service).

Quote specifiche per Microsoft Windows

Per ulteriori informazioni, vedere Limiti NTFS in Microsoft Windows Dev Center.

Risoluzione dei problemi di Amazon FSx

Utilizza le seguenti sezioni per risolvere i problemi riscontrati con Amazon FSx.

Se riscontri problemi non elencati di seguito durante l'utilizzo di Amazon FSx, prova a porre una domanda nel forum Amazon FSx.

Argomenti

Non puoi accedere al tuo file system

Esistono diverse cause potenziali per cui non è possibile accedere al file system, ognuna con la propria risoluzione, come segue.

Argomenti

- Il nuovo file system non è registrato nel DNS
- Impossibile accedere al file system utilizzando un alias DNS
- Impossibile accedere al file system utilizzando un indirizzo IP

L'interfaccia elastic network interface del file system è stata modificata o eliminata

Non è necessario modificare o eliminare l'elastic network interface del file system. La modifica o l'eliminazione dell'interfaccia di rete può causare una perdita permanente della connessione tra il VPC e il file system. Crea un nuovo file system e non modificare o eliminare l'interfaccia di rete elastica Amazon FSx. Per ulteriori informazioni, consulta Controllo degli accessi ai file system con Amazon VPC.

L'indirizzo IP elastico collegato all'interfaccia di rete elastica del file system è stato eliminato

Amazon FSx non supporta l'accesso ai file system dalla rete Internet pubblica. Amazon FSx scollega automaticamente qualsiasi indirizzo IP elastico, che è un indirizzo IP pubblico raggiungibile da Internet, che viene collegato all'interfaccia di rete elastica di un file system. Per ulteriori informazioni, consulta Client, metodi di accesso e ambienti supportati per Amazon FSx for Windows File Server.

Il gruppo di sicurezza del file system non dispone delle regole in entrata o in uscita 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 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.

Istanza di calcolo non unita a un Active Directory

Le tue istanze di calcolo potrebbero non essere unite correttamente a uno dei due tipi di Active Directory:

- La AWS Managed Microsoft AD directory a cui è unito il file system.
- Una directory di Microsoft Active Directory che ha una relazione di forest trust unidirezionale stabilita con la AWS Managed Microsoft AD directory.

Assicurati che le istanze di calcolo siano unite a uno dei due tipi di directory. Un tipo è la AWS Managed Microsoft AD directory a cui è unito il file system. L'altro tipo è una directory di Microsoft Active Directory che ha una relazione di trust unidirezionale tra foreste stabilita con la AWS Managed Microsoft AD directory. Per ulteriori informazioni, consulta Utilizzo di Amazon FSx con AWS Directory Service for Microsoft Active Directory.

La condivisione di file non esiste

La condivisione di file di Microsoft Windows a cui stai tentando di accedere non esiste.

Se utilizzi una condivisione di file esistente, assicurati che il nome DNS del file system e il nome della condivisione siano specificati correttamente. Per gestire le condivisioni di file, consultaGestione delle condivisioni di file su file system FSx for Windows File Server.

L'utente di Active Directory non dispone delle autorizzazioni necessarie

L'utente di Active Directory a cui stai accedendo alla condivisione di file non dispone delle autorizzazioni di accesso necessarie.

Assicurati che le autorizzazioni di accesso per la condivisione di file e gli elenchi di controllo di accesso (ACL) di Windows per la cartella condivisa consentano l'accesso agli utenti di Active Directory che devono accedervi.

Consenti la rimozione delle autorizzazioni ACL NTFS (controllo completo)

Se rimuovi le autorizzazioni Allow Full control NTFS ACL per l'utente SYSTEM su una cartella condivisa, tale condivisione può diventare inaccessibile e qualsiasi backup del file system eseguito da quel momento in poi potrebbe non essere utilizzabile.

Dovrai ricreare la condivisione di file interessata. Per ulteriori informazioni, consulta Gestione delle condivisioni di file su file system FSx for Windows File Server. Dopo aver ricreato la cartella o la condivisione, puoi mappare e utilizzare le condivisioni di file Windows dalle tue istanze di calcolo.

Impossibile accedere a un file system utilizzando un client locale

Stai usando il tuo file system Amazon FSx in locale AWS Direct Connect o tramite VPN e stai utilizzando un intervallo di indirizzi IP non privato per il client locale.

Amazon FSx supporta solo l'accesso da client locali con indirizzi IP non privati su file system creati dopo il 17 dicembre 2020.

Se è necessario accedere al file system FSx for Windows File Server creato prima del 17 dicembre 2020 utilizzando un intervallo di indirizzi IP non privato, è possibile creare un nuovo file system ripristinando un backup del file system. Per ulteriori informazioni, consulta Utilizzo dei backup.

Il nuovo file system non è registrato nel DNS

Per i file system uniti a un Active Directory autogestito, Amazon FSx non ha registrato il DNS del file system al momento della creazione perché la rete del cliente non utilizza Microsoft DNS.

Amazon FSx non registra i file system nel DNS se la rete utilizza un servizio DNS di terze parti anziché Microsoft DNS. È necessario configurare manualmente le voci DNS A per i file system Amazon FSx. Per i file system Single-AZ 1, dovrai aggiungere una voce DNS A; per i file system Single-AZ 2 e Multi-AZ, dovrai aggiungere due voci DNS A. Utilizzare la procedura seguente per ottenere l'indirizzo o gli indirizzi IP del file system da utilizzare per l'aggiunta manuale delle voci DNS A.

1. In https://console.aws.amazon.com/fsx/, scegliete il file system di cui desiderate ottenere l'indirizzo IP per visualizzare la pagina dei dettagli del file system.
2. Nella scheda Rete e sicurezza, effettuate una delle seguenti operazioni:

   - Per un file system Single-AZ 1:
     - Nel pannello Subnet, scegli l'interfaccia di rete elastica mostrata in Interfaccia di rete per aprire la pagina Interfacce di rete in Amazon EC2.
     - L'indirizzo IP da utilizzare per il file system Single-AZ 1 è indicato nella colonna IP IPv4 privato primario.
   - Per un file system Single-AZ 2 o Multi-AZ:
     - Nel pannello Preferred subnet, scegli l'interfaccia di rete elastica mostrata in Interfaccia di rete per aprire la pagina Interfacce di rete in Amazon EC2.
     - L'indirizzo IP della sottorete preferita da utilizzare è mostrato nella colonna IP IPv4 privato secondario.

- Nel pannello della sottorete Amazon FSx Standby, scegli l'interfaccia di rete elastica mostrata in Interfaccia di rete per aprire la pagina Interfacce di rete nella console Amazon EC2.
- L'indirizzo IP della sottorete di standby da utilizzare è mostrato nella colonna IP IPv4 privato secondario.

Impossibile accedere al file system utilizzando un alias DNS

Se non riesci ad accedere a un file system utilizzando un alias DNS, utilizza la seguente procedura per risolvere il problema.

1. Verifica che l'alias sia associato al file system eseguendo una delle seguenti operazioni:

   a. Utilizzo della console Amazon FSx: scegli il file system a cui stai tentando di accedere. Nella pagina dei dettagli del file system, gli alias DNS vengono visualizzati nella scheda Rete e sicurezza.

   b. Utilizzo della CLI o dell'API: utilizza il comando `describe-file-system-aliases`CLI o l'operazione DescribeFileSystemAliasesAPI per recuperare gli alias attualmente associati al file system.

2. Se l'alias DNS non è elencato, è necessario associarlo al file system. Per ulteriori informazioni, consulta Gestione degli alias DNS sui file system esistenti.
3. Se l'alias DNS è associato al file system, verifica di aver configurato anche i seguenti elementi obbligatori:

   - Nomi principali di servizio (SPN) creati corrispondenti all'alias DNS sull'oggetto computer Active Directory del file system Amazon FSx.

     Per ulteriori informazioni, consulta Passaggio 2: Configurazione dei nomi principali di servizio (SPN) per Kerberos.

   - Creato un record DNS CNAME per l'alias DNS che si risolve nel nome DNS predefinito del file system Amazon FSx.

     Per ulteriori informazioni, consulta Passaggio 3: Aggiornare o creare un record DNS CNAME per il file system.

4. Se hai creato SPN validi e un record DNS CNAME, verifica che il DNS del client disponga del record DNS CNAME che si risolve nel file system corretto.

a. Esegui `nslookup` per confermare che il record esiste e che sia stato risolto nel nome DNS predefinito del file system.

b. Se il CNAME DNS passa a un altro file system, attendi che la cache DNS del client si aggiorni, quindi ricontrolla il record CNAME. È possibile accelerare il processo svuotando la cache DNS del client utilizzando il comando seguente.

```
ipconfig /flushdns
```

5. Se il record DNS CNAME si risolve nel DNS predefinito del file system Amazon FSx e il client non è ancora in grado di accedere al file system, consulta ulteriori passaggi per la risoluzione dei problemi. Non puoi accedere al tuo file system

Impossibile accedere al file system utilizzando un indirizzo IP

Se non riesci ad accedere al file system utilizzando un indirizzo IP, prova invece a utilizzare il nome DNS o l'alias DNS associato.

Puoi trovare il nome DNS del file system e tutti gli alias DNS associati sulla console Amazon FSx scegliendo Windows File Server, rete e sicurezza. Oppure, puoi trovarli nella risposta dell'operazione o dell'CreateFileSystemAPI. DescribeFileSystems Per ulteriori informazioni sull'utilizzo degli alias DNS, consulta. Gestione degli alias DNS

- Per un file system Single-AZ unito a un Microsoft Active Directory AWS gestito, il nome DNS è simile al seguente.

```
fs-0123456789abcdef0.ad-domain.com
```

- Per tutti i file system Multi-AZ e i file system Single-AZ uniti a un Active Directory autogestito, il nome DNS è simile al seguente.

```
amznfsxaa11bb22.ad-domain.com
```

La creazione di un nuovo file system Amazon FSx non riesce

L'esito negativo di una richiesta di creazione del file system può essere causato da diverse cause, come descritto nella sezione seguente.

Argomenti

Risoluzione dei problemi dei file system uniti a una Microsoft Active Directory AWS gestita

Utilizzate le seguenti sezioni per risolvere i problemi relativi al tentativo di creare un file system FSx for Windows File Server unito al vostro Active Directory autogestito.

ACL di rete e gruppi di sicurezza VPC configurati in modo errato

Assicurati che i gruppi di sicurezza VPC e gli ACL di rete siano configurati utilizzando la configurazione dei gruppi di sicurezza consigliata. Per ulteriori informazioni, consulta Creazione di gruppi di sicurezza.

La creazione di un file system unito a un Active Directory autogestito non riesce

Argomenti

Nomi di gruppi di amministratori del file system duplicati

La creazione di un file system unito ad Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
File system creation failed. Amazon FSx is unable to apply your Microsoft Active
 Directory configuration with the
specified file system administrators group. Please ensure that your Active Directory
 does not contain multiple domain
groups with the name: domain_group.
```

Amazon FSx non ha creato il file system perché esistono più gruppi di amministratori nel dominio con lo stesso nome.

Se non specifichi un nome di gruppo, Amazon FSx tenterà di utilizzare il valore predefinito «Domain Admins» come gruppo di amministratori. La richiesta avrà esito negativo se più di un gruppo utilizza il nome predefinito «Domain Admins».

Utilizza i seguenti passaggi per risolvere il problema.

1. Esamina i prerequisiti per aggiungere il tuo file system all'Active Directory autogestito.
2. Utilizza lo strumento di convalida di Amazon FSx Active Directory per convalidare la configurazione di Active Directory autogestita prima di creare un file system FSx for Windows File Server unito a un Active Directory autogestito.
3. Crea un nuovo file system utilizzando o. AWS Management Console AWS CLI Per ulteriori informazioni, consulta Unire un file system Amazon FSx a un dominio Microsoft Active Directory autogestito.
4. Fornisci un nome per il gruppo di amministratori del file system che sia unico nel dominio dell'Active Directory autogestito.

Server DNS o controller di dominio non raggiungibili

La creazione di un file system unito all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
Amazon FSx can't reach the DNS servers provided or the domain controllers for your
 self-managed directory in Microsoft Active Directory.
File system creation failed. Amazon FSx is unable to communicate with your Microsoft
 Active Directory domain controllers.
```

```
This is because Amazon FSx can't reach the DNS servers provided or domain controllers
 for your domain.
To fix this problem, delete your file system and create a new one with valid DNS
 servers and networking configuration that allows
traffic from the file system to the domain controller.
```

Utilizza la procedura seguente per risolvere il problema.

1. Verifica di aver soddisfatto i prerequisiti per stabilire la connettività di rete e il routing tra la sottorete in cui stai creando un file system Amazon FSx e il tuo Active Directory autogestito. Per ulteriori informazioni, consulta Prerequisiti per l'utilizzo di un Microsoft Active Directory autogestito.

   Utilizza lo strumento di convalida di Amazon FSx Active Directory per testare e verificare queste impostazioni di rete.

   > **Note**
   >
   > Se hai definito più siti Active Directory, assicurati che le sottoreti nel VPC associato al tuo file system Amazon FSx siano definite in un sito Active Directory e che non esistano conflitti IP tra le sottoreti nel tuo VPC e le sottoreti negli altri siti. È possibile visualizzare e modificare queste impostazioni utilizzando lo snap-in MMC Active Directory Sites and Services.

2. Verifica di aver configurato i gruppi di sicurezza VPC associati al tuo file system Amazon FSx, insieme a qualsiasi ACL di rete VPC, per consentire il traffico di rete in uscita su tutte le porte.

   > **Note**
   >
   > Se desideri implementare il privilegio minimo, puoi consentire il traffico in uscita solo verso le porte specifiche necessarie per la comunicazione con i controller di dominio Active Directory. Per ulteriori informazioni, consulta la documentazione di Microsoft Active Directory.

3. Verificare che i valori per le proprietà amministrative del file server o della rete di Microsoft Windows non contengano caratteri non latino-1. Ad esempio, la creazione del file system non riesce se viene utilizzato `Domänen-Admins` come nome del gruppo di amministratori del file system.

4. Verifica che i server DNS e i controller di dominio del tuo dominio Active Directory siano attivi e in grado di rispondere alle richieste per il dominio fornito.
5. Assicurati che il livello funzionale del tuo dominio Active Directory sia Windows Server 2008 R2 o superiore.
6. Assicurati che le regole del firewall sui controller di dominio del tuo dominio Active Directory consentano il traffico proveniente dal tuo file system Amazon FSx. Per ulteriori informazioni, consulta la documentazione di Microsoft Active Directory.

Credenziali dell'account di servizio non valide

La creazione di un file system unito a un Active Directory autogestito non riesce e viene visualizzato il seguente messaggio di errore:

```
Amazon FSx is unable to establish a connection with your Microsoft Active Directory
 domain controllers
because the service account credentials provided are invalid. To fix this problem,
 delete your file
system and create a new one using a valid service account.
```

Utilizza la procedura seguente per risolvere il problema.

1. Verifica di inserire solo il nome utente come nome utente dell'account di servizio, ad esempio nella configurazione di Active `ServiceAcct` Directory autogestita.

   > **Important**
   >
   > NON includere un prefisso di dominio (`corp.com\ServiceAcct`) o un suffisso di dominio (`ServiceAcct@corp.com`) quando inserisci il nome utente dell'account del servizio.
   > NON utilizzate il nome distinto (DN) quando inserite il nome utente dell'account di servizio (CN=ServiceAcct, OU=example, DC=corp, DC=com).

2. Verifica che l'account di servizio che hai fornito esista nel tuo dominio Active Directory.
3. 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

Per ulteriori informazioni sulla creazione di un account di servizio con le autorizzazioni corrette, consulta. Delega dei privilegi al tuo account di servizio Amazon FSx

Autorizzazioni insufficienti per l'account di servizio

La creazione di un file system unito all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
Amazon FSx is unable to establish a connection with your
Microsoft Active Directory domain controllers. This is because the service account
 provided does not
have permission to join the file system to the domain with the specified organizational
 unit.
To fix this problem, delete your file system and create a new one using a service
 account with
permission to join the file system to the domain with the specified organizational
 unit.
```

Per risolvere il problema, utilizzare la procedura seguente.

- 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

Per ulteriori informazioni sulla creazione di un account di servizio con le autorizzazioni corrette, consulta. Delega dei privilegi al tuo account di servizio Amazon FSx

Capacità dell'account di servizio superata

La creazione di un file system unito ad Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
Amazon FSx can't establish a connection with your Microsoft Active Directory
domain controllers. This is because the service account provided has reached the
maximum number of computers that it can join to the domain. To fix this problem,
delete your file system and create a new one, supplying a service account that
is able to join new computers to the domain.
```

Per risolvere il problema, verifica che l'account di servizio fornito abbia raggiunto il numero massimo di computer che può aggiungere al dominio. Se ha raggiunto il limite massimo, crea un nuovo account di servizio con le autorizzazioni corrette. Utilizza il nuovo account di servizio e crea un nuovo file system. Per ulteriori informazioni, consulta Delega dei privilegi al tuo account di servizio Amazon FSx .

Amazon FSx non può accedere all'unità organizzativa (OU)

La creazione di un file system unito all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
Amazon FSx can't establish a connection with your Microsoft Active Directory domain
 controller(s).
This is because the organizational unit you specified either doesn't exist or isn't
 accessible
to the service account provided. To fix this problem, delete your file system and
 create a new one specifying an
organizational unit to which the service account can join the file system.
```

Utilizza la procedura seguente per risolvere il problema.

1. Verifica che l'unità organizzativa fornita si trovi nel tuo dominio Active Directory.
2. 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 effettuando l'accesso al file system. L'account di servizio deve inoltre disporre, come minimo, 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
- Assumi il controllo della creazione e dell'eliminazione di 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. Delega dei privilegi al tuo account di servizio Amazon FSx

L'account di servizio non può accedere al gruppo degli amministratori

La creazione di un file system unito all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. This is
 because the file system
administrators group you provided either doesn't exist or isn't accessible to the
 service account you
provided. To fix this problem, delete your file system and create a new one specifying
 a file
system administrators group in the domain that is accessible to the service account
provided.
```

Utilizza la procedura seguente per risolvere il problema.

1. Assicurati di fornire solo il nome del gruppo come stringa per il parametro del gruppo degli amministratori.

   > **Important**
   >
   > NON includete un prefisso di dominio (`corp.com\FSxAdmins`) o un suffisso di dominio (`FSxAdmins@corp.com`) quando fornite il parametro del nome del gruppo.

NON utilizzate il nome distinto (DN) per il gruppo. Un esempio di nome distinto è CN=FSxAdmins, OU=example, DC=corp, DC=com.

2. Assicurati che il gruppo di amministratori fornito esista nello stesso dominio Active Directory a cui desideri aggiungere il file system.
3. Se non hai fornito un parametro del gruppo di amministratori, Amazon FSx tenta di utilizzare il `Builtin Domain Admins` gruppo nel tuo dominio Active Directory. Se il nome di questo gruppo è stato modificato o se utilizzi un gruppo diverso per l'amministrazione del dominio, devi fornire quel nome per il gruppo.

Amazon FSx ha perso la connettività nel dominio

La creazione di un file system unito al tuo Active Directory autogestito non riesce e viene visualizzato il seguente messaggio di errore:

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. To fix
 this problem, delete your file system and create a new one
meeting the pre-requisites described in the Amazon FSx user guide.
```

Durante la creazione del tuo file system, Amazon FSx è riuscito a raggiungere i server DNS e i controller di dominio del tuo dominio Active Directory e a unire correttamente il file system al tuo dominio Active Directory. Tuttavia, durante il completamento della creazione del file system, Amazon FSx ha perso la connettività o l'appartenenza al tuo dominio. Utilizza i seguenti passaggi per risolvere il problema.

1. Assicurati che la connettività di rete continui a esistere tra il file system Amazon FSx e Active Directory. Inoltre, assicurati che il traffico di rete continui a essere consentito tra di loro utilizzando regole di routing, regole del gruppo di sicurezza VPC, ACL di rete VPC e regole firewall del controller di dominio.
2. Assicurati che gli oggetti informatici creati da Amazon FSx per i tuoi file system nel tuo dominio Active Directory siano ancora attivi e non siano stati eliminati o manipolati in altro modo.

L'account di servizio non dispone delle autorizzazioni corrette

La creazione di un file system unito ad Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
File system creation failed. Amazon FSx is unable to establish a connection with your
 Microsoft Active Directory domain controller(s).
This is because the service account provided does not have permission to join the file
 system to the domain with the specified
organizational unit (OU). To fix this problem, delete your file system and create a new
 one using a service account with permission
to create computer objects and reset passwords within the specified organizational
 unit.
```

Assicurati di aver delegato le autorizzazioni richieste all'account di servizio che hai fornito. Utilizza i seguenti passaggi per risolvere il problema.

L'account di servizio deve disporre almeno delle seguenti autorizzazioni:

- Assumi il controllo della creazione e dell'eliminazione di oggetti informatici nell'unità organizzativa a cui ti stai collegando al file system
- Disponi delle seguenti autorizzazioni nell'unità organizzativa per la quale ti stai collegando al file system:
  - Possibilità di reimpostare le password
  - Possibilità di impedire agli account di leggere e scrivere dati
  - Capacità convalidata di scrittura sull'hostname DNS
  - Capacità convalidata di scrivere sul nome principale del servizio
  - Capacità (può essere delegata) di creare ed eliminare oggetti informatici
  - Capacità convalidata di leggere e scrivere le restrizioni relative all'account
  - Possibilità di modificare le autorizzazioni

  Per ulteriori informazioni sulla creazione di un account di servizio con le autorizzazioni corrette, vedere. Delega dei privilegi al tuo account di servizio Amazon FSx

Caratteri Unicode utilizzati nei parametri di creazione

La creazione di un file system unito ad Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
File system creation failed. Amazon FSx is unable to create a file system within the
 specified
Microsoft Active Directory. To fix this problem, please delete your file system and
 create a new one
```

```
meeting the pre-requisites described in the FSx for ONTAP User Guide.
```

Amazon FSx non supporta i caratteri Unicode. Verifica che nessuno dei parametri di creazione contenga caratteri Unicode, come gli accenti. Ciò include i parametri che possono essere lasciati vuoti laddove un valore predefinito viene inserito automaticamente. Assicurati che anche i valori predefiniti corrispondenti in Active Directory non contengano caratteri Unicode.

Se riscontri problemi non elencati qui durante l'utilizzo di Amazon FSx, fai una domanda nel forum Amazon FSx o contatta Amazon Web Services Support.

Il file system è in uno stato configurato in modo errato

Un file system FSx for Windows File Server può entrare in uno stato di configurazione errata a causa di una modifica dell'ambiente Active Directory. In questo stato, il file system non è attualmente disponibile o rischia di perdere la disponibilità e i backup potrebbero non riuscire.

Lo stato Non configurato correttamente include un messaggio di errore e un'azione correttiva consigliata a cui puoi accedere utilizzando la console Amazon FSx, l'API o. AWS CLI Dopo aver intrapreso l'azione correttiva, verifica che alla fine lo stato del file system cambi a`Available`: tieni presente che il completamento di questa modifica può richiedere diversi minuti.

Il file system può entrare in uno stato di configurazione errata per diversi motivi, come i seguenti:

- Gli indirizzi IP del server DNS non sono più validi.
- Le credenziali dell'account di servizio non sono più valide o non dispongono delle autorizzazioni necessarie.
- Il controller di dominio Active Directory non è raggiungibile a causa di problemi di connettività di rete, ad esempio gruppi di sicurezza VPC non validi, ACL di rete VPC o configurazione della tabella di routing o impostazioni del firewall del controller di dominio.

(Per l'elenco completo dei requisiti di Active Directory, vedere. Prerequisiti per l'utilizzo di un Microsoft Active Directory autogestito Puoi anche verificare che il tuo ambiente Active Directory sia configurato correttamente per soddisfare questi requisiti utilizzando lo strumento di convalida di Amazon FSx Active Directory.)

La risoluzione di alcuni di questi problemi richiede l'aggiornamento diretto di uno o più parametri nella configurazione di Active Directory del file system, ad esempio la modifica degli indirizzi IP del server

DNS o la modifica del nome utente o della password dell'account di servizio. In questi casi, l'azione correttiva comporterà necessariamente l'utilizzo della console Amazon FSx, dell'API AWS CLI o l'aggiornamento dei parametri di configurazione richiesti.

Altri problemi potrebbero non richiedere la modifica dei parametri di configurazione di Active Directory, come la modifica delle impostazioni del firewall del controller di dominio o dei gruppi di sicurezza VPC. In questi casi, tuttavia, sarà necessario intraprendere ulteriori azioni prima che il file system possa `Available` diventarlo. Dopo esserti assicurato che l'ambiente Active Directory sia configurato correttamente, seleziona il pulsante Attempt Recovery accanto allo stato Non configurato correttamente nella console Amazon FSx oppure usa `StartMisconfiguredStateRecovery` il comando nella console Amazon FSx, nell'API o. AWS CLI

Argomenti

File system configurato in modo errato: Amazon FSx non può raggiungere né i server DNS né i controller di dominio del tuo dominio.

Un file system entra in uno `Misconfigured` stato in cui Amazon FSx non è in grado di comunicare con il controller o i controller di dominio Microsoft Active Directory.

Per risolvere questa situazione, procedi come segue:

1. Assicurati che la configurazione di rete consenta il traffico dal file system al controller di dominio.
2. Utilizza lo strumento di convalida di Amazon FSx Active Directory per testare e verificare le impostazioni di rete per il tuo Active Directory autogestito. Per ulteriori informazioni, consulta Utilizzo di Amazon FSx con Microsoft Active Directory autogestito.
3. Esamina la configurazione di Active Directory autogestita del file system nella console Amazon FSx.

4. Per aggiornare la configurazione di Active Directory autogestita del file system, puoi utilizzare la console Amazon FSx.

   a. Nel pannello di navigazione, scegli File system e scegli il file system da aggiornare; viene visualizzata la pagina dei dettagli del file system.

   b. Nella pagina dei dettagli del file system, scegli Aggiorna nella scheda Rete e sicurezza.

   Puoi anche utilizzare il `update-file-system` comando Amazon FSx CLI o l'operazione API. UpdateFileSystem

File system configurato in modo errato: le credenziali dell'account di servizio non sono valide

Amazon FSx non è in grado di stabilire una connessione con il controller o i controller di dominio Microsoft Active Directory. Questo perché le credenziali dell'account di servizio fornite non sono valide. Per ulteriori informazioni, consulta Utilizzo di Amazon FSx con Microsoft Active Directory autogestito.

Per risolvere l'errore di configurazione, procedi come segue:

1. Verifica di utilizzare l'account di servizio corretto e di utilizzare le credenziali corrette per quell'account.
2. Quindi aggiorna la configurazione del file system con l'account di servizio o le credenziali dell'account corretti utilizzando la console Amazon FSx.

   a. Nel pannello di navigazione, scegli File system e scegli il file system non configurato correttamente da aggiornare.

   b. Nella pagina dei dettagli del file system, scegli Aggiorna nella scheda Rete e sicurezza.

   Puoi anche utilizzare il funzionamento dell'API Amazon FSx. `update-file-system` Per ulteriori informazioni, consulta il riferimento UpdateFileSystemall'API Amazon FSx.

File system configurato in modo errato: l'account di servizio fornito non dispone dell'autorizzazione per aggiungere il file system al dominio

Amazon FSx non è in grado di stabilire una connessione ai controller di dominio Microsoft Active Directory. Questo perché l'account di servizio fornito non dispone dell'autorizzazione per aggiungere il file system al dominio con l'unità organizzativa specificata.

Per risolvere l'errore di configurazione, procedi come segue:

1. Aggiungi le autorizzazioni richieste all'account del servizio Amazon FSx o crea un nuovo account di servizio con le autorizzazioni richieste. Per ulteriori informazioni su questa operazione, consulta. Delega dei privilegi al tuo account di servizio Amazon FSx
2. Aggiorna quindi la configurazione di Active Directory autogestita del file system con le nuove credenziali dell'account di servizio. Per aggiornare la configurazione, puoi utilizzare la console Amazon FSx.

   a. Nel pannello di navigazione, scegli File system e scegli il file system da aggiornare; viene visualizzata la pagina dei dettagli del file system.

   b. Nella pagina dei dettagli del file system, scegli Aggiorna nella scheda Rete e sicurezza.

   Puoi anche utilizzare il funzionamento dell'API Amazon FSx. `update-file-system` Per ulteriori informazioni, consulta il riferimento UpdateFileSystemall'API Amazon FSx.

File system configurato in modo errato: l'account di servizio non può aggiungere altri computer al dominio

Amazon FSx non è in grado di stabilire una connessione ai controller di dominio Microsoft Active Directory. In questo caso, ciò è dovuto al fatto che l'account di servizio fornito ha raggiunto il numero massimo di computer che può aggiungere al dominio.

Per risolvere l'errore di configurazione, procedi come segue:

1. Identifica un altro account di servizio o crea un nuovo account di servizio che possa aggiungere nuovi computer al dominio.
2. Quindi aggiorna la configurazione di Active Directory autogestita del file system con le nuove credenziali dell'account di servizio utilizzando la console Amazon FSx.

a. Nel pannello di navigazione, scegli File system e scegli il file system da aggiornare; viene visualizzata la pagina dei dettagli del file system.

b. Nella pagina dei dettagli del file system, scegli Aggiorna nella scheda Rete e sicurezza.

Puoi anche utilizzare il funzionamento dell'API Amazon FSx. `update-file-system` Per ulteriori informazioni, consulta il riferimento UpdateFileSystemall'API Amazon FSx.

File system configurato in modo errato: l'account del servizio non ha accesso all'unità organizzativa

Amazon FSx non è in grado di stabilire una connessione ai controller di dominio Microsoft Active Directory perché l'account di servizio fornito non ha accesso all'unità organizzativa specificata.

Per risolvere l'errore di configurazione, procedi come segue:

1. Identifica un altro account di servizio o crea un nuovo account di servizio con accesso all'unità organizzativa.
2. Quindi aggiorna la configurazione di Active Directory autogestita del file system con le nuove credenziali dell'account di servizio.

   a. Nel riquadro di navigazione, scegli File system e scegli il file system da aggiornare; viene visualizzata la pagina dei dettagli del file system.

   b. Nella pagina dei dettagli del file system, scegli Aggiorna nella scheda Rete e sicurezza.

   Puoi anche utilizzare il funzionamento dell'API Amazon FSx. `update-file-system` Per ulteriori informazioni, consulta il riferimento UpdateFileSystemall'API Amazon FSx.

Risoluzione dei problemi con Remote Power Shell su FSx for Windows File Server

È possibile amministrare i file system FSx for Windows File Server utilizzando comandi di gestione remota personalizzati PowerShell .

Argomenti

Il comando New-F ha esito negativo con trust unidirezionale SxSmbShare

Amazon FSx non supporta l'esecuzione del `New-FSxSmbShare` PowerShell comando nei casi in cui si dispone di un trust unidirezionale e il dominio in cui risiede l'utente non è configurato per considerare attendibile il dominio associato al file system Amazon FSx.

Puoi risolvere questa situazione utilizzando una delle seguenti soluzioni:

- L'utente che esegue il `New-FSxSmbShare` comando deve trovarsi nello stesso dominio del file system FSx.
- È possibile utilizzare la GUI fsmgmt.msc per creare condivisioni sul file system. Per ulteriori informazioni, consulta Gestione delle condivisioni di file con l'interfaccia grafica delle cartelle condivise.

Non è possibile accedere al file system utilizzando Remote PowerShell

Esistono diverse cause potenziali per cui non è possibile connettersi al file system tramite Remote PowerShell, ognuna con la propria risoluzione, come segue.

Per assicurarti innanzitutto di poterti connettere correttamente a Windows Remote PowerShell Endpoint, puoi anche eseguire un test di connettività di base. Ad esempio, è possibile eseguire il `test-netconnection endpoint -port 5985` comando.

Il gruppo di sicurezza del file system non dispone delle regole in entrata richieste per consentire una connessione PowerShell remota

Il gruppo di sicurezza del file system deve disporre di una regola in entrata che consenta il traffico sulla porta 5985 per stabilire una sessione remota. PowerShell Per ulteriori informazioni, consulta Gruppi di sicurezza Amazon VPC.

È configurato un trust esterno tra Microsoft Active Directory AWS gestito e Active Directory locale

Per utilizzare Amazon FSx Remote PowerShell con l'autenticazione Kerberos, è necessario configurare una policy di gruppo locale sul client per l'ordine di ricerca nella foresta. Per ulteriori informazioni, consulta la documentazione Microsoft Configure Kerberos Forest Search Order (KFSO).

Si verifica un errore di localizzazione della lingua quando si tenta di avviare una sessione remota PowerShell

È necessario aggiungere quanto segue `-SessionOption` al comando: `-SessionOption (New-PSSessionOption -uiCulture "en-US")`

Di seguito sono riportati due esempi da utilizzare per l'`-SessionOption`avvio di una PowerShell sessione remota sul file system.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {fsx-command} -SessionOption
 (New-PSSessionOption -uiCulture "en-US")
```

```
PS C:\Users\delegateadmin> Enter-Pssession -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FsxRemoteAdmin -SessionOption (New-PSSessionOption -
uiCulture "en-US")
```

Non è possibile configurare DFS-R su un file system Multi-AZ o Single-AZ 2

Microsoft Distributed File System Replication (DFS-R) non è supportato sui file system Multi-AZ e Single-AZ 2.

I file system Multi-AZ sono configurati per la ridondanza tra più zone di accesso in modo nativo. Utilizza il tipo di implementazione Multi-AZ per un'elevata disponibilità su più zone di disponibilità. Per ulteriori informazioni, consulta Disponibilità e durabilità: file system Single-AZ e Multi-AZ.

Gli aggiornamenti della capacità di storage o di throughput falliscono

Le richieste di aggiornamento della capacità di throughput e storage del file system possono avere diverse cause potenziali, ognuna con una propria risoluzione.

L'aumento della capacità di storage non riesce perché Amazon FSx non può accedere alla chiave di crittografia KMS del file system

Una richiesta di aumento della capacità di storage non è riuscita perché Amazon FSx non è stato in grado di accedere alla chiave di crittografia del file system AWS Key Management Service (AWS KMS).

Devi assicurarti che Amazon FSx abbia accesso alla AWS KMS chiave per eseguire l'azione amministrativa. Utilizza le seguenti informazioni per risolvere il problema di accesso alle chiavi.

- Se la chiave KMS è stata eliminata, è necessario creare un nuovo file system da un backup utilizzando una nuova chiave KMS. Per ulteriori informazioni, consulta Procedura guidata 2: Creare un file system da un backup. Puoi riprovare la richiesta dopo che il nuovo file system sarà disponibile.
- Se la chiave KMS è disabilitata, riattivala e quindi riprova a eseguire la richiesta di aumento della capacità di archiviazione. Per ulteriori informazioni, consulta Abilitazione e disattivazione delle chiavi nella Guida per gli sviluppatori.AWS Key Management Service
- Se la chiave non è valida a causa della sua eliminazione in sospeso, è necessario creare un nuovo file system da un backup utilizzando una nuova chiave KMS. Puoi riprovare la richiesta dopo che il nuovo file system sarà disponibile. Per ulteriori informazioni, consulta Procedura guidata 2: Creare un file system da un backup.
- Se la chiave non è valida a causa dell'importazione in sospeso, è necessario attendere il completamento dell'importazione e quindi ripetere la richiesta di aumento dello spazio di archiviazione.
- Se il limite di concessione della chiave è stato superato, è necessario richiedere un aumento del numero di concessioni per la chiave. Per ulteriori informazioni, consulta Resource quotas nella Developer Guide.AWS Key Management Service Quando viene concesso l'aumento della quota, riprova la richiesta di aumento dello spazio di archiviazione.

L'aggiornamento della capacità di storage o di throughput non riesce perché l'Active Directory autogestito non è configurato correttamente

La richiesta di aggiornamento della capacità di archiviazione o della capacità di throughput non è riuscita perché Active Directory gestita automaticamente del file system è in uno stato di configurazione errata.

Per risolvere lo stato specifico di configurazione errata, vedere. Il file system è in uno stato configurato in modo errato

L'aumento della capacità di storage non riesce a causa dell'insufficiente capacità di throughput

La richiesta di aumento della capacità di archiviazione non è riuscita perché la capacità di throughput del file system è impostata su 8 MB/s.

Aumenta la capacità di trasmissione del file system a un minimo di 16 MB/s, quindi riprova la richiesta. Per ulteriori informazioni, consulta Gestione della capacità di throughput.

L'aggiornamento della capacità di throughput a 8 MB/s non riesce

Una richiesta di modifica della capacità di trasmissione del file system a 8 MB/s non è riuscita.

Ciò può verificarsi quando una richiesta di aumento della capacità di archiviazione è in sospeso o in corso. L'aumento della capacità di archiviazione richiede un throughput minimo di 16 MB/s. Attendi il completamento della richiesta di aumento della capacità di archiviazione, quindi riprova la richiesta di modifica della capacità di throughput.

La commutazione del tipo di archiviazione su HDD durante il ripristino di un backup non riesce

La creazione di un file system da un backup non riesce e viene visualizzato il seguente messaggio di errore:

```
Switching storage type to HDD while creating a file system from backup
backup_id is not supported because a storage scaling activity was still
under way on the source file system to increase storage capacity from less
```

`than 2000 GiB when the backup backup_id was taken, and the minimum storage capacity for HDD storage is 2000 GiB.`

Questo problema si verifica quando si ripristina un backup e il tipo di archiviazione è stato modificato da SSD a HDD. Il ripristino dal backup non riesce perché il backup che si sta ripristinando è stato eseguito mentre era ancora in corso un aumento della capacità di archiviazione sul file system originale. La capacità di archiviazione SSD del file system prima della richiesta di aumento era inferiore a 2000 GiB, che è la capacità di archiviazione minima richiesta per creare un file system HDD.

Utilizzare la procedura seguente per risolvere questo problema.

1. Attendi il completamento della richiesta di aumento della capacità di archiviazione e il file system ha almeno 2000 GiB di capacità di archiviazione SSD. Per ulteriori informazioni, consulta Monitoraggio dell'aumento della capacità di archiviazione.
2. Esegui un backup del file system avviato dall'utente. Per ulteriori informazioni, consulta Utilizzo dei backup avviati dall'utente.
3. Ripristina il backup avviato dall'utente su un nuovo file system utilizzando l'archiviazione su HDD. Per ulteriori informazioni, consulta Ripristino dei backup.

Risoluzione dei problemi relativi alle copie shadow

La mancanza o l'inaccessibilità delle copie shadow sono diverse le cause potenziali, come descritto nella sezione seguente.

Argomenti

- Mancano le copie shadow più vecchie
- Mancano tutte le mie copie shadow
- Non è possibile creare backup Amazon FSx o accedere a copie shadow su un file system ripristinato o aggiornato di recente

Mancano le copie shadow più vecchie

Le copie shadow più vecchie vengono eliminate in una di queste situazioni:

- Se si dispone di 500 copie shadow, la copia shadow successiva sostituisce la copia shadow più vecchia, indipendentemente dallo spazio di archiviazione rimanente allocato per le copie shadow.

- Se viene raggiunto lo spazio massimo di archiviazione delle copie shadow configurato, la copia shadow successiva sostituisce una o più delle copie shadow più vecchie, anche se si dispone di meno di 500 copie shadow.

Entrambi i risultati sono un comportamento previsto. Se lo spazio di archiviazione allocato per le copie shadow non è sufficiente, valuta la possibilità di aumentare lo spazio di archiviazione allocato.

Mancano tutte le mie copie shadow

Una capacità di prestazioni di I/O insufficiente sul file system (ad esempio, perché si utilizza lo storage su HDD, perché la capacità di archiviazione su disco rigido ha esaurito la capacità di burst o perché la capacità di trasmissione è insufficiente) può causare l'eliminazione di tutte le copie shadow da parte di Windows Server, poiché non è in grado di mantenere le copie shadow con la capacità prestazionale di I/O disponibile. Considerate i seguenti consigli per prevenire questo problema:

- Se utilizzi lo storage su HDD, utilizza la console Amazon FSx o l'API Amazon FSx per passare all'utilizzo dello storage SSD. Per ulteriori informazioni, consulta Gestione del tipo di storage.
- Aumenta la capacità di throughput del file system portandola a un valore tre volte superiore al carico di lavoro previsto.
- Accertatevi che il file system disponga di almeno 320 MB di spazio libero, oltre alla quantità massima di storage per copie shadow configurata.
- Pianificate le copie shadow quando vi aspettate che il file system sia inattivo.

Per ulteriori informazioni, consulta Raccomandazioni relative ai file system per le copie shadow.

Non è possibile creare backup Amazon FSx o accedere a copie shadow su un file system ripristinato o aggiornato di recente

Questo è il comportamento previsto. Amazon FSx ricostruisce lo stato di shadow-copy su un file system ripristinato di recente e non consente l'accesso a copie shadow o backup durante la ricostruzione dello stato di copia shadow.

Risoluzione dei problemi di prestazioni del file system

Le prestazioni del file system dipendono da diversi fattori, tra cui il traffico indirizzato al file system, la modalità di provisioning del file system e le funzionalità abilitate, come la deduplicazione dei dati

o le copie shadow. Per informazioni sulla comprensione delle prestazioni del file system, vedere. Prestazioni di FSx for Windows File Server

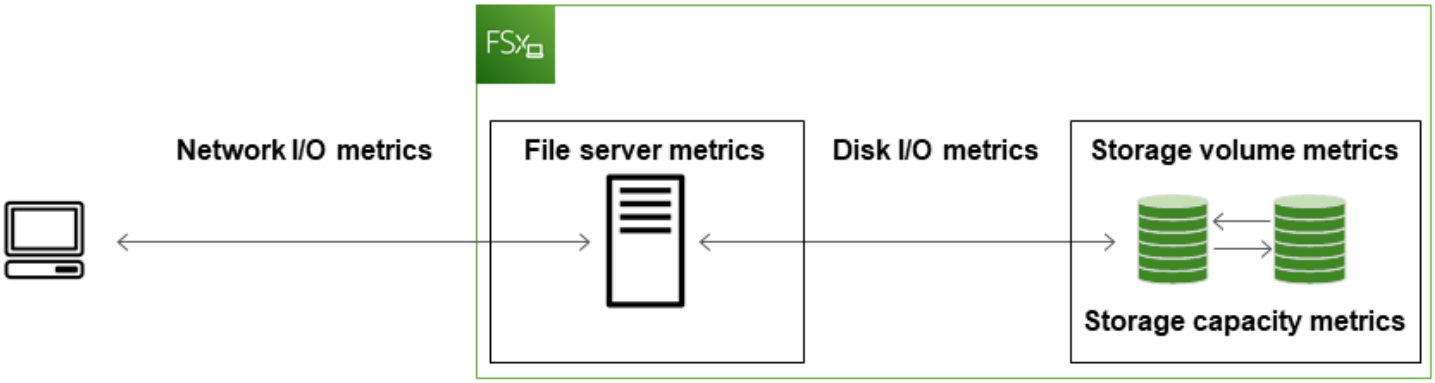
Argomenti

Come posso determinare il throughput e i limiti di IOPS per il mio file system?

Per visualizzare il throughput e i limiti IOPS di un file system, consultate la tabella che mostra i livelli di prestazioni in base alla quantità di capacità di throughput di provisioning.

Qual è la differenza tra I/O di rete e I/O su disco? Perché l'I/O della mia rete è diverso dall'I/O del mio disco?

I file system Amazon FSx includono uno o più file server che forniscono dati in rete ai client che accedono al file system. Si tratta dell'I/O di rete. Il file server dispone di una cache veloce in memoria per migliorare le prestazioni dei dati a cui si accede più frequentemente. I file server indirizzano inoltre il traffico verso i volumi di storage che ospitano i dati del file system. Questo è l'I/O del disco. Il diagramma seguente illustra l'I/O della rete e del disco per un file system Amazon FSx.



Per ulteriori informazioni, consulta Monitoraggio delle metriche con Amazon CloudWatch.

Perché l'utilizzo della CPU o della memoria è elevato, anche quando l'I/O di rete è basso?

L'utilizzo della CPU e della memoria del file server dipende non solo dal traffico di rete generato, ma anche dalle funzionalità abilitate sul file system. Il modo in cui configuri e pianifichi queste funzionalità può influire sull'utilizzo della CPU e della memoria.

I processi di deduplicazione dei dati in corso possono consumare memoria. È possibile modificare la configurazione dei processi di deduplicazione per ridurre i requisiti di memoria. Ad esempio, è possibile limitare l'ottimizzazione in modo che venga eseguita su tipi di file o cartelle specifici oppure impostare una dimensione e una durata minime del file per l'ottimizzazione. Si consiglia inoltre di configurare i processi di deduplicazione in modo che vengano eseguiti durante i periodi di inattività quando il carico sul file system è minimo. Per ulteriori informazioni, consulta Deduplicazione dei dati.

Se è abilitata l'enumerazione basata sull'accesso, è possibile che si verifichi un elevato utilizzo della CPU quando gli utenti finali visualizzano o elencano le condivisioni di file o durante la fase di ottimizzazione di un processo di scalabilità dello storage. Per ulteriori informazioni, vedere Abilitare l'enumerazione basata sull'accesso su uno spazio dei nomi nella documentazione di Microsoft Storage.

Che cos'è lo scoppio? Quanta frammentazione utilizza il mio file system? Cosa succede quando i crediti burst si esauriscono?

I carichi di lavoro basati su file sono in genere caratterizzati da picchi, caratterizzati da periodi brevi e intensi di I/O elevati con tempi di inattività tra i burst. Per supportare questi tipi di carichi di lavoro, oltre alle velocità di base che un file system può sostenere, Amazon FSx offre la possibilità di

raggiungere velocità più elevate per periodi di tempo sia per le operazioni di I/O di rete che di I/O su disco.

Amazon FSx utilizza un meccanismo di crediti I/O per allocare throughput e IOPS in base all'utilizzo medio: i file system accumulano crediti quando il loro throughput e l'utilizzo di IOPS sono inferiori ai limiti di base e possono utilizzare questi crediti per superare i limiti di base (fino ai limiti di burst) quando necessario. Per ulteriori informazioni sui limiti di burst e sulla durata del file system, consulta. Prestazioni di FSx for Windows File Server

Nella pagina Monitoraggio e prestazioni viene visualizzato un avviso: devo modificare la configurazione del mio file system?

La pagina Monitoraggio e prestazioni include avvisi che indicano quando le richieste recenti del carico di lavoro hanno raggiunto o superato i limiti di risorse determinati dalla configurazione del file system. Ciò non significa necessariamente che sia necessario modificare la configurazione, anche se non si esegue l'azione consigliata, il file system potrebbe non disporre di sufficienti risorse per il carico di lavoro.

Se il carico di lavoro che ha causato l'avviso era atipico e non ti aspetti che continui, può essere sicuro non intraprendere alcuna azione e monitorare attentamente l'utilizzo in futuro. Tuttavia, se il carico di lavoro che ha causato l'avviso è tipico e si prevede che continui o addirittura si intensifichi, consigliamo di seguire l'azione consigliata per aumentare le prestazioni del file server (aumentando la capacità di throughput) o aumentare le prestazioni del volume di archiviazione (aumentando la capacità di archiviazione o passando dallo storage HDD a SSD).

> **Note**
>
> Alcuni eventi del file system possono consumare le risorse prestazionali di I/O del disco e potenzialmente attivare avvisi relativi alle prestazioni. Per esempio:
>
> - La fase di ottimizzazione della scalabilità della capacità di archiviazione può generare un aumento della velocità effettiva del disco, come descritto in Aumento della capacità di storage e delle prestazioni del file system
> - Per i file system Multi-AZ, eventi quali la scalabilità della capacità di throughput, la sostituzione dell'hardware o l'interruzione della zona di disponibilità determinano eventi automatici di failover e failback. Tutte le modifiche ai dati che si verificano durante questo periodo devono essere sincronizzate tra i file server primari e secondari e Windows Server

esegue un processo di sincronizzazione dei dati che può consumare risorse di I/O del disco. Per ulteriori informazioni, consulta Gestione della capacità di throughput.

Le mie metriche mancavano temporaneamente, devo preoccuparmi?

I file system Single-AZ subiranno un'indisponibilità durante la manutenzione del file system, la sostituzione dei componenti dell'infrastruttura e quando non è disponibile una zona di disponibilità. Durante questi periodi, le metriche non saranno disponibili.

In una distribuzione Multi-AZ, Amazon FSx effettua automaticamente il provisioning e mantiene un file server di standby in una zona di disponibilità diversa. In caso di manutenzione del file system o di interruzione non pianificata del servizio, Amazon FSx esegue automaticamente il failover sul file server secondario, consentendoti di continuare ad accedere ai dati senza interventi manuali. Durante il breve periodo in cui il file system è in fase di failover e failback, i parametri potrebbero essere temporaneamente non disponibili.

Informazioni aggiuntive

Questa sezione fornisce un riferimento alle funzionalità di Amazon FSx supportate ma obsolete.

Argomenti

Configurazione di una pianificazione di backup personalizzata

Ti consigliamo di AWS Backup utilizzarlo per impostare una pianificazione di backup personalizzata per il tuo file system. Le informazioni fornite qui sono a scopo di riferimento se è necessario pianificare i backup più frequentemente di quanto sia possibile durante l'utilizzo AWS Backup.

Se abilitato, Amazon FSx for Windows File Server esegue automaticamente un backup del file system una volta al giorno durante una finestra di backup giornaliera. Amazon FSx impone un periodo di conservazione specificato dall'utente per questi backup automatici. Supporta anche backup avviati dall'utente, quindi puoi eseguire backup in qualsiasi momento.

Di seguito, puoi trovare le risorse e la configurazione per implementare una pianificazione dei backup personalizzata. La pianificazione dei backup personalizzata esegue backup avviati dall'utente su un file system Amazon FSx secondo una pianificazione personalizzata definita dall'utente. Alcuni esempi potrebbero essere una volta ogni sei ore, una volta alla settimana e così via. Questo script configura anche l'eliminazione dei backup più vecchi del periodo di conservazione specificato.

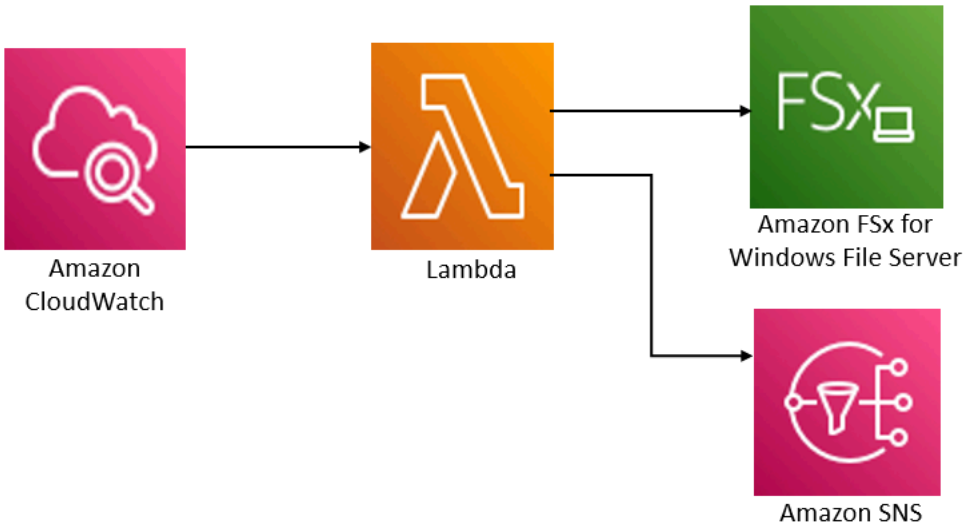
La soluzione distribuisce automaticamente tutti i componenti necessari e utilizza i seguenti parametri:

- Il file system
- Un modello di pianificazione CRON per l'esecuzione dei backup
- Il periodo di conservazione dei backup (in giorni)
- I tag con i nomi di backup

Per ulteriori informazioni sui modelli di pianificazione CRON, consulta Schedule Expressions for Rules nella Amazon CloudWatch User Guide.

Panoramica dell'architettura

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



Questa soluzione esegue le seguenti operazioni:

1. Il AWS CloudFormation modello implementa un CloudWatch evento, una funzione Lambda, una coda Amazon SNS e un ruolo IAM. Il ruolo IAM consente alla funzione Lambda di richiamare le operazioni dell'API Amazon FSx.
2. L' CloudWatch evento viene eseguito secondo una pianificazione definita come pattern CRON, durante la distribuzione iniziale. Questo evento richiama la funzione Lambda del gestore di backup della soluzione che richiama l'operazione dell'API Amazon FSx `CreateBackup` per avviare un backup.
3. Il backup manager recupera un elenco di backup esistenti avviati dall'utente per il file system specificato utilizzando. `DescribeBackups` Quindi elimina i backup precedenti al periodo di conservazione specificato durante la distribuzione iniziale.
4. Il backup manager invia un messaggio di notifica alla coda di Amazon SNS in caso di backup riuscito se scegli l'opzione per ricevere una notifica durante la distribuzione iniziale. Una notifica viene sempre inviata in caso di errore.

AWS CloudFormation modello

Questa soluzione consente AWS CloudFormation di automatizzare l'implementazione della soluzione di pianificazione del backup personalizzata Amazon FSx. Per utilizzare questa soluzione, scarica il modello fsx-scheduled-backup.template. AWS CloudFormation

Distribuzione automatizzata

La procedura seguente configura e implementa questa soluzione di pianificazione dei backup personalizzata. L'implementazione richiede circa cinque minuti. Prima di iniziare, devi avere l'ID di un file system Amazon FSx in esecuzione su Amazon Virtual Private Cloud (Amazon VPC) nel tuo account. AWS Per ulteriori informazioni sulla creazione di queste risorse, consulta. Guida introduttiva ad Amazon FSx for Windows File Server

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

Per avviare lo stack di soluzioni di backup personalizzate

1. Scarica il modello AWS CloudFormation fsx-scheduled-backup.template. Per ulteriori informazioni sulla creazione di uno AWS CloudFormation stack, vedere Creazione di uno stack sulla console nella Guida per l'utente. AWS CloudFormation AWS CloudFormation

   > **Note**
   >
   > Per impostazione predefinita, questo modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). AWS Amazon FSx è attualmente disponibile solo in alcuni casi specifici. Regioni AWSÈ necessario avviare questa soluzione in una AWS regione in cui è disponibile Amazon FSx. Per ulteriori informazioni, consulta la sezione Amazon FSx Regioni AWS e gli endpoints 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
ID del file system Amazon FSx	Nessun valore predefinito	L'ID del file system del file system di cui desideri eseguire il backup.

Parametro	Predefinito	Descrizione
Schema di pianificazione CRON per i backup.	0 0/4 * *? *	La pianificazione per l'esecuzione dell' CloudWatch evento, l'attivazione di un nuovo backup e l'eliminazione dei vecchi backup al di fuori del periodo di conservazione.
Conservazione del backup (giorni)	30	Il numero di giorni in cui conservare i backup avviati dall'utente. La funzione Lambda elimina i backup avviati dall'utente più vecchi di questo numero di giorni.
Nome per i backup	backup pianificato dall'utente	Il nome di questi backup, visualizzato nella colonna Backup Name della console di gestione Amazon FSx.
Notifiche di backup	Sì	Scegli se ricevere una notifica quando i backup vengono avviati correttamente. Viene sempre inviata una notifica in caso di errore.
Indirizzo e-mail	Nessun valore predefinito	L'indirizzo e-mail a cui iscriversi alle notifiche SNS.

3. Seleziona Successivo.
4. Per Opzioni, scegli Avanti.
5. Per Revisione, rivedi e conferma le impostazioni. È necessario selezionare la casella di controllo per confermare che il modello crea risorse IAM.
6. Scegli Crea per distribuire lo stack.

Puoi visualizzare lo stato dello stack nella AWS CloudFormation console nella colonna Status. Dovresti vedere lo stato di CREATE_COMPLETE tra circa cinque minuti.

Opzioni aggiuntive

Puoi utilizzare la funzione Lambda creata da questa soluzione per eseguire backup pianificati personalizzati di più di un file system Amazon FSx. L'ID del file system viene passato alla funzione Amazon FSx nell'input JSON dell'evento. CloudWatch Il JSON predefinito passato alla funzione Lambda è il seguente, in cui i valori `FileSystemId` per `SuccessNotification` e vengono passati dai parametri specificati all'avvio AWS CloudFormation dello stack.

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
}
```

Per pianificare i backup per un file system Amazon FSx aggiuntivo, crea CloudWatch un'altra regola di evento. A tale scopo, è possibile utilizzare l'origine dell'evento Schedule, con la funzione Lambda creata da questa soluzione come destinazione. Scegliete Constant (testo JSON) in Configura input. Per l'input JSON, è sufficiente sostituire l'ID del file system Amazon FSx di cui eseguire il backup al posto di. `${FileSystemId}` Inoltre, sostituiscilo con `Yes` o al posto del `No` codice JSON riportato sopra`${SuccessNotification}`.

Eventuali regole di CloudWatch evento aggiuntive create manualmente non fanno parte dello stack di soluzioni AWS CloudFormation di backup pianificato personalizzate Amazon FSx. Pertanto, non vengono rimosse se elimini lo stack.

Utilizzo della replica del file system distribuito di Microsoft

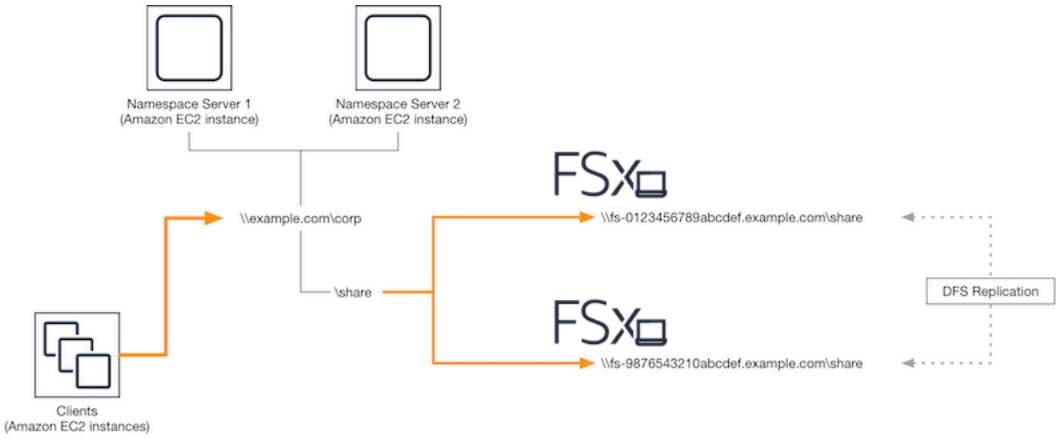
> **Note**
>
> Per implementare l'alta disponibilità per un FSx for Windows File Server, consigliamo di utilizzare Amazon FSx Multi-AZ. Per ulteriori informazioni su Amazon FSx Multi-AZ, consulta Disponibilità e durabilità: file system Single-AZ e Multi-AZ

Amazon FSx supporta l'uso del Microsoft Distributed File System (DFS) per le implementazioni di file system su più zone di disponibilità (AZ) per ottenere disponibilità e durabilità Multi-AZ. Utilizzando DFS Replication, puoi replicare automaticamente i dati tra due file system. Utilizzando DFS Namespaces, è possibile configurare un file system come principale e l'altro come standby, con failover automatico in standby se il principale non risponde.

Prima di utilizzare DFS Replication, procedi nel seguente modo:

- Configura i tuoi gruppi di sicurezza come descritto in Step 8 Getting Started with Amazon FSx.
- Crea due file system Amazon FSx in diverse AZ all'interno di una regione. AWS Per ulteriori informazioni sulla creazione dei tuoi file system, consulta. Scrivi dati nella tua condivisione di file
- Assicuratevi che entrambi i file system siano nello stesso sistema AWS Directory Service for Microsoft Active Directory.
- Dopo aver creato i file system, prendete nota degli ID dei relativi file system per utilizzarli in seguito.

Nei seguenti argomenti, puoi trovare una descrizione di come configurare e utilizzare DFS Replication e il failover dei namespace DFS tra AZ con Amazon FSx.



Configurazione della replica DFS

Puoi utilizzare DFS Replication per replicare automaticamente i dati tra due file system Amazon FSx. Questa replica è bidirezionale, il che significa che è possibile scrivere su entrambi i file system e le modifiche vengono replicate sull'altro.

> **Important**
>
> Non è possibile utilizzare l'interfaccia utente di gestione DFS negli Strumenti di amministrazione di Microsoft Windows (dfsmgmt.msc) per configurare la replica DFS sul file system FSx for Windows File Server.

Per configurare la replica DFS (con script)

1. Inizia il processo di gestione di DFS avviando l'istanza e collegandola a Microsoft Active Directory dove hai inserito i tuoi file system Amazon FSx. A tale scopo, scegli una delle seguenti procedure dalla Guida all'AWS Directory Service amministrazione:

   - Aggiunta di un'istanza EC2 Windows
   - Collegamento manuale di un'istanza Windows

2. Connect alla propria istanza come utente di Active Directory membro del gruppo di amministratori del file system. In AWS Managed AD, questo gruppo è denominato AWS Delegated FSx Administrators. In Microsoft AD autogestito, questo gruppo è denominato Domain Admins o il nome personalizzato per il gruppo di amministratori fornito durante la creazione.

   Questo utente deve inoltre essere membro di un gruppo a cui sono state delegate le autorizzazioni di amministrazione DFS. In AWS Managed AD, questo gruppo è denominato AWS Delegated Distributed File System Administrators. Nel tuo AD autogestito, questo utente deve essere membro di Domain Admins o di un altro gruppo a cui hai delegato le autorizzazioni di amministrazione DFS.

   Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.

3. Scarica lo script FSX-DFSR-Setup.ps1 PowerShell .
4. Apri il menu Start ed entra. PowerShell Dall'elenco, scegli Windows PowerShell.
5. Esegui lo PowerShell script con i seguenti parametri specificati per stabilire la replica DFS tra i tuoi due file system:

   - I nomi del gruppo e della cartella DFS Replication
   - Il percorso locale della cartella che desideri replicare sui tuoi file system (ad esempio, `D:\share` per la condivisione predefinita inclusa nel file system Amazon FSx)
   - I nomi DNS dei file system Amazon FSx primari e in standby creati nei passaggi preliminari

Example

```
FSx-DFSr-Setup.ps1 -group Group -folder Folder -path ContentPath -
primary FSxFileSystem1-DNS-Name -standby FSxFileSystem2-DNS-Name
```

Per configurare la replica DFS (passo dopo passo)

1. Inizia il processo di gestione di DFS avviando l'istanza e collegandola a Microsoft Active Directory dove hai inserito i tuoi file system Amazon FSx. A tale scopo, scegli una delle seguenti procedure dalla Guida all'AWS Directory Service amministrazione:

   - Aggiunta di un'istanza EC2 Windows
   - Collegamento manuale di un'istanza Windows

2. Connect alla propria istanza come utente di Active Directory membro del gruppo di amministratori del file system. In AWS Managed AD, questo gruppo è denominato AWS Delegated FSx Administrators. In Microsoft AD autogestito, questo gruppo è denominato Domain Admins o il nome personalizzato per il gruppo di amministratori fornito durante la creazione.

   Questo utente deve inoltre essere membro di un gruppo a cui sono state delegate le autorizzazioni di amministrazione DFS. In AWS Managed AD, questo gruppo è denominato AWS Delegated Distributed File System Administrators. Nel tuo AD autogestito, questo utente deve essere membro di Domain Admins o di un altro gruppo a cui hai delegato le autorizzazioni di amministrazione DFS.

   Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.

3. Apri il menu Start ed entra PowerShell. Dall'elenco, scegli Windows PowerShell.

4. Se non hai già installato gli strumenti di gestione DFS, installali sulla tua istanza con il seguente comando.

   ```
   Install-WindowsFeature RSAT-DFS-Mgmt-Con
   ```

5. Dal PowerShell prompt, crea un gruppo e una cartella di replica DFS con i seguenti comandi.

   ```
   $Group = "Name of the DFS Replication group"
   $Folder = "Name of the DFS Replication folder"
   ```

```
New-DfsReplicationGroup -GroupName $Group
New-DfsReplicatedFolder -GroupName $Group -FolderName $Folder
```

6. Determina il nome del computer Active Directory associato a ciascun file system con i seguenti comandi.

```
$Primary = "DNS name of the primary FSx file system"
$Standby = "DNS name of the standby FSx file system"

$C1 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -
eq 'HOST/$Primary'").Name
$C2 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -
eq 'HOST/$Standby'").Name
```

7. Aggiungi i tuoi file system come membri del gruppo DFS Replication creato con i seguenti comandi.

```
Add-DfsrMember -GroupName $Group -ComputerName $C1
Add-DfsrMember -GroupName $Group -ComputerName $C2
```

8. Utilizzate i seguenti comandi per aggiungere il percorso locale (ad esempio,`D:\share`) per ogni file system al gruppo DFS Replication. In questa procedura, *`file system 1`* funge da membro principale, il che significa che il suo contenuto viene inizialmente sincronizzato con l'altro file system.

```
$ContentPath1 = "Local path to the folder you want to replicate on file system 1"
$ContentPath2 = "Local path to the folder you want to replicate on file system 2"

Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath1
 -ComputerName $C1 -PrimaryMember $True
Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath2
 -ComputerName $C2 -PrimaryMember $False
```

9. Aggiungere una connessione tra i file system con il seguente comando.

```
Add-DfsrConnection -GroupName $Group -SourceComputerName $C1 -
DestinationComputerName $C2
```

Entro pochi minuti, entrambi i file system dovrebbero iniziare a sincronizzare il contenuto del file precedente `ContentPath` specificato.

Configurazione dei namespace DFS per il failover

È possibile utilizzare i namespace DFS per trattare un file system come principale e l'altro come file di standby. In questo modo, è possibile configurare il failover automatico in standby se il primario non risponde. DFS Namespaces consente di raggruppare cartelle condivise su server diversi in un unico Namespace, dove un singolo percorso di cartella può portare a file archiviati su più server. I namespace DFS sono gestiti dai server DFS Namespace, che indirizzano le istanze di calcolo che mappano una cartella DFS Namespace ai file server appropriati.

Per configurare i namespace DFS per il failover (UI)

1. Se non disponi già di server DFS Namespace in esecuzione, avvia un paio di server DFS Namespace ad alta disponibilità utilizzando il modello Setup-DFSN-Servers.template. AWS CloudFormation Per ulteriori informazioni sulla creazione di uno stack, consulta Creazione di uno stack sulla console nella Guida per l'utente. AWS CloudFormation AWS CloudFormation AWS CloudFormation
2. Connect a uno dei server DFS Namespace avviati nel passaggio precedente come utente del gruppo AWS Delegated Administrators. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
3. Apri la console di gestione DFS. Apri il menu Start ed `dfsmgmt.msc` esegui. In questo modo si apre lo strumento GUI di gestione DFS.
4. In Azione, scegli Nuovo spazio dei nomi e inserisci il nome del computer del primo server DFS Namespace che hai avviato per Server e scegli Avanti.
5. Per Nome, inserisci lo spazio dei nomi che stai creando (ad esempio,). **`corp`**
6. Scegli Modifica impostazioni e imposta le autorizzazioni appropriate in base alle tue esigenze. Seleziona Successivo.
7. Mantieni selezionata l'opzione predefinita dello spazio dei nomi basato sul dominio, mantieni selezionata l'opzione Abilita la modalità Windows Server 2008 e scegli Avanti.

   > **Note**
   >
   > La modalità Windows Server 2008 è l'ultima opzione disponibile per i namespace.

8. Controlla le impostazioni del namespace e scegli Crea.

9. Con lo spazio dei nomi appena creato selezionato in Namespace nella barra di navigazione, scegli Azione, quindi Aggiungi server dello spazio dei nomi.
10. Per il server Namespace, inserisci il nome del computer del secondo server DFS Namespace che hai avviato.
11. Scegliete Modifica impostazioni, impostate le autorizzazioni appropriate in base ai vostri requisiti e scegliete OK.
12. ***Scegli Aggiungi, inserisci il nome UNC della condivisione di file sul file system Amazon FSx principale (ad esempio\\ fs-0123456789abcdef0 .example.com\ share) per Path to folder target e scegli OK.***
13. ***Scegli Aggiungi, inserisci il nome UNC della condivisione di file sul file system Amazon FSx in standby (ad esempio,\\ fs-fedbca9876543210f .example.com\ share) per Path to folder target e scegli OK.***
14. Nella finestra Nuova cartella, scegli OK. La nuova cartella viene creata con le due destinazioni delle cartelle nel tuo namespace.
15. Ripeti gli ultimi tre passaggi per ogni condivisione di file che desideri aggiungere al tuo namespace.

Per configurare i namespace DFS per il failover () PowerShell

1. Se non disponi già di server DFS Namespace in esecuzione, avvia un paio di server DFS Namespace ad alta disponibilità utilizzando il modello Setup-DFSN-Servers.template. AWS CloudFormation Per ulteriori informazioni sulla creazione di uno stack, consulta Creazione di uno stack sulla console nella Guida per l'utente. AWS CloudFormation AWS CloudFormation AWS CloudFormation
2. Connect a uno dei server DFS Namespace avviati nel passaggio precedente come utente del gruppo AWS Delegated Administrators. Per ulteriori informazioni, consulta Connessione all'istanza Windows nella Guida per l'utente di Amazon EC2.
3. Apri il menu Start ed entra PowerShell. Windows PowerShell appare nell'elenco delle corrispondenze.
4. Apri il menu contestuale (fai clic con il pulsante destro del mouse) per Windows PowerShell e scegli Esegui come amministratore.
5. Se non hai già installato DFS Management Tools, installalo sulla tua istanza con il seguente comando.

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

6. Se non disponi già di un namespace DFS esistente, puoi crearne uno utilizzando i seguenti comandi. PowerShell

```
$NSS1 = computer name of the 1st DFS Namespace server
$NSS2 = computer name of the 2nd DFS Namespace server

$DNSRoot = fully qualified Active Directory domain name (e.g. mydomain.com)
$Namespace = Namespace name you want to use
$Folder = Folder path you want to use within the Namespace
$FS1FolderTarget = Share path to Folder Target on File System 1
$FS2FolderTarget = Share path to Folder Target on File System 2

$NSS1,$NSS2 | ForEach-Object { Invoke-Command -ComputerName $_ -ScriptBlock { mkdir
 “C:\DFS\${using:Namespace}”;
New-SmbShare -Name ${using:Namespace} -Path “C:\DFS\${using:Namespace}” } }

New-DfsnRoot -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS1}.${DNSRoot}\
${Namespace}" -Type DomainV2
New-DfsnRootTarget -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS2}.
${DNSRoot}\${Namespace}"
```

7. Per creare una cartella all'interno del tuo spazio dei nomi DFS, puoi usare il seguente comando. PowerShell In questo modo viene creata una cartella che indirizza le istanze di calcolo che accedono alla cartella verso il file system Amazon FSx primario per impostazione predefinita.

```
$FS1 = DNS name of primary FSx file system
New-DfsnFolder -Path “\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath “\\${FS1}\
${FS1FolderTarget}” -EnableTargetFailback $True -ReferralPriorityClass GlobalHigh
```

8. Aggiungi il tuo file system Amazon FSx in standby alla stessa cartella DFS Namespace. Le istanze di calcolo che accedono alla cartella rientrano in questo file system se non riescono a connettersi al file system Amazon FSx primario.

```
$FS2 = DNS name of secondary FSx file system
New-DfsnFolderTarget -Path “\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath “\\
${FS2}\${FS2FolderTarget}”
```

Ora puoi accedere ai dati dalle istanze di calcolo utilizzando il percorso remoto della cartella DFS Namespace specificato in precedenza. In questo modo le istanze di calcolo vengono indirizzate al file system Amazon FSx primario (e al file system di standby, se il file system primario non risponde).

Ad esempio, apri il menu Start ed entra. `PowerShell` Dall'elenco, scegli `Windows PowerShell` ed esegui il comando seguente.

```
net use Z: \\${DNSRoot}\${Namespace}\${Folder} /persistent:yes
```

Utilizzo di Windows di manutenzione e FSx Multi-AZ

Per garantire un'elevata disponibilità della distribuzione del file system Multi-AZ, ti consigliamo di scegliere finestre di manutenzione non sovrapposte per i due file system Amazon FSx nella tua implementazione Multi-AZ. In questo modo è possibile garantire che i dati dei file continuino a essere disponibili per le applicazioni e gli utenti durante le finestre di manutenzione del sistema.

> **Note**
>
> Per consentire il traffico di replica DFS da e verso i file system, assicurati di aggiungere le regole in entrata e in uscita del gruppo di sicurezza VPC come descritto in. Gruppi di sicurezza Amazon VPC

Cronologia dei documenti

- Versione API: 2018-03-01
- Ultimo aggiornamento della documentazione: 17 gennaio 2024

La tabella seguente descrive importanti modifiche alla Amazon FSx Windows User Guide. Per ricevere notifiche sugli aggiornamenti della documentazione, è possibile sottoscrivere il feed RSS.

Modifica	Descrizione	Data
Support aggiunto per livelli più elevati di IOPS su file system con capacità di throughput pari o superiori a 4 Gb/s	FSx for Windows File Server sta aumentando gli IOPS massimi da 130.000 a 150.000 per file system con capacità di throughput di 4 GB/s o superiore, da 175K a 200K per file system con capacità di trasmissione di 6 GB/s o superiore, da 260K a 300K per file system con capacità di throughput di 9 GB/s o superiore e da 350K a 400K per file system con 12 GB/s di capacità di throughput o superiore. Per ulteriori informazioni, consulta FSx for Windows File Server performance.	17 gennaio 2024
Amazon FSX ha aggiornato le politiche gestite di AmazonFSx FullAccess, AmazonFSx ConsoleFullAccess, AmazonFe SxReadOnlyAccess AmazonF SxConsole	Amazon FSX ha aggiornato le politiche AmazonFSx FullAccess, AmazonF, AmazonF SxConsoleFullAccess e AmazonF per SxReadOnlyAccess aggiungere l'autorizzazioneSxConsoleRe	9 gennaio 2024

ReadOnlyAccess SxService RolePolicy AWS	adOnlyAccess. SxService RolePolicy `ec2:GetSecurityGroupsForVpc` Per ulteriori informazioni, consulta gli aggiornamenti di Amazon FSx alle policy AWS gestite.	
Amazon FSx ha aggiornato le politiche gestite di AmazonFSxFullAccess e AmazonFSxConsoleFullAccess AWS	Amazon FSx ha aggiornato le politiche AmazonF SxFullAccess e AmazonF SxConsole FullAccess per aggiungere l'azione. `ManageCrossAccountDataReplication` Per ulteriori informazioni, consulta gli aggiornamenti di Amazon FSx alle policy AWS gestite.	20 dicembre 2023
Amazon FSx ha aggiornato le politiche gestite di AmazonFSxFullAccess e AmazonFSxConsoleFullAccess AWS	Amazon FSX ha aggiornato le politiche AmazonF SxFullAccess e AmazonF SxConsole FullAccess per aggiungere l'autorizzazione. `fsx:CopySnapshotAndUpdateVolume` Per ulteriori informazioni, consulta gli aggiornamenti di Amazon FSx alle policy AWS gestite.	26 novembre 2023

Amazon FSx ha aggiornato le politiche gestite di AmazonFSxFullAccess e AmazonFSxConsoleFullAccess AWS	Amazon FSX ha aggiornato le SxConsoleFullAccess politiche AmazonF SxFullAccess e AmazonF per aggiungere le autorizzazioni e. `fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` Per ulteriori informazioni, consulta gli aggiornamenti di Amazon FSx alle policy AWS gestite.	14 novembre 2023
Support aggiunto per l'aggiornamento del tipo di storage del file system	I file system FSx for Windows File Server ora supportano l'aggiornamento dal tipo di storage HDD al tipo di storage SSD. Per ulteriori informazioni, vedere Gestione del tipo di archiviazione.	9 agosto 2023
Support aggiunto per una maggiore capacità di throughput massima	I file system FSx for Windows File Server ora supportano una capacità di throughput fino a 12 GBps. Per ulteriori informazioni, consulta FSx for Windows File Server performance.	9 agosto 2023

Support aggiunto per il provisioning di IOPS SSD	I file system FSx for Windows File Server ora supportano il provisioning di IOPS SSD indipendentemente dalla capacità di archiviazione, fino a un massimo di 350.000 IOPS. Per ulteriori informazioni, vedere Gestione degli IOPS SSD.	9 agosto 2023
Amazon FSx ha aggiornato la policy gestita di SxService RolePolicy AWS AmazonF	Amazon FSx ha aggiornato l'`cloudwatch:PutMetricData` autorizzazione in AmazonF. SxServiceRolePolicy Per ulteriori informazioni, consulta AmazonF. SxService RolePolicy	24 luglio 2023
Amazon FSx ha aggiornato la policy gestita di SxFullAccess AWS AmazonF	Amazon FSx ha aggiornato la SxFullAccess policy di AmazonF per rimuovere l'`fsx:*`autorizzazione e aggiungere azioni specifiche. `fsx` Per ulteriori informazioni, consulta la politica di AmazonF. SxFullAccess	13 luglio 2023
Amazon FSx ha aggiornato la policy gestita di SxConsole FullAccess AWS AmazonF	Amazon FSx ha aggiornato la SxConsoleFullAccess policy di AmazonF per rimuovere l'`fsx:*`autorizzazione e aggiungere azioni specifiche. `fsx` Per ulteriori informazioni, consulta la politica di AmazonF. SxConsole FullAccess	13 luglio 2023

Supporto aggiunto per nuove CloudWatch metriche per Amazon FSx for Windows File Server	FSx for Windows File Server ora fornisce metriche CloudWatch aggiuntive per monitorare le prestazioni e l'utilizzo della capacità dei file server e dei volumi di storage. Per ulteriori informazioni, consulta Metriche e dimensioni.	22 settembre 2022
Support aggiunto per gli avvisi sulle prestazioni del file system	Amazon FSx ora fornisce avvisi nella finestra Prestazioni e monitoraggio quando una serie di CloudWatch parametri si avvicina o supera soglie predeterminate per tali parametri. Ogni avviso fornisce anche una raccomandazione pratica per migliorare le prestazioni del file system. Per ulteriori informazioni, consulta Avvertenze e raccomandazioni sulle prestazioni.	22 settembre 2022

Support aggiunto per un migliore monitoraggio delle prestazioni del file system	La dashboard di monitoraggio del file system della console Amazon FSx per i file system FSx for Windows File Server include nuove sezioni Riepilogo, Archiviazione e Prestazioni. Queste sezioni mostrano grafici di nuove CloudWatch metriche che forniscono un monitoraggio avanzato delle prestazioni. Per ulteriori informazioni, consulta Monitoraggio delle metriche con. CloudWatch	22 settembre 2022
Support aggiunto per gli AWS PrivateLink endpoint VPC di interfaccia.	Ora puoi utilizzare gli endpoint VPC dell'interfaccia per accedere all'API Amazon FSx dal tuo VPC senza inviare traffico su Internet. Per ulteriori informazioni, consulta Amazon FSx e interfaccia gli endpoint VPC.	5 aprile 2022
Support aggiunto per Amazon Kendra	Ora puoi utilizzare il file system FSx for Windows File Server come fonte di dati per Amazon Kendra, consentendoti di indicizzare e cercare informazioni contenute nei documenti archiviati nel tuo file system. Per ulteriori informazioni, consulta Usare FSx for Windows File Server con Amazon Kendra.	26 marzo 2022

Support aggiunto per il controllo dell'accesso ai file	Ora puoi abilitare il controllo degli accessi degli utenti finali su file, cartelle e condivisi oni di file. Puoi scegliere di inviare i log degli eventi di controllo ai servizi Amazon CloudWatch Logs o Amazon Data Firehose. Per ulteriori informazioni, consulta Controllo dell'accesso ai file.	8 giugno 2021
Support aggiunto per la copia dei backup	Ora puoi usare Amazon FSx per copiare i backup all'inter no dello stesso AWS account su un altro Regione AWS (copie tra regioni) o all'inter no dello stesso (copie all'inter no della stessa Regione AWS regione). Per ulteriori informazi oni, consulta Copiare i backup.	12 Aprile 2021
Aumenta automaticamente la capacità di archiviazione di un file system	Utilizza un AWS CloudForm ation modello personali zzabile AWS sviluppato per aumentare automaticamente la capacità di archiviazione del file system quando la capacità raggiunge una soglia specifica ta. Per ulteriori informazi oni, consulta Aumentare la capacità di archiviazione in modo dinamico.	17 febbraio 2021

Support aggiunto per l'accesso del client tramite indirizzi IP non privati	È possibile accedere ai file system FSx for Windows File Server con client locali utilizzando indirizzi IP non privati. Per ulteriori informazioni, vedere Ambienti supportati. È possibile unire il file system FSx for Windows File Server a un Microsoft Active Directory autogestito con server DNS e controller di dominio AD che utilizzano indirizzi IP non privati. Per ulteriori informazioni, consulta Utilizzo di Amazon FSx con Microsoft Active Directory autogestito.	17 dicembre 2020
Support aggiunto per l'utilizzo degli alias DNS	È ora possibile associare gli alias DNS ai file system FSx for Windows File Server che è possibile utilizzare per accedere ai dati sul file system. Per ulteriori informazioni, vedere Gestione degli alias DNS e Procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.	9 novembre 2020
Supporto aggiunto per Amazon Elastic Container Service	Ora puoi usare FSx for Windows File Server con Amazon ECS. Per ulteriori informazioni, consulta Supported Clients.	9 novembre 2020

Amazon FSx è ora integrato con AWS Backup	Ora puoi utilizzarli AWS Backup per eseguire il backup e il ripristino dei file system FSx oltre a utilizzare i backup nativi di Amazon FSx. Per ulteriori informazioni, consulta Utilizzo AWS Backup con Amazon FSx.	9 novembre 2020
Support aggiunto per la scalabilità della capacità di throughput	Ora è possibile modificar e la capacità di throughpu t per i file system FSx for Windows File Server esistenti man mano che i requisiti di throughput evolvono. Per ulteriori informazioni, vedere Gestione della capacità di throughput.	1 giugno 2020
Support aggiunto per la scalabilità della capacità di archiviazione	Ora è possibile aumentare la capacità di storage per i file system FSx for Windows File Server esistenti man mano che i requisiti di storage evolvono. Per ulteriori informazioni, vedere Gestione della capacità di storage.	1 giugno 2020
Support aggiunto per l'archivi azione su disco rigido (HDD)	Lo storage su disco rigido offre flessibilità in termini di prezzi e prestazioni quando si utilizza FSx for Windows File Server. Per ulteriori informazi oni, consulta Ottimizzazione dei costi con Amazon FSx.	26 marzo 2020

Support aggiunto per il trasferimento di file tramite AWS DataSync	È ora possibile AWS DataSync utilizzarlo per trasferire file da e verso FSx for Windows File Server. Per ulteriori informazioni, consulta Migrare i file su Amazon FSx for Windows File Server Using. AWS DataSync	4 febbraio 2020
FSx for Windows File Server rilascia il supporto per ulteriori attività di amministrazione del file system Windows	Ora puoi gestire e amministrare le condivisioni di file, la deduplicazione dei dati, le quote di storage e la crittografia in transito per le tue condivisioni di file utilizzando l'interfaccia a riga di comando di Amazon FSx per la gestione remota su. PowerShell Per ulteriori informazioni, consulta Amministrazione dei file system.	20 novembre 2019
FSx for Windows File Server rilascia il supporto Multi-AZ nativo	È possibile utilizzare l'implementazione Multi-AZ per FSx for Windows File Server per creare più facilmente file system ad alta disponibilità che si estendono su più zone di disponibilità (AZ). Per ulteriori informazioni, consulta l'argomento relativo a disponibilità e durabilità: file system Single-AZ e Multi-AZ.	20 novembre 2019

FSx for Windows File Server rilascia il supporto per la gestione delle sessioni utente e dei file aperti	È ora possibile utilizzare lo strumento Cartelle condivise nativo di Microsoft Windows per gestire le sessioni utente e aprire file sui file system FSx for Windows File Server. Per ulteriori informazioni, vedere Gestione delle sessioni utente e dei file aperti.	17 ottobre 2019
Amazon FSx rilascia il supporto per le copie shadow di Microsoft Windows	È ora possibile configurare le copie shadow di Windows sui file system FSx for Windows File Server. Le copie shadow consentono agli utenti di annullare facilmente le modifiche ai file e confrontare le versioni dei file ripristinando i file nelle versioni precedenti. Per ulteriori informazioni, consultate Working with Shadow Copies.	31 luglio 2019
Amazon FSx rilascia il supporto condiviso per Microsoft Active Directory	È ora possibile unire i file system FSx for Windows File Server AWS Managed Microsoft AD a directory che si trovano in un VPC diverso o in un file system Account AWS diverso. Per ulteriori informazioni, consulta Active Directory Support.	25 giugno 2019

Amazon FSx rilascia il supporto avanzato per Microsoft Active Directory	Ora puoi aggiungere i file system FSx for Windows File Server ai tuoi domini Microsoft Active Directory autogestiti, in locale o nel cloud. Per ulteriori informazioni, consulta Active Directory Support.	24 giugno 2019
Amazon FSx è conforme alla certificazione SOC	Amazon FSx è stato valutato come conforme alla certifica zione SOC. Per ulteriori informazioni, consulta Sicurezza e protezione dei dati.	16 maggio 2019
Aggiunta una nota chiarific atrice riguardante AWS Direct Connect il supporto per connessioni peering VPN e VPC interregionali	I file system Amazon FSx creati dopo il 22 febbraio 2019 sono accessibili tramite VPN e AWS Direct Connect peering VPC interregionale. Per ulteriori informazioni, consulta Metodi di accesso supportati.	25 febbraio 2019
AWS Direct Connect, Aggiunto il supporto per connessioni peering VPN e VPC interregi onali	Ora puoi accedere ai file system Amazon FSx for Windows File Server da risorse locali e da risorse in un altro Amazon VPC o. Account AWS Per ulteriori informazioni, consulta Metodi di accesso supportati.	22 febbraio 2019

Amazon FSx è ora disponibile a livello generale	Amazon FSx for Windows File Server fornisce file server Microsoft Windows completamente gestiti, supportati da un file system Windows completamente nativo. Amazon FSx for Windows File Server offre le caratteristiche, le prestazioni e la compatibilità per trasferire facilmente le applicazioni AWS aziendali.	28 novembre 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.