



Guida per l'utente di Windows

File server Amazon FSx per Windows



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

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

I marchi e l'immagine commerciale di Amazon non possono essere utilizzati in relazione a prodotti o servizi che non siano di Amazon, in una qualsiasi modalità che possa causare confusione tra i clienti o in una qualsiasi modalità che denigri o discrediti Amazon. Tutti gli altri marchi non di proprietà di Amazon sono di proprietà dei rispettivi proprietari, che possono o meno essere affiliati, collegati o sponsorizzati da Amazon.

Table of Contents

Che cos'è FSx per Windows File Server?	1
FSx Risorse Amazon	1
Accesso alle condivisioni di file	2
Sicurezza e protezione dei dati	2
Disponibilità e durabilità	3
Gestione dei file system	3
Flessibilità in termini di prezzi e prestazioni	3
Prezzi per Amazon FSx	4
Presupposti	4
Prerequisiti	4
Forum FSx di Amazon per Windows File Server	5
Sei un utente di Amazon FSx per la prima volta?	5
FSx per le best practice di Windows	6
Best practice generali	6
Creazione di un piano di monitoraggio	6
Garantire che i file system dispongano di risorse sufficienti	6
Best practice di sicurezza	6
Sicurezza di rete	7
Active Directory	7
Evita di perdere la disponibilità a causa di una configurazione errata di Active Directory	8
Windows ACLs	9
Configurazione e dimensionamento corretto del file system	9
Selezione di un tipo di distribuzione	9
Selezione di una capacità di throughput	10
Aumento della capacità di archiviazione e della capacità di throughput	10
Modifica della capacità di throughput durante i periodi di inattività	11
Nozioni di base	12
Configurare il Account AWS	12
.....	13
Passaggio 1. Configurazione di un Active Directory	15
Fase 2: Avvio di un'istanza Windows nella console Amazon EC2	16
Fase 3: connessione all'istanza	18
Passaggio 4: Unisci l'istanza alla tua Directory Service directory	20
Fase 5. Crea il tuo file system	21

Fase 6. Mappa la condivisione di file su un'istanza EC2 che esegue Windows Server	28
Fase 7. Scrivi dati nella tua condivisione di file	29
Fase 8. Esegui il backup del file system	29
Fase 9. Eseguire la pulizia delle risorse	30
Accesso ai tuoi dati	32
Client supportati	32
Accesso ai dati dall'interno di Cloud AWS	33
Accesso ai dati da un altro VPC, oppure Account AWS Regione AWS	35
Accesso ai dati dall'ambiente locale	35
Accesso ai dati utilizzando nomi DNS predefiniti	36
Utilizzo dell'autenticazione Kerberos con nomi DNS	37
Support per gli spazi dei nomi DFS (Distributed File System)	37
Accesso ai dati tramite alias DNS	37
Utilizzo dell'autenticazione e della crittografia Kerberos con alias DNS	38
Associa gli alias DNS al tuo file system	39
Configura i nomi principali dei servizi (SPNs) per Kerberos	40
Aggiorna o crea un record DNS CNAME	44
Applicazione dell'autenticazione Kerberos utilizzando Group Policy Objects () GPOs	45
Accesso ai dati tramite condivisioni di file	46
Mappatura delle condivisioni di file	47
Mappatura di una condivisione di file su un'istanza Amazon EC2 Windows	47
Montaggio di una condivisione di file su un'istanza Amazon EC2 per Mac	50
Montaggio di una condivisione di file su un'istanza Amazon EC2 Linux	53
Monta automaticamente le condivisioni di file su un'istanza Amazon EC2 Linux	58
Gestione delle condivisioni di file	61
Il FSx SmbShare comando New- ha esito negativo con un trust unidirezionale	67
Disponibilità e durabilità	68
Scelta del tipo di implementazione del file system Single-AZ o Multi-AZ	68
Supporto delle funzionalità per tipo di implementazione	69
Processo di failover	70
Esperienza di failover su client Windows	70
Esperienza di failover su client Linux	71
Test del failover su un file system	71
Risorse del file system Single-AZ e Multi-AZ	71
Sottoreti	71
Interfacce di rete elastiche del file system	72

Lavorare con Active Directory	74
Usando AWS Managed Microsoft AD	75
Prerequisiti di rete	76
Utilizzo di un modello di isolamento delle foreste di risorse	80
Verifica la configurazione di Active Directory	81
Utilizzo AWS Managed Microsoft AD in un VPC o account diverso	81
Convalida della connettività ai controller di dominio Active Directory	83
Utilizzo di un Active Directory autogestito	86
Prerequisiti	87
Autorizzazioni dell'account di servizio	92
Procedure consigliate per l'utilizzo di un Active Directory autogestito	93
Account FSx di servizio Amazon	103
Delega dei privilegi ad Amazon FSx	104
Convalida della configurazione di Active Directory	105
Iscriviti FSx a un Active Directory autogestito	110
Ottenere indirizzi IP per le immissioni DNS manuali	119
Aggiornamento di Active Directory autogestito	120
Modifica dell'account del FSx servizio Amazon	122
Monitoraggio degli aggiornamenti di Active Directory gestiti autonomamente	124
Performance	128
Prestazioni del file system	128
Considerazioni aggiuntive sulle prestazioni	129
Latenza	130
Throughput e IOPS	130
Prestazioni con un solo client	130
Prestazioni impennate	130
Capacità di throughput e prestazioni	131
Scelta della capacità di trasmissione	133
Configurazione e prestazioni dello storage	135
Prestazioni HDD burst	135
Esempio: capacità di archiviazione e capacità di throughput	136
Misurazione delle prestazioni mediante metriche CloudWatch	137
Risoluzione dei problemi di prestazioni	137
Determinare il throughput del file system e i limiti di IOPS	138
Cos'è l'I/O di rete I/O rispetto a quello su disco? Perché sono diversi?	138
Perché l'utilizzo della CPU o della memoria è elevato quando la rete I/O è scarsa?	138

Che cos'è lo scoppio? Quanta frammentazione viene utilizzata dal mio file system? Cosa succede quando i crediti burst si esauriscono?	139
Nella pagina Monitoraggio e prestazioni viene visualizzato un avviso: devo modificare la configurazione del mio file system?	139
Le mie metriche mancavano temporaneamente, devo preoccuparmi?	140
Amministrazione dei file system	141
Stato FSx del file system Amazon	142
Utilizzo dell'Amazon FSx CLI per PowerShell	143
Avvio di una PowerShell sessione FSx remota Amazon	145
Attività di configurazione del file system una tantum	146
Gestione del consumo di storage	146
Attivazione delle copie shadow per consentire agli utenti finali di ripristinare file e cartelle nelle versioni precedenti	147
Applicazione della crittografia in transito	147
Risoluzione dei problemi di accesso all'Amazon FSx CLI su PowerShell	148
Il gruppo di sicurezza del file system non dispone delle regole in entrata richieste per consentire una connessione PowerShell remota	148
È configurato un trust esterno tra Microsoft Active Directory AWS gestito e Active Directory locale	148
Si verifica un errore di localizzazione della lingua quando si tenta di avviare una sessione remota PowerShell	148
Finestra di manutenzione	149
Modifica della finestra di manutenzione settimanale	150
Alias DNS	150
Stato dell'alias DNS	153
Utilizzo di alias DNS con Kerberos	153
Visualizzazione degli alias DNS esistenti	153
Associazione degli alias DNS ai file system	154
Gestione degli alias DNS sui file system esistenti	156
Sessioni utente e file aperti	158
Utilizzo della GUI per gestire utenti e sessioni	158
Utilizzato PowerShell per gestire le sessioni utente e aprire file	161
File Server Resource Manager	162
Funzionalità chiave	163
Come iniziare	164
Gestione delle quote	167

Gruppi di file	181
Screening dei file	186
Classificazione dei file	200
Rapporti di archiviazione	221
Attività di gestione dei file	235
Impostazioni FSRM	235
Registri eventi	241
Casi di utilizzo comune	242
Gestione dello storage	250
Ottimizzazione dei costi di archiviazione	250
Gestione della capacità di storage	251
Gestione dei tipi di storage	255
Gestione degli IOPS SSD	256
Deduplicazione dei dati	258
Gestione delle quote di archiviazione	262
Aumento della capacità di storage	263
Il monitoraggio degli aumenti dello storage	265
Aumento dinamico della capacità di storage	268
Aggiornamento del tipo di archiviazione	274
Monitoraggio degli aggiornamenti dei tipi di archiviazione	275
Aggiornamento degli IOPS SSD	276
Monitoraggio degli aggiornamenti IOPS degli SSD forniti	277
Gestione della deduplicazione dei dati	278
Risoluzione dei problemi di deduplicazione dei dati	282
Utilizzo dei namespace DFS	285
Utilizzo dei namespace DFS	285
Miglioramento delle prestazioni con gli shard	286
Raggruppa i file system in un unico spazio dei nomi	286
Suddivisione dei dati utilizzando i namespace DFS per prestazioni di scalabilità orizzontale	288
Gestione della capacità di throughput	290
Come funziona la scalabilità del throughput	291
Sapere quando modificare la capacità di throughput	292
Modifica della capacità di throughput	293
Monitoraggio degli aggiornamenti della capacità di throughput	294
Gestione del tipo di rete	296

Utilizzo della modalità dual-stack	297
Modifica del tipo di rete	297
Applicazione di tag alle risorse	298
Nozioni di base sui tag	299
Tagging delle risorse	299
Limitazioni applicate ai tag	300
Autorizzazioni necessarie per etichettare le risorse	301
Aggiornare un file system utilizzando AWS CLI	301
Protezione dei dati	303
Protezione dei dati con backup	303
Utilizzo di backup giornalieri automatici	305
Utilizzo dei backup avviati dall'utente	306
Utilizzo AWS Backup con Amazon FSx	306
Copia di backup	307
Ripristino dei backup su un nuovo file system	310
Creazione di backup avviati dall'utente	311
Eliminazione di backup	311
Dimensioni dei backup	312
Copia di backup	313
Ripristino di un backup	314
Protezione dei dati con copie shadow	315
Best practice	316
Configurazione di copie shadow	317
Configura le copie shadow per utilizzare le impostazioni predefinite	322
Impostazione della quantità massima di spazio di archiviazione per copie shadow	324
Visualizzazione dell'archiviazione delle copie shadow	326
Creazione di una pianificazione personalizzata delle copie shadow	327
Visualizzazione della pianificazione della copia ombra	329
Creazione di una copia shadow	329
Visualizzazione delle copie shadow esistenti	329
Eliminazione di copie shadow	330
Eliminazione di una pianificazione di copie shadow	331
Eliminazione di una configurazione di copia shadow	332
Risoluzione dei problemi relativi alle copie shadow	332
Replica pianificata	334
Utilizzo FSx per Windows File Server con Microsoft SQL Server	335

Utilizzo di Amazon FSx per i file di dati di Active SQL Server	335
Crea una condivisione sempre disponibile	336
Configurare le impostazioni di timeout SMB	336
Utilizzo di Amazon FSx come testimone della condivisione di file per PMI	336
Migrazione ad Amazon FSx	337
Migrazione dei file verso FSx Windows File Server	337
Le migliori pratiche di migrazione	338
Migrazione di file utilizzando AWS DataSync	338
Migrazione di file con Robocopy	342
Migrazione delle configurazioni di condivisione di file	346
Migrazione della configurazione DNS locale a Windows File Server FSx	348
Passaggio a FSx Windows File Server	350
Preparazione per il passaggio ad Amazon FSx	351
Configura SPNs per l'autenticazione Kerberos	351
Aggiorna i record DNS CNAME per il file system Amazon FSx	355
Monitoraggio dei file system	357
Monitoraggio automatico e manuale	357
Strumenti automatici	357
Strumenti di monitoraggio manuali	358
Monitoraggio con Amazon CloudWatch	359
Parametri e dimensioni	360
Utilizzo delle metriche CloudWatch	366
Avvertenze e raccomandazioni sulle prestazioni	370
Accesso alle metriche del file system	372
Creazione di CloudWatch allarmi	376
CloudTrail registri	379
FSx Informazioni su Amazon in CloudTrail	380
Comprendere le voci dei file di FSx log di Amazon	381
Sicurezza	383
Protezione dei dati	384
Crittografia dei dati	385
Crittografia a riposo	385
Crittografia in transito	387
Windows ACLs	389
Collegamenti correlati	390
Controllo degli accessi ai file system con Amazon VPC	390

Gruppi di sicurezza Amazon VPC	391
Rete Amazon VPC ACLs	395
Registrazione dell'accesso dell'utente finale	395
Controlla le destinazioni del registro degli eventi	397
Migrazione dei controlli di audit	398
Visualizzazione dei registri degli eventi	398
Impostazione dei controlli di controllo di file e cartelle	406
Gestione del controllo degli accessi ai file	408
Gestione dell'identità e degli accessi	413
Destinatari	413
Autenticazione con identità	414
Gestione dell'accesso tramite policy	415
Come funziona Amazon FSx per Windows File Server con IAM	417
Esempi di policy basate su identità	422
AWS politiche gestite	425
Risoluzione dei problemi	443
Usare i tag con Amazon FSx	445
Uso di ruoli collegati ai servizi	451
Convalida della conformità	457
Endpoint VPC di interfaccia	458
Considerazioni sugli endpoint VPC con FSx interfaccia Amazon	458
Creazione di un endpoint VPC di interfaccia per Amazon API FSx	459
Creazione di una policy sugli endpoint VPC per Amazon FSx	459
Utilizzo di altri servizi	460
Utilizzo di Amazon FSx con WorkSpaces le applicazioni Amazon	460
Fornire spazio di archiviazione personale persistente a ciascun utente	461
Fornire una cartella condivisa tra gli utenti	463
Utilizzo FSx per Windows File Server con Amazon Kendra	464
Prestazioni del file system	465
Quote	466
Quote che è possibile incrementare	466
Quote di risorse per ogni file system	468
Ulteriori considerazioni	468
Quote specifiche per Microsoft Windows	469
Risoluzione dei problemi	470
Non riesci ad accedere al tuo file system	470

L'interfaccia elastic network interface del file system è stata modificata o eliminata	471
L'indirizzo IP elastico collegato all'interfaccia di rete elastica del file system è stato eliminato	471
Il gruppo di sicurezza del file system non dispone delle regole in entrata o in uscita richieste.	471
Il gruppo di sicurezza dell'istanza di calcolo non dispone delle regole in uscita richieste	471
Istanza di calcolo non unita a un Active Directory	471
La condivisione di file non esiste	472
L'utente di Active Directory non dispone delle autorizzazioni necessarie	472
Consenti la rimozione delle autorizzazioni ACL NTFS (controllo completo)	472
Impossibile accedere a un file system utilizzando un client locale	472
Il nuovo file system non è registrato nel DNS	473
Impossibile accedere al file system utilizzando un alias DNS	474
Impossibile accedere al file system utilizzando un indirizzo IP	475
La creazione del file system non riesce	475
Gruppo di sicurezza VPC configurato in modo errato	476
Nomi di gruppi di amministratori del file system duplicati	476
Server DNS o controller di dominio non raggiungibili	477
Credenziali dell'account di servizio non valide	478
Amazon non FSx può accedere alle credenziali del tuo account del servizio Active Directory in Gestione dei segreti AWS	480
Autorizzazioni insufficienti per l'account di servizio	482
Capacità dell'account di servizio superata	483
Impossibile accedere all'unità organizzativa	483
Gruppo di amministratori del file system non valido	484
Amazon FSx ha perso la connettività nel dominio	485
L'account di servizio non dispone delle autorizzazioni corrette	485
Caratteri Unicode utilizzati nei parametri di creazione	486
La commutazione del tipo di archiviazione su HDD durante il ripristino di un backup non riesce	487
Il file system è in uno stato configurato in modo errato	487
File system configurato in modo errato: Amazon non FSx riesce a raggiungere né i server DNS né i controller di dominio del tuo dominio.	489
File system configurato in modo errato: le credenziali dell'account di servizio non sono valide	490

File system configurato in modo errato: la chiave Gestione dei segreti AWS segreta o KMS non è configurata correttamente	490
File system configurato in modo errato: l'account di servizio fornito non dispone dell'autorizzazione per aggiungere il file system al dominio	491
File system configurato in modo errato: l'account del servizio non può aggiungere altri computer al dominio	491
File system configurato in modo errato: l'account del servizio non ha accesso all'unità organizzativa	492
Non è possibile configurare DFS-R su un file system Multi-AZ o Single-AZ 2	493
Gli aggiornamenti della capacità di storage o di throughput non riescono	493
L'aumento della capacità di storage non riesce perché Amazon non FSx può accedere al file system AWS KMS key	493
L'aggiornamento della capacità di storage o di throughput non riesce perché l'Active Directory autogestito non è configurato correttamente	494
L'aumento della capacità di storage non riesce a causa dell'insufficiente capacità di throughput	494
L'aggiornamento della capacità di throughput a 8 non riesce MBps	494
Cronologia dei documenti	495
.....	dxi

Che cos'è FSx per Windows File Server?

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

Amazon FSx supporta un'ampia gamma di carichi di lavoro Windows aziendali con storage di file completamente gestito basato su Microsoft Windows Server. Amazon FSx offre il supporto nativo per le funzionalità del file system di Windows e per il protocollo Server Message Block (SMB) standard di settore per accedere allo storage di file su una 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.

Con lo storage di file su Amazon FSx, il codice, le applicazioni e gli strumenti utilizzati oggi da sviluppatori e amministratori Windows possono continuare a funzionare senza modifiche. 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.

Essendo un servizio completamente gestito, FSx per Windows File Server elimina il sovraccarico amministrativo legato alla configurazione e al 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](#), [WorkSpaces](#), [AWS Key Management Service](#), [Amazon](#) e [AWS CloudTrail](#).

FSx per le risorse di Windows File Server: file system, backup e condivisioni di file

Le risorse principali di Amazon FSx sono i file system e i 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). MBps È possibile modificare queste proprietà in base alle diverse esigenze dopo la creazione del file system. Per ulteriori informazioni, consultare [Gestione della capacità di storage](#), [Gestione degli IOPS SSD](#) e [Gestione della capacità di throughput](#).

FSx per Windows File Server i backup sono file-system-consistent 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 [Protezione dei dati con 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 [Accesso ai dati tramite condivisioni di file](#).

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 FSx file Amazon su istanze Amazon Elastic Compute Cloud (Amazon EC2) e su istanze WorkSpaces , istanze Amazon AppStream 2.0 e Cloud on. VMware AWS VMs

Puoi accedere alle tue condivisioni di file da istanze di calcolo locali utilizzando o. AWS Direct Connect Site-to-Site VPN Oltre ad accedere alle condivisioni di file che si trovano nello stesso VPC, AWS account e Regione AWS file system, puoi anche accedere alle tue condivisioni da istanze di calcolo che si trovano in un altro Amazon VPC, account o. Regione AWS Puoi farlo utilizzando il peering VPC o i gateway di transito. Per ulteriori informazioni, consulta [Accesso ai dati dall'interno di Cloud AWS](#).

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 cartelle con gli elenchi di controllo degli accessi di Windows (ACLs). 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 per Windows File Server offre file system con due livelli di disponibilità e durabilità. I file Single-AZ garantiscono un'elevata disponibilità all'interno di una singola 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 per Windows File Server utilizzando PowerShell comandi di gestione remota personalizzati o utilizzando la GUI nativa di Windows in alcuni casi. Per ulteriori informazioni sulla gestione dei FSx file system Amazon, consulta [Amministrazione FSx per i file system Windows](#).

Flessibilità in termini di prezzi e prestazioni

FSx per Windows File Server offre la flessibilità in termini di prezzo e prestazioni offrendo tipi di storage con unità a stato solido (SSD) e unità disco rigido (HDD). L'archiviazione HDD è pensata per un ampio spettro di carichi di lavoro, che comprende home directory, condivisioni tra utenti e dipartimenti, nonché sistemi per la gestione dei contenuti. L'archiviazione SSD è progettata per i carichi di lavoro più performanti e sensibili alla latenza, inclusi database, carichi di lavoro di elaborazione multimediale e applicazioni di analisi dei dati.

Con FSx for Windows File Server, puoi 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. Puoi 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 hai bisogno.

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 installazione o costi aggiuntivi. Per informazioni sui prezzi e le tariffe associati al servizio, consulta i [prezzi di Amazon FSx per Windows File Server](#).

Presupposti

Per utilizzare Amazon FSx, è necessario un AWS account con un' EC2 istanza Amazon, un' WorkSpaces istanza, un'istanza WorkSpaces Applications o una VM in esecuzione nel VMware cloud su AWS ambienti del tipo supportato.

In questa guida, facciamo i seguenti presupposti:

- Se utilizzi Amazon EC2, supponiamo che tu conosca bene 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 FSx file system Amazon, hai bisogno di quanto segue:

- Un AWS account con le autorizzazioni necessarie per creare un FSx file system Amazon e un' EC2 istanza Amazon. Per ulteriori informazioni, consulta [Configurare il Account AWS](#).
- Un' EC2 istanza Amazon 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 la sezione [Getting Started with Amazon EC2 Windows Instances](#) nella Amazon EC2 User Guide.

- Amazon FSx collabora con Microsoft Active Directory per eseguire l'autenticazione degli utenti e il controllo degli accessi. Unisci il tuo FSx file system Amazon a Microsoft Active Directory durante la creazione. Per ulteriori informazioni, consulta [Lavorare con Microsoft Active Directory](#).
- 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' EC2 istanza Amazon al FSx file system Amazon. Per ulteriori dettagli, consultare [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 FSx di Amazon per Windows File Server

Se riscontri problemi durante l'utilizzo di Amazon FSx, usa i [forum](#).

Sei un utente di Amazon FSx per la prima volta?

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

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

Procedure consigliate FSx per Windows File Server

Ti consigliamo di seguire queste best practice quando lavori con Amazon FSx for Windows File Server.

Argomenti

- [Best practice generali](#)
- [Best practice di sicurezza](#)
- [Active Directory](#)
- [Configurazione e dimensionamento corretto del file system](#)

Best practice generali

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 FSx file system Amazon 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 [Avvertenze e raccomandazioni sulle prestazioni](#)

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 FSx file system Amazon 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 di gruppi di sicurezza e rete ACLs

È possibile utilizzare i gruppi di sicurezza e gli elenchi di controllo degli accessi alla rete (ACLs) 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 la rete ACLs per le sottoreti in cui crei il file system consentano il traffico sulle porte.

Active Directory

Quando crei un FSx file system Amazon, puoi aggiungerlo al tuo [dominio Microsoft Active Directory](#) 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 Active Directory 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: Microsoft Active Directory AWS gestita o Microsoft Active Directory autogestita.

Se utilizzi un Microsoft Active Directory AWS gestito, ti consigliamo di lasciare le impostazioni predefinite del tuo gruppo di sicurezza Active Directory. 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 Active Directory autogestito, hai a disposizione opzioni aggiuntive per la configurazione del file system. Consigliamo le seguenti best practice per la configurazione iniziale quando usi Amazon FSx con Microsoft Active Directory autogestito:

- Assegna sottoreti a un singolo sito Active Directory: se il tuo ambiente Active Directory ha un gran numero di controller di dominio, utilizza Siti e servizi di Active Directory per assegnare le sottoreti utilizzate dai tuoi file system FSx Amazon a un singolo sito Active Directory con la massima disponibilità e affidabilità. Assicurati che il gruppo di sicurezza VPC, l'ACL di rete VPC, le regole del

firewall di Windows e tutti gli altri controlli di routing di rete presenti nella tua infrastruttura Active Directory consentano la comunicazione da Amazon sulle porte richieste. DCs FSx Ciò consente a Windows di tornare ad altro DCs se non può utilizzare il sito Active Directory assegnato. Per ulteriori informazioni, consulta [Controllo degli accessi ai file system con Amazon VPC](#).

- Utilizza un'unità organizzativa (OU) separata: utilizza un'unità organizzativa per i tuoi FSx file system Amazon 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 [Utilizzo di un Microsoft Active Directory autogestito](#).
- Verifica continua la configurazione di Active Directory: esegui [lo strumento di convalida Amazon FSx Active Directory](#) sulla configurazione di Active Directory prima di creare il FSx file system Amazon 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.
- Archiviazione delle credenziali di Active Directory tramite Gestione dei segreti AWS: È possibile utilizzare Gestione dei segreti AWS per archiviare e gestire in modo sicuro le credenziali dell'account di accesso al servizio di accesso al dominio Microsoft Active Directory. Questo approccio elimina la necessità di archiviare credenziali sensibili in testo semplice nel codice dell'applicazione o nei file di configurazione, rafforzando il livello di sicurezza. Per ulteriori informazioni, consulta [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#).

Evita di perdere la disponibilità a causa di una configurazione errata di Active Directory

Quando usi Amazon FSx con il tuo Microsoft Active Directory autogestito, è importante disporre di una configurazione Active Directory 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 al tuo Active Directory. Se la configurazione di Active Directory 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 la perdita di disponibilità:

- Mantieni aggiornata la configurazione di Active Directory 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 di Active Directory: imposta automaticamente le notifiche sullo stato di configurazione errata in modo da poter ripristinare la configurazione di Active Directory del file system, se necessario. Per un esempio che utilizza una soluzione basata su Lambda per raggiungere questo obiettivo, consulta [Monitoraggio dello stato dei FSx file system Amazon utilizzando Amazon and EventBridge AWS Lambda](#).
- Convalida regolarmente la configurazione di Active Directory: se desideri rilevare in modo proattivo un'errata configurazione di Active Directory, ti consigliamo di eseguire [lo strumento di convalida di Active Directory sulla tua configurazione di Active Directory 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 Active Directory, 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.

Windows ACLs

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

- 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 i file system Multi-AZ per la maggior parte dei carichi di lavoro di produzione che richiedono un'elevata disponibilità per i dati condivisi dei file Windows. Per ulteriori informazioni, consulta [Disponibilità e durabilità: file system Single-AZ e Multi-AZ](#).

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 20% della capacità di archiviazione gratuita sul tuo file system. Si consiglia inoltre di aumentare la capacità di throughput di almeno il 20% prima di aumentare la capacità di storage per compensare l'eventuale impatto sulle prestazioni durante un aumento dello storage. Puoi utilizzare la FreeStorageCapacity CloudWatch metrica per monitorare la quantità di storage gratuito disponibile e comprenderne le tendenze. Per ulteriori informazioni, consulta [Gestione della capacità di storage](#).

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 FSx console per verificare se le richieste del carico di lavoro hanno raggiunto o superato i limiti prestazionali e determinare se il numero di provisioning del file system è insufficiente 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 una volta completato l'aumento della capacità di storage. La maggior parte dei carichi di lavoro ha un impatto minimo sulle prestazioni durante la scalabilità dello storage. Tuttavia, i file system con tipo di storage HDD e i carichi di lavoro che coinvolgono un gran numero di utenti finali, alti livelli di I/O o i set di dati con un gran numero di file di piccole dimensioni potrebbero subire temporaneamente una riduzione delle prestazioni. Per ulteriori informazioni, consulta [Aumento della capacità di storage e delle prestazioni del file system](#).

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 per Windows File Server

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

1. Registrati Account AWS e crea un utente amministrativo nell'account.
2. Creare un Microsoft AD Active Directory AWS gestito utilizzando 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 FSx console Amazon.
5. Mappa il tuo file system sulla tua istanza EC2
6. Scrivi dati sul tuo file system.
7. Esegui il backup del file system.
8. Eliminare tutte le risorse create.

Argomenti

- [Configurare il Account AWS](#)
- [Passaggio 1. Configurazione di un Active Directory](#)
- [Fase 2: Avvio di un'istanza Windows nella console Amazon EC2](#)
- [Fase 3: connessione all'istanza](#)
- [Passaggio 4: Unisci l'istanza alla tua Directory Service directory](#)
- [Fase 5. Crea il tuo file system](#)
- [Fase 6. Mappa la condivisione di file su un'istanza EC2 che esegue Windows Server](#)
- [Fase 7. Scrivi dati nella tua condivisione di file](#)
- [Fase 8. Esegui il backup del file system](#)
- [Fase 9. Eseguire la pulizia delle risorse](#)

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

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

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

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

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

1. Accedi [Console di gestione AWS](#) come proprietario dell'account scegliendo Utente root e inserendo il tuo indirizzo Account AWS email. Nella pagina successiva, inserisci la password.

Per informazioni sull'accesso utilizzando un utente root, consulta la pagina [Accedere come utente root](#) nella Guida per l'utente di Accedi ad AWS .

2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

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

Crea un utente con accesso amministrativo

1. Abilita il Centro identità IAM.

Per istruzioni, consulta [Abilitazione del AWS IAM Identity Center](#) nella Guida per l'utente di AWS IAM Identity Center .

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

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

Accesso come utente amministratore

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

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

Assegnazione dell'accesso ad altri utenti

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

Segui le istruzioni riportate nella pagina [Creazione di un set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

Per istruzioni, consulta [Aggiungere gruppi](#) nella Guida per l'utente di AWS IAM Identity Center .

Passaggio 1. Configurazione di un Active Directory

Con Amazon FSx, puoi gestire lo storage di file completamente gestito per carichi di lavoro basati su Windows. Allo stesso modo, Directory Service fornisce directory completamente gestite da utilizzare nella distribuzione dei carichi di lavoro. Se disponi di un dominio Active Directory aziendale esistente in esecuzione AWS in un cloud privato virtuale (VPC) utilizzando istanze EC2, puoi abilitare l'autenticazione e il controllo degli accessi basati sull'utente. A tale scopo, è necessario stabilire una relazione di fiducia tra il proprio AWS Managed Microsoft Active Directory e il dominio aziendale. 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 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.

Note

Puoi anche utilizzare un tipo di trust esterno con Amazon FSx per domini affidabili.

Il tuo gruppo di sicurezza Active Directory deve abilitare l'accesso in entrata dal gruppo di sicurezza del FSx file system Amazon.

Per creare un AWS Directory Services per Microsoft Active Directory

- Se non ne hai già uno, usa Directory Service per creare la tua directory AWS gestita di Microsoft Active Directory. Per ulteriori informazioni, vedere [Create Your AWS Managed Microsoft Active Directory](#) nella Guida all'AWS Directory Service amministrazione.

Important

Ricorda la password che assegni all'utente amministratore; ti servirà più avanti in questo esercizio introduttivo. Se dimentichi la password, devi ripetere i passaggi di questo esercizio con la nuova Directory Service directory e l'utente amministratore.

- Se disponi di un Active Directory esistente, crea una relazione di trust tra la tua versione AWS gestita di Microsoft Active Directory e la tua Active Directory esistente. Per ulteriori informazioni,

consulta [Quando creare una relazione di trust](#) nella Guida di amministrazione di AWS Directory Service .

Fase 2: Avvio di un'istanza Windows nella console Amazon EC2

È possibile avviare un'istanza Windows utilizzando la Console di gestione AWS procedura descritta nella procedura seguente. Questo ha lo scopo di aiutarti ad avviare rapidamente la tua prima istanza, quindi non copre tutte le opzioni possibili. Per ulteriori informazioni sulle opzioni avanzate, consulta l'argomento relativo all'[avvio di un'istanza](#).

Per avviare un'istanza

1. Apri 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. La pagina Choose an Amazon Machine Image (AMI) mostra un elenco di configurazioni di base, chiamate Amazon Machine Images (AMIs), che fungono da modelli per la tua istanza. Seleziona l'AMI per Windows Server 2016 Base o versione successiva. Nota che queste AMIs sono contrassegnate come «Idonee al 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. Nella pagina Review Instance Launch, in Security Groups, viene visualizzato un gruppo di sicurezza creato e selezionato automaticamente dalla procedura guidata. Puoi utilizzare questo gruppo di sicurezza oppure puoi scegliere il gruppo di sicurezza che hai creato durante la configurazione utilizzando i seguenti passaggi:
 - 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 avvia 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 avvia 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) o (IPv6) è nascosta, scegli Mostra/Nascondi colonne (l'icona a forma di ingranaggio) nell'angolo in alto a destra della pagina, quindi seleziona Public DNS () o (IPv4).) IPv6
11. Possono essere necessari alcuni minuti affinché l'istanza sia pronta e sia possibile connettersi. Controllare che l'istanza abbia superato i controlli relativi allo stato. È possibile visualizzare queste informazioni nella colonna Status Checks (Verifiche dello stato).

 Important

Prendi nota dell'ID del gruppo di sicurezza che è stato creato quando hai avviato questa istanza. Ti servirà quando creerai il tuo FSx file system Amazon.

Ora che l'istanza è stata lanciata, 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. Ad esempio, per l'inglese è Administrator, per il francese è Administrateur e per il portoghese è Administrador. Per ulteriori informazioni, vedere [Nomi localizzati per l'account amministratore in Windows](#) in Microsoft TechNet Wiki.

Se hai aggiunto la tua istanza a un dominio, puoi connetterti all'istanza utilizzando le credenziali di dominio che hai definito in Directory Service. Nella schermata di accesso a Remote Desktop, non utilizzare il nome del computer locale e la password generata. Utilizza 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 (OS) 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, vedere [Configurare il 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. Nella finestra di dialogo Connect to Your Instance, scegli Ottieni password (occorrono alcuni minuti dopo l'avvio dell'istanza 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 amministratore predefinita per l'istanza nella finestra di dialogo Connect to Your Instance, sostituendo il collegamento a Get Password mostrato 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, puoi scegliere Chiudi per chiudere la finestra di dialogo Connect to Your Instance.
 - 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. Scegli la scheda Dettagli e scorri verso il basso fino alla voce Impronta digitale su un PC Windows o alla voce SHA1Impronte digitali su un 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 log 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 all'istanza, puoi aggiungere l'istanza alla tua directory. Directory Service

Passaggio 4: Unisci l'istanza alla tua Directory Service directory

La procedura seguente mostra come aggiungere manualmente un'istanza Amazon EC2 Windows esistente alla tua Directory Service directory.

Per aggiungere un'istanza Windows alla tua directory Directory Service

1. Connettiti all'istanza utilizzando qualsiasi client Remote Desktop Protocol.
2. Aprire la finestra di dialogo TCP/ IPv4 o IPv6 properties 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. Apri il menu contestuale (fai clic con il pulsante destro del mouse) per qualsiasi connessione di rete abilitata, quindi scegli Proprietà.
 - c. Nella finestra di dialogo delle proprietà della connessione, apri (fate doppio clic) Protocollo Internet versione 4 o Protocollo Internet versione 6.

3. (Facoltativo) Seleziona Usa i seguenti indirizzi di server DNS, modifica gli indirizzi del server DNS preferito e del server DNS alternativo con gli IPv4 o gli IPv6 indirizzi dei server DNS Directory Service forniti e scegli OK.
4. Apri la finestra di dialogo delle proprietà del sistema per l'istanza, scegli la scheda Nome computer e scegli Cambia.

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. Nella casella Membro di, scegliete Dominio, immettete il nome completo della Directory Service directory e scegliete OK.
6. Quando vengono richiesti il nome e la password per l'amministratore del dominio, inserisci il nome utente e la password dell'account amministratore.

Note

Puoi inserire il nome completo del tuo dominio o il NetBios nome, seguito da una barra rovesciata (\) e quindi dal nome utente, in questo caso, Admin. 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 dell'utente amministratore della Directory Service directory.

Ora che la tua istanza è stata aggiunta al dominio, sei pronto per creare il tuo FSx file system Amazon.

Fase 5. Crea il tuo file system

Per creare il tuo file system (console)

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

2. Nel pannello di controllo, scegli Crea file system per avviare la procedura guidata di creazione del file system.
3. Nella pagina Seleziona il tipo di file system, scegli FSx Windows File Server, quindi scegli Avanti. Viene visualizzata la pagina Crea file system.
4. Per Metodo di creazione, scegliete 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 per Windows File Server offre tipi di storage con unità a stato solido (SSD) e unità disco rigido (HDD). L'archiviazione SSD è progettata 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 [Informazioni sui tipi di storage](#).

4. Per Provisioned SSD IOPS, puoi scegliere la modalità Automatica o User-provisioned.

Se si sceglie la modalità Automatica, FSx per Windows File Server ridimensiona automaticamente gli IOPS SSD per mantenere 3 IOPS SSD per GiB di capacità di archiviazione. Se scegli la modalità User-provisioned, inserisci 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 storage](#).
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 [FSx per le prestazioni di Windows File Server](#).

Note

Se intendi abilitare il controllo dell'accesso ai file, devi scegliere una capacità di throughput pari o superiore a 32. MBps Per ulteriori informazioni, consulta [Registrazione dell'accesso dell'utente finale con il 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 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.

Regole	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 il gruppo di sicurezza IDs 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 FSx file system Amazon. Per ulteriori informazioni sulle regole in entrata richieste, consulta [AWS Managed Microsoft AD Prerequisiti nella Guida all'AWS Directory Service amministrazione](#).

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 sottorete. Se state creando un file system Multi-AZ (vedere il passaggio 5), scegliete un valore di sottorete preferito per il file server principale 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 file system.

4. Per Tipo di rete, selezionate IPv4(solo per il IPv4 supporto) o Dual-stack (per entrambi i tipi di supporto). IPv4 IPv6 È possibile modificare il tipo di rete di un file system esistente in qualsiasi momento. Per ulteriori informazioni, consulta [Modifica del tipo di rete](#).

Note

Se intendi creare un file system FSx per Windows File Server che utilizzi la modalità dual-stack, devi prima assegnare un IPv6 blocco CIDR fornito da Amazon al tuo VPC e alle tue sottoreti. Per ulteriori informazioni, consulta [Aggiungere il IPv6 supporto per il tuo VPC](#) nella Guida per l'utente di Amazon Virtual Private Cloud.

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 Directory Service directory dall'elenco. Per ulteriori informazioni, consulta [Lavorare con Microsoft Active Directory](#).

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 un 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 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. Direct Connect AWS Transit Gateway

- Indirizzi IP dei server DNS: gli indirizzi IPv4 o gli IPv6 indirizzi dei server DNS del tuo dominio.

 Note

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

- Credenziali per un account del servizio Active Directory che Amazon FSx utilizza per aggiungere il file system al tuo dominio. Puoi fornirle in uno dei seguenti modi:
 - Opzione 1: ARN Gestione dei segreti AWS segreto: il segreto contenente il nome utente e la password per un account di servizio nel dominio Active Directory. Per ulteriori informazioni, consulta [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#).
 - Opzione 2: credenziali in chiaro
 - Nome utente dell'account di servizio: il nome utente dell'account di servizio nel Microsoft Active Directory esistente. Non includere un prefisso o un suffisso di dominio. Ad esempio `EXAMPLE\ADMIN`, solo per. ADMIN
 - Password dell'account di servizio: la password per l'account di servizio.
- (Facoltativo) 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 [Account FSx di servizio Amazon](#).

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 a riposo](#).
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 [Registrazione dell'accesso dell'utente finale con il controllo dell'accesso ai file](#).
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, vedere [Protezione dei dati con backup](#).

1. Il backup automatico giornaliero è abilitato per impostazione predefinita. 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 più adatta al flusso di lavoro.
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 [Taggare le tue risorse Amazon FSx](#).

Scegli 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 ha FSx creato il file system, scegli l'ID del file system dall'elenco nella dashboard File Systems 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.

Fase 6. 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. 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, è necessario avviare l'istanza EC2 e aggiungerla a AWS Directory Service for Microsoft Active Directory quella a cui è stato aggiunto il file system. Per eseguire questa azione, 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 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. [Accesso ai dati tramite alias DNS](#)

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

Fase 7. 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.

Fase 8. Esegui il backup del file system

Ora che hai avuto la possibilità di utilizzare il tuo FSx file system Amazon 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 FSx console Amazon 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.

Fase 9. Eseguire la 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 [Terminazione dell'istanza](#) nella Guida per l'utente di Amazon EC2.
2. Sulla FSx console Amazon, elimina il tuo 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 FSx console Amazon 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 tuo FSx file system Amazon e i relativi backup automatici sono ora eliminati.

3. Per eliminare la Directory Service directory creata per questo esercizio, consulta [Eliminare la directory](#) nella Guida all' AWS Directory Service amministrazione.

Accesso ai tuoi dati

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

Argomenti

- [Client supportati](#)
- [Accesso ai dati dall'interno di Cloud AWS](#)
- [Accesso ai dati dall'ambiente locale](#)
- [Accesso ai dati utilizzando nomi DNS predefiniti](#)
- [Support per gli spazi dei nomi DFS \(Distributed File System\)](#)
- [Accesso ai dati tramite alias DNS](#)
- [Accesso ai dati tramite condivisioni di file](#)
- [Creazione, aggiornamento e rimozione di condivisioni di file](#)

Client supportati

FSx per Windows File Server supporta le versioni del protocollo Server Message Block (SMB) dalla 2.0 alla 3.1.1, offrendoti la flessibilità necessaria per connetterti ai tuoi file system utilizzando un'ampia varietà di istanze di calcolo e sistemi operativi.

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

- Istanze Amazon Elastic Compute Cloud (Amazon EC2), incluse istanze Microsoft Windows, Mac, Amazon Linux e Amazon Linux 2. Per ulteriori informazioni, consulta [Mappatura delle condivisioni di file](#).
- Contenitori Amazon Elastic Container Service (Amazon ECS). Per ulteriori informazioni, consulta [FSx i volumi di Windows File Server](#) nella Amazon Elastic Container Service Developer Guide.
- WorkSpaces istanze: per ulteriori informazioni, consulta il post del AWS blog [Using FSx for Windows File Server with Amazon WorkSpaces](#).
- Istanze Amazon AppStream 2.0: per ulteriori informazioni, consulta il post del AWS blog [Using Amazon FSx with Amazon AppStream 2.0](#).

- VMs esecuzione in AWS ambienti VMware Cloud: per ulteriori informazioni, consulta il post di AWS blog [Archiviazione e condivisione di file with FSx for Windows File Server in a VMware Cloud on AWS Environment](#).

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

- Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 e Windows Server 2022.
- 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 lo `cifs-utils` strumento.
- macOS

Accesso ai dati dall'interno di Cloud AWS

Ogni FSx file system Amazon è associato a un Virtual Private Cloud (VPC). È possibile accedere al file system FSx per Windows File Server da qualsiasi punto del VPC del file system, indipendentemente dalla zona di disponibilità. È inoltre possibile accedere al file system da VPCs un file system diverso Account AWS o Regioni AWS diverso dal file system. Oltre ai requisiti descritti nelle seguenti sezioni per l'accesso alle FSx risorse di Windows File Server, è necessario assicurarsi che il gruppo di sicurezza VPC del file system sia configurato in modo che il traffico di dati e di gestione possa fluire tra il file system e i client. Per ulteriori informazioni sulla configurazione dei gruppi di sicurezza con le porte richieste, vedere. [Controllo degli accessi ai file system con Amazon VPC](#)

È possibile accedere FSx al file system Windows File Server dai client supportati che si trovano nello stesso VPC del file system.

La tabella seguente illustra gli ambienti da cui Amazon FSx supporta l'accesso dai client in ciascuno degli ambienti supportati, a seconda di quando è stato creato il file system.

Client situati 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	✓	✓	✓
Secondario CIDRs del VPC in cui è stato creato il file system		Client con indirizzi IP in un intervallo di indirizzi IP privati RFC 1918 :	Client con indirizzi IP al di fuori del seguente intervallo di blocchi CIDR:
CIDRs Reti altre o peer-to-peer		• 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	198.19.0.0/16

Note

In alcuni casi, potresti voler accedere da locale a un file system creato prima del 17 dicembre 2020 utilizzando un intervallo di indirizzi IP non privato. A tale scopo, create un nuovo file system da un backup del file system. Per ulteriori informazioni, consulta [Protezione dei dati con backup](#).

Accesso ai dati da un altro VPC, oppure Account AWS Regione AWS

È possibile accedere al file system FSx per Windows File Server dai client di supporto che si trovano in un VPC Regione AWS diverso o da quello associato al file system utilizzando i gateway di peering o di transito VPC. Account AWS Quando utilizzi una connessione peering VPC o un gateway di transito per connetterti VPCs, le istanze di calcolo che si trovano in un VPC possono accedere ai file system FSx Amazon che si trovano in un altro VPC. Questo accesso è possibile anche se VPCs appartengono a paesi diversi e anche se risiedono in paesi diversi Account AWS. VPCs Regioni AWS

Una connessione peering VPC è una connessione di rete tra due VPCs che puoi utilizzare per instradare il traffico tra di loro utilizzando indirizzi privati IPv4 o IP versione 6 (IPv6). Puoi utilizzare il peering VPC per connetterti VPCs all'interno della stessa AWS regione o tra regioni. AWS Per ulteriori informazioni, consulta [Che cos'è il peering di VPC?](#) nella Guida al peering di Amazon VPC.

Un gateway di transito è un hub di transito di rete che puoi utilizzare per interconnettere le tue reti VPCs e quelle locali. Per ulteriori informazioni sull'utilizzo dei gateway di transito VPC, consulta [Guida introduttiva ai gateway di transito nei gateway](#) di transito Amazon VPC.

Dopo aver configurato un peering VPC o una connessione gateway di transito, puoi accedere al file system utilizzando il relativo nome DNS. Lo fai esattamente come fai con le istanze di calcolo all'interno del VPC associato.

Accesso ai dati dall'ambiente locale

FSx per Windows File Server supporta l'uso AWS Direct Connect o l'accesso Site-to-Site VPN ai file system dalle istanze di elaborazione locali. Con il supporto per AWS Direct Connect, FSx for Windows File Server consente di accedere al file system tramite una connessione di rete dedicata dall'ambiente locale. Con il supporto per Site-to-Site 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 FSx Amazon, puoi accedere al file system utilizzando il nome DNS o un alias DNS. Lo fai esattamente come fai con le istanze di calcolo all'interno del VPC. Per ulteriori informazioni su Direct Connect, consulta la Guida per l'utente di [Direct Connect](#). Per ulteriori informazioni sulla configurazione delle Site-to-Site VPN connessioni, consulta [Connessioni VPN](#) nella Amazon VPC User Guide.

 Note

In alcuni casi, potresti voler accedere da locale a un file system creato prima del 17 dicembre 2020 utilizzando un intervallo di indirizzi IP non privato. A tale scopo, create un nuovo file system da un backup del file system. Per ulteriori informazioni, consulta [Protezione dei dati con backup](#).

FSx for Windows File Server supporta anche l'uso di Amazon FSx File Gateway per fornire un accesso semplice e a bassa latenza al cloud FSx per le condivisioni di file Windows File Server dalle istanze di calcolo locali. Per ulteriori informazioni, consulta la [Amazon FSx File Gateway User Guide](#).

 Note

Amazon FSx File Gateway non è più disponibile per i nuovi clienti. I clienti esistenti di FSx File Gateway possono continuare a utilizzare il servizio normalmente. Per funzionalità simili a FSx File Gateway, consulta [questo post del blog](#).

Accesso ai dati utilizzando nomi DNS predefiniti

FSx per Windows File Server fornisce un nome DNS (Domain Name System) per ogni file system. Puoi accedere al tuo file system FSx per Windows File Server mappando una lettera di unità sull'istanza di calcolo alla condivisione di FSx file Amazon utilizzando questo nome DNS. Per ulteriori informazioni, consulta [Accesso ai dati tramite condivisioni di file](#).

 Important

Amazon registra i record DNS per un file system FSx solo se utilizzi Microsoft DNS come DNS predefinito. Se utilizzi un DNS di terze parti, devi configurare manualmente le voci DNS per i tuoi FSx file system Amazon. Per 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 le immissioni DNS manuali](#)

Per trovare il nome DNS:

- Nella FSx console Amazon, scegli File system, quindi scegli Dettagli. Visualizza il nome DNS nella sezione Rete e sicurezza.
- Oppure, visualizzalo nella risposta del comando CreateFileSystem o DescribeFileSystems API.

Per tutti i file system Single-AZ uniti a una Microsoft Active Directory AWS gestita, il nome DNS ha il seguente formato: 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 formato: amznfsxaa11bb22.*ad-domain*.com

Utilizzo dell'autenticazione Kerberos con nomi DNS

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 tuo file system. Per abilitare l'autenticazione e la crittografia dei dati in transito basate su Kerberos per le sessioni SMB, utilizza il nome DNS del file system fornito da Amazon FSx per accedere al file system.

Se disponi di un trust esterno configurato tra Microsoft Active Directory AWS gestito e Active Directory locale, per utilizzare Amazon FSx Remote PowerShell con autenticazione Kerberos, devi configurare una policy di gruppo locale sul client per l'ordine di ricerca nella foresta. Per ulteriori informazioni, vedere [Configurare Kerberos Forest Search Order \(KFSO\) nella documentazione Microsoft](#).

Support per gli spazi dei nomi DFS (Distributed File System)

FSx per Windows File Server supporta l'uso dei namespace Microsoft DFS. Utilizza i namespace DFS per organizzare le condivisioni di file che si trovano 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 spazio dei nomi DFS per accedere al tuo FSx file system Amazon configurando la destinazione del collegamento in modo che sia il nome DNS del file system. Per ulteriori informazioni, consulta [Raggruppa più file system FSx per Windows File Server con namespace DFS](#).

Accesso ai dati tramite alias DNS

FSx per Windows File Server fornisce un nome DNS per ogni file system che è possibile utilizzare per accedere alle condivisioni di file. È inoltre possibile accedere alle condivisioni di file utilizzando

nomi DNS diversi dal nome DNS predefinito registrando alias DNS per i file system per Windows File Server FSx .

Utilizzando gli alias DNS, puoi spostare i dati di condivisione di file di Windows su Windows File Server e continuare a utilizzare i nomi DNS esistenti per accedere ai dati su Amazon. FSx 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 Puoi associare fino a 50 alias DNS a un file system contemporaneamente. Per ulteriori informazioni sull'associazione e la dissociazione degli alias DNS con un file system FSx per Windows File Server, vedere. [Gestione degli alias DNS](#)

Per configurare l'accesso ai file system FSx per Windows File Server utilizzando alias DNS, è necessario effettuare le seguenti operazioni:

1. [Associa gli alias DNS al tuo file system.](#)
2. [Create un record DNS CNAME](#) per il file system e gli alias DNS ad esso associati.

Per ulteriori informazioni sull'utilizzo degli alias DNS con i file system Windows File FSx Server, consulta. [Gestione degli alias DNS](#)

Utilizzo dell'autenticazione e della crittografia Kerberos con alias DNS

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 tuo 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 (SPNs) che corrispondono all'alias DNS sull'oggetto computer Active Directory del tuo FSx file system Amazon.

Per configurare l'autenticazione e la crittografia Kerberos quando si accede al file system utilizzando alias DNS, consulta. [Configura i nomi principali dei servizi \(SPNs\) per Kerberos](#)

Facoltativamente, puoi imporre ai client che accedono al file system utilizzando un alias DNS di utilizzare l'autenticazione e la crittografia Kerberos impostando i seguenti oggetti di policy di gruppo () in Active Directory: GPOs

- 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: 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.

Per applicare l'autenticazione e la crittografia Kerberos quando si accede al file system utilizzando alias DNS, vedere. [Applicazione dell'autenticazione Kerberos utilizzando Group Policy Objects \(\) GPOs](#)

Per ulteriori informazioni sulla configurazione del file system per l'utilizzo di alias DNS, consulta le seguenti procedure:

- [Associa gli alias DNS al tuo file system](#)
- [Configura i nomi principali dei servizi \(SPNs\) per Kerberos](#)
- [Aggiorna o crea un record DNS CNAME](#)
- [Applicazione dell'autenticazione Kerberos utilizzando Group Policy Objects \(\) GPOs](#)

Associa gli alias DNS al tuo file system

Puoi associare gli alias DNS ai file system esistenti FSx per Windows File Server, quando crei nuovi file system e quando crei un nuovo file system da un backup utilizzando la FSx console Amazon, la CLI e l'API. 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](#)

Per associare gli alias DNS durante la creazione di un nuovo file system

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Segui la procedura per creare un nuovo file system, come descritto nella [Fase 5. 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 memorizza i caratteri alfabetici come lettere minuscole (a-z), indipendentemente da come li specifichi: come lettere maiuscole, lettere minuscole o le lettere corrispondenti nei codici di escape.

4. Per le preferenze di manutenzione, apporta le modifiche che desideri.
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.

Configura i nomi principali dei servizi (SPNs) 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 tuo 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 (SPNs) che corrispondono all'alias DNS sull'oggetto computer Active Directory del tuo FSx file system Amazon. Un SPN può essere associato solo a un singolo oggetto informatico Active Directory alla volta. Se disponete di un nome DNS configurato SPNs per l'oggetto computer Active Directory del file system originale, dovete prima eliminarli.

Ce ne sono due necessari SPNs per l'autenticazione Kerberos:

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

Se l'alias è `finance.domain.com`, sono necessari i due seguenti: SPNs

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

 Note

Dovrai eliminare qualsiasi HOST esistente SPNs che corrisponde all'alias DNS sull'oggetto computer Active Directory prima di creare un nuovo HOST SPNs per l'oggetto computer Active Directory (AD) del tuo FSx file system Amazon. I tentativi di impostazione SPNs per il tuo FSx file system Amazon falliranno se nell'AD esiste un SPN per l'alias DNS.

Le seguenti procedure descrivono come eseguire le seguenti operazioni:

- Trova qualsiasi alias DNS esistente nell' SPNs oggetto computer Active Directory del file system originale.
- Elimina l'eventuale SPNs trovato esistente.
- Crea un nuovo alias DNS SPNs per l'oggetto informatico Active Directory del tuo FSx file system Amazon.

Per installare il modulo PowerShell Active Directory richiesto

1. Accedi a un'istanza Windows aggiunta all'Active Directory a cui è collegato il tuo FSx file system Amazon.
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 l'alias DNS esistente nell' SPNs oggetto computer Active Directory del file system originale

Se avete SPNs configurato l'alias DNS assegnato a un altro file system su un oggetto computer in Active Directory, dovete prima rimuoverlo prima di aggiungerlo all'oggetto computer del file SPNs system. SPNs

1. Trovate quelli esistenti utilizzando i seguenti comandi. SPNs 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 l'HOST esistente SPNs restituito 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.](#)

Da impostare SPNs sull'oggetto informatico Active Directory del tuo FSx file system Amazon

1. Imposta SPNs un nuovo FSx file system Amazon eseguendo i seguenti comandi.
 - Sostituisci *file_system_DNS_name* con il nome DNS FSx assegnato da Amazon al file system.

Per trovare il nome DNS del tuo file system sulla FSx console Amazon, 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 [DescribeFileSystemsAPI](#).

- [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 the following command to set both the full FQDN and Alias SPNs
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-AdditionalDnsHostname" =
@($Alias, $Alias.Split(".")[0])}

```

Note

L'impostazione di un SPN per il tuo FSx file system Amazon 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 elementi esistenti, consulta [SPNs Per trovare ed eliminare l'alias DNS esistente nell' SPNs oggetto computer Active Directory del file system originale](#)

2. Verificate che i nuovi alias SPNs siano configurati per l'alias DNS utilizzando lo script di esempio seguente. Assicuratevi che la risposta includa due HOST HOST/*alias* e SPNSHOST/*alias_fqdn*, come descritto in precedenza in questa procedura.

Sostituiscilo *file_system_dns_name* con il nome DNS FSx assegnato da Amazon al tuo file system. Per trovare il nome DNS del tuo file system sulla FSx console Amazon, 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 [DescribeFileSystemsAPI](#).

```

## 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 che hai associato al file system nel passaggio 1.](#)

Aggiorna o crea un record DNS CNAME

Dopo aver SPNs configurato correttamente il 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 moduli richiesti

1. Accedi a un'istanza Windows aggiunta alla stessa Active Directory a cui appartiene il tuo FSx file system Amazon come utente membro di un gruppo con autorizzazioni di amministrazione DNS (AWS Delegated Domain Name System Administrators in e Domain Admins o un altro gruppo a AWS Managed Microsoft AD 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 tuo FSx file system Amazon

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 nel tuo 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 tuo file system Amazon. FSx

Per eseguire lo script:

- Sostituiscilo *alias_fqdn* con l'alias DNS che hai associato al file system.
- Sostituisci *file_system_DNS_name* con il nome DNS FSx che Amazon 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
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
  $DnsServerComputerName -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 FSx file system Amazon 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 FSx file system Amazon 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 utilizzando Group Policy Objects (GPOs)

È possibile applicare l'autenticazione Kerberos quando si accede al file system impostando i seguenti oggetti di policy di gruppo (GPOs) 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: 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 FSx file system Amazon come amministratore. Se stai configurando un Active Directory autogestito, applica questi passaggi direttamente ad Active Directory.
 2. Scegli Start, scegli Strumenti di amministrazione, quindi scegli 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.

Accesso ai dati tramite condivisioni di file

Una condivisione di file di Microsoft Windows è una cartella o una directory specifica del file system. Include tutte le sottocartelle che potrebbero esistere. I client accedono alle condivisioni di file sul file system utilizzando il protocollo Server Message Block (SMB). Il file system FSx per Windows File Server è dotato di una condivisione di file Windows predefinita, denominata `share`. È possibile creare

e gestire tutte le altre condivisioni di file che si desidera utilizzando lo strumento di interfaccia grafica utente (GUI) Windows Shared Folders.

Le condivisioni a disponibilità continua (CA) di Microsoft Windows offrono il vantaggio principale di mantenere l'accesso ininterrotto ai file condivisi anche in caso di guasto di un nodo server all'interno di un cluster. L'utilizzo delle condivisioni di file CA consente di ridurre al minimo le interruzioni delle applicazioni server che archiviano i relativi file di dati su tali condivisioni di file durante le finestre di manutenzione del file system.

Per ulteriori informazioni sulla creazione e la gestione delle condivisioni di file sul file system FSx per Windows File Server, incluse le condivisioni CA, vedere [Creazione, aggiornamento e rimozione di condivisioni di file](#).

Mappatura delle condivisioni di file

Per accedere alle tue condivisioni di file, utilizza la funzionalità Windows Map Network Drive per mappare una lettera di unità sulla tua istanza di calcolo alla tua condivisione di FSx file Amazon. 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.

Per ulteriori informazioni sulla mappatura e il montaggio di condivisioni di file per accedere ai dati sul file system, vedere le seguenti procedure:

- [Mappatura di una condivisione di file su un'istanza Amazon EC2 Windows](#).
- [Montaggio di una condivisione di file su un'istanza Amazon EC2 per Mac](#)
- [Montaggio di una condivisione di file su un'istanza Amazon EC2 Linux](#)

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

Puoi mappare una condivisione di file su un'istanza EC2 Windows FSx per accedere al file system per Windows File Server utilizzando Windows File Explorer o il prompt dei comandi.

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

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

- [Unisciti senza problemi a un'istanza Windows EC2](#)
 - [Unisciti manualmente a un'istanza Windows](#)
2. 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 [FSx console Amazon](#) scegliendo Windows File Server, rete e sicurezza. Oppure, puoi trovarli nella risposta dell'operazione [CreateFileSystem](#) o [DescribeFileSystems](#) dell'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.

```
\\amznfsxaa11bb22.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 ti sei unito al FSx file system Amazon. A tale scopo, scegli una delle seguenti procedure dalla Guida all'AWS Directory Service amministrazione:
 - [Unisciti senza problemi a un'istanza Windows EC2](#)
 - [Unisciti manualmente a un'istanza Windows](#)
2. Connect alla 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 [FSx console Amazon](#) 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: \\amznfsxaa11bb22.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

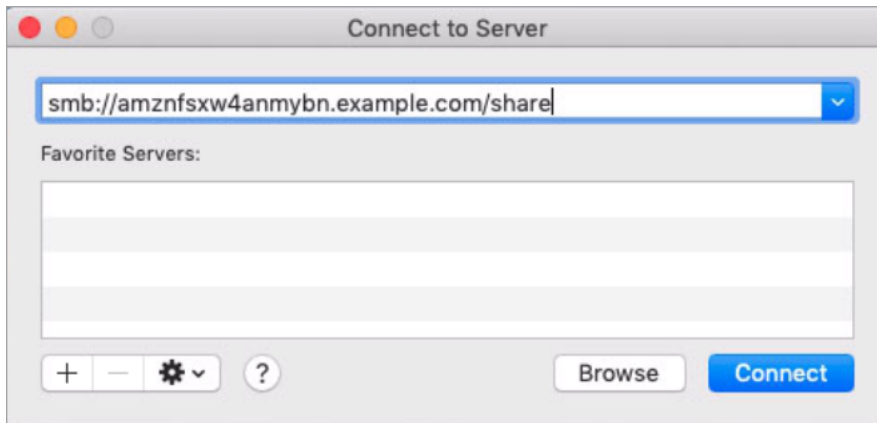
Puoi montare una condivisione di file su un'istanza Amazon EC2 per Mac che è aggiunta al tuo Active Directory o non unita per accedere al tuo file system FSx per Windows File Server. Se l'istanza non è aggiunta al tuo Active Directory, assicurati di aggiornare le opzioni DHCP impostate per Amazon Virtual 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

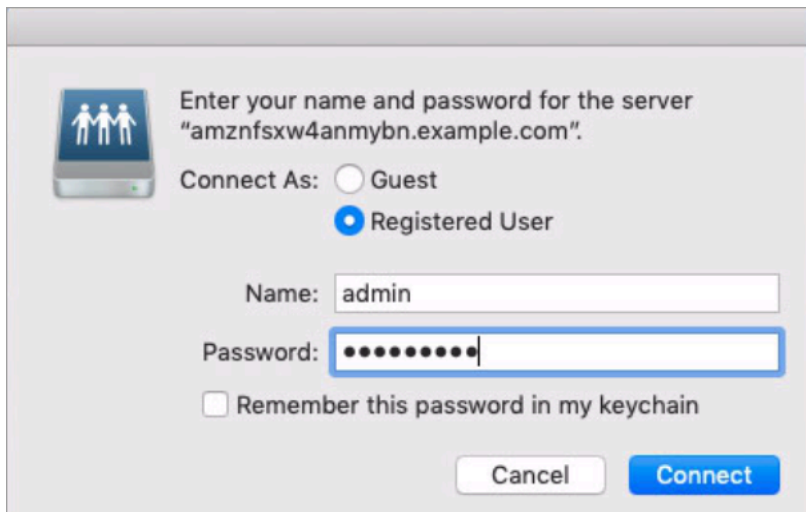
1. Avvia l'istanza EC2 per Mac. A tale scopo, scegli una delle seguenti procedure dalla Guida per l'utente di Amazon EC2:
 - [Avvia un'istanza Mac utilizzando la console](#)
 - [Avvia un'istanza Mac utilizzando il AWS CLI](#)
2. Connect alla tua istanza EC2 per Mac utilizzando Virtual Network Computing (VNC). Per ulteriori informazioni, consulta [Connect to your instance using VNC](#) nella Amazon EC2 User Guide.
3. Sulla tua istanza Mac EC2, connettiti alla condivisione di FSx file Amazon, 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 [FSx console Amazon](#) scegliendo Windows File Server, rete e sicurezza. Oppure, puoi trovarli nella risposta dell'operazione [CreateFileSystem](#) [DescribeFileSystems](#) dell'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 FSx servizio Amazon, come mostrato nell'esempio seguente. Quindi scegliere Connetti.



- e. Se la connessione è riuscita, puoi vedere la FSx condivisione Amazon nella sezione 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 il 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 [FSxconsole Amazon](#) 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 si sta 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 è aggiunta al tuo Active Directory o non unita per FSx accedere al tuo file system per Windows File Server.

Note

- I comandi seguenti specificano parametri come il protocollo SMB, la memorizzazione nella cache e le dimensioni del buffer di lettura e scrittura solo a titolo di esempio. 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 per l'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 a un 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 instance](#) 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 dei punti di montaggio `/mnt/fsx`. Qui è dove installerai il FSx file system Amazon.

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

5. Effettua l'autenticazione con kerberos usando 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,cuid=ad_user,rsiz=CIFSMaxBufSize,wsiz=CIFSMaxBufSize,cache=no
file-server-IP
```

Puoi trovare il nome DNS sulla [FSxconsole Amazon](#) scegliendo Windows File Server, Rete e sicurezza. Oppure, puoi trovarli nella risposta della nostra CreateFileSystem operazione 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 si sta montando il file system.
- `-t cifs vers=SMB_version`— Specifica 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 ed 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.
- `cuid=ad_user`— Imposta l'uid del proprietario della cache delle credenziali all'amministratore della directory AD.
- `/mnt/fsx`— Specifica il punto di montaggio per la condivisione di file Amazon FSx sull'istanza EC2.
- `rsize=CIFSMaxBufSize, wsize=CIFSMaxBufSize`— Specifica 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 FSx console Amazon, 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 unita a un 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 per Windows File Server solo utilizzando il relativo indirizzo IP privato. Puoi ottenere l'indirizzo IP privato del file system utilizzando la [FSx console Amazon](#), nella scheda Rete e sicurezza, in Indirizzo IP preferito del file server.

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 instance](#) 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 FSx file system Amazon.

```
$ 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 [FSx console Amazon](#), 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=ntlmssp,cred=/home/ec2-user/  
creds.txt,rsize=CIFSMaxBufSize,wsiz=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=ntlmssp,cache=cache_mode,username=user1,domain=CORP.EXAMPLE)
```

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

- *//file-system-IP-address/file_share*— Specificano l'indirizzo IP e la condivisione del file system che state montando.
- *-t cifs vers=SMB_version*— Specifica 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=ntlmssp`— 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 ed 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`— Specifica dove ottenere le credenziali dell'utente.
- `/mnt/fsx`— Specifica il punto di montaggio per la condivisione di file Amazon FSx sull'istanza EC2.
- `rsize=CIFSMaxBufSize`, `wsize=CIFSMaxBufSize`— Specifica 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)
```

Monta automaticamente le condivisioni di file su un'istanza Amazon EC2 Linux

Puoi montare automaticamente la condivisione di file FSx for Windows File Server per accedere al file system 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 comando `mount -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 per Windows File Server solo utilizzando il relativo indirizzo IP privato. Puoi ottenere l'indirizzo IP privato del file system utilizzando la [FSx console Amazon](#), nella scheda Rete e sicurezza, in Indirizzo IP preferito del file server.

La procedura seguente utilizza l'autenticazione Microsoft NTLM. Il file system viene montato come utente membro del dominio Microsoft Active Directory a cui fa parte il file system FSx for Windows File Server. È possibile recuperare le credenziali per l'account utente dal `creds.txt` file utilizzando il comando seguente.

```
$ 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 instance](#) 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`. Qui è dove installerai il FSx file system Amazon.

```
$ 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 [FSx console Amazon](#), nella scheda Rete e sicurezza, in Indirizzo IP preferito del file server.
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=ntlmssp,cred=/home/ec2-user/  
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none 0 0
```

Sostituisci **CIFSMaxBufSize** con il valore massimo consentito dal tuo kernel. Esegui 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=ntlmssp,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 FSx file system Amazon che stai montando.
- `/mnt/fsx`: specifica il punto di montaggio per il file system Amazon FSx sull'istanza EC2.
- `cifs vers=SMB_version`— Specifica 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=ntlmssp`— 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 ed 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`— Specifica 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 `dadump`, se è un valore diverso da zero. Per Amazon FSx, questo valore dovrebbe essere `0`.
- `0`— Specifica l'ordine in cui `fsck` controlla i file system all'avvio. Per i FSx file system Amazon, questo valore dovrebbe essere `0` indicare che non `fsck` deve essere eseguito all'avvio.

Creazione, aggiornamento e rimozione di condivisioni di file

Questo argomento descrive come gestire le condivisioni di file eseguendo le seguenti attività.

- Creare una nuova condivisione di file
- Modificare una condivisione di file esistente
- Rimuovere una condivisione di file esistente

Puoi utilizzare la GUI delle cartelle condivise native di Windows e l'Amazon FSx CLI per la gestione PowerShell remota per gestire le condivisioni di file sul tuo file system FSx per 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.

Microsoft Windows impone regole e limitazioni per la denominazione 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, consulta [Convenzioni di denominazione](#).

 Warning

Amazon FSx richiede che l'utente SYSTEM disponga delle autorizzazioni ACL NTFS Full control su ogni cartella in cui crei una condivisione di file SMB. Non modificare le autorizzazioni NTFS ACL per questo utente sulle tue cartelle, poiché così facendo potresti 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 FSx file system Amazon, puoi utilizzare la GUI 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 per Windows File Server

1. Avvia la tua EC2 istanza Amazon e collegala a Microsoft Active Directory a cui è collegato il tuo FSx file system Amazon. A tale scopo, scegli una delle seguenti procedure dalla Guida all'AWS Directory Service amministrazione:
 - [Unisciti senza problemi a un'istanza di 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 FSx Amministratori AWS delegati. 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) del tuo FSx file system Amazon, ad esempio **amznfsxabcd0123.corp.example.com**.

Per trovare il nome DNS del tuo file system sulla FSx console Amazon, 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 [DescribeFileSystemsAPI](#).

6. Scegli OK. Viene quindi visualizzata una voce relativa al tuo FSx file system Amazon nell'elenco dello strumento Cartelle condivise.

Ora che Shared Folders è connesso al tuo FSx file system Amazon, puoi gestire le condivisioni di file Windows sul file system. Viene chiamata la condivisione predefinita `\share`. È possibile farlo con le seguenti azioni:

- Crea una nuova condivisione di file: nello strumento Cartelle condivise, scegli Condivisioni nel riquadro a sinistra per vedere le condivisioni attive per il tuo FSx file system Amazon. 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. Modificate le proprietà e scegliete OK.
- Rimuovi una condivisione di file: nello strumento Cartelle condivise, apri il menu contestuale (fai clic con il pulsante destro del mouse) relativo alla condivisione di file che desideri rimuovere nel riquadro di destra, quindi scegli Interrompi condivisione.

 Note

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 ti connetti 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 presenti su più file system FSx per Windows File Server, potrebbero verificarsi ritardi alla prima apertura del menu contestuale di condivisione di file per una condivisione che si trova 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 FSx per Windows File Server per PowerShell. Questi comandi possono aiutarti ad automatizzare la gestione di attività di condivisione di file come:

- Migrazione di condivisioni di file da file server esistenti ad Amazon FSx
- Sincronizzazione delle condivisioni di file Regioni AWS per il disaster recovery
- Gestione programmatica dei flussi di lavoro di condivisione di file in corso, ad esempio il provisioning della condivisione di file tra team

Per informazioni su come utilizzare l'Amazon FSx CLI per la gestione remota su PowerShell, consulta [Utilizzo dell'Amazon FSx CLI per PowerShell](#)

La tabella seguente elenca i PowerShell comandi di gestione remota di Amazon FSx CLI che puoi utilizzare per gestire le condivisioni di file sui FSx file system Windows File Server.

Comando di gestione della condivisione	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 tutte le autorizzazioni ACEs 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 tutta la negazione ACEs di 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-FSxSmbShare

È possibile passare le credenziali a New, in FSx SmbShare 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 Gestione dei segreti AWS risorsa, utilizzate il comando seguente.

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

Per creare una condivisione a disponibilità continua (CA)

Puoi creare condivisioni a disponibilità continua (CA) utilizzando l'Amazon FSx CLI for Remote Management on. PowerShell Le condivisioni CA create su un file system Multi-AZ FSx per Windows File Server 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 estremamente 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-fsxshare -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-fsxshare -name share_name -ContinuouslyAvailable $True}
```

Il FSx SmbShare comando New- ha esito negativo con un trust unidirezionale

Amazon FSx non supporta l'esecuzione del New-FSxSmbShare PowerShell comando nei casi in cui disponi di un trust unidirezionale e il dominio in cui risiede l'utente non è configurato per considerare attendibile il dominio associato al FSx file system Amazon.

Puoi risolvere questa situazione utilizzando una delle seguenti soluzioni:

- L'utente che esegue il New-FSxSmbShare comando deve appartenere allo stesso dominio del FSx file system.
- 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](#).

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 monitora FSx continuamente i guasti hardware e ripristina automaticamente gli eventi di guasto sostituendo il componente dell'infrastruttura guasto. I file system Single-AZ di solito subiscono circa 30 minuti di inattività durante gli eventi di ripristino in caso di guasto e durante la finestra di manutenzione pianificata 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 AZs (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 ciascuno dei due AZs. I dati vengono replicati in modo sincrono all'interno di ogni singola AZ e tra le due. AZs Rispetto all'implementazione Single-AZ, le implementazioni Multi-AZ offrono una maggiore durabilità grazie all'ulteriore replica dei dati e una maggiore disponibilità durante la manutenzione pianificata AZs 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 da guasti delle istanze e interruzioni della fase di disponibilità.

Scelta del tipo di implementazione del 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 disponibilità e requisiti RPO ridotti 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 e, in rari casi, la perdita di aggiornamenti dei dati dopo il backup più recente.

Consigliamo inoltre di esaminare il modello di disponibilità per il file system e di garantire che il carico di lavoro sia resiliente al comportamento di ripristino previsto per il tipo di distribuzione scelto durante eventi come la manutenzione del file system, le modifiche della capacità di throughput e le interruzioni non pianificate del servizio.

Supporto delle funzionalità per tipo di implementazione

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

Il tipo di implementazione	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

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 in genere viene 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.

Durante il breve periodo in cui il file system è in fase di failover e failback, I/O potrebbe essere messo in pausa e i CloudWatch parametri Amazon potrebbero essere temporaneamente non disponibili. Per i file system Multi-AZ, qualsiasi attività di lettura e scrittura dei file che si verifica durante il failover e il failback dovrà essere sincronizzata tra i file server primari e secondari. Questo processo può richiedere fino a diverse ore per i file system con storage su HDD e per i carichi di lavoro con elevati livelli di scrittura e IOPS. Consigliamo di testare l'impatto dei failover sull'applicazione quando 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 soddisfare 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 prima il file server preferito. Quindi il file system torna automaticamente al nuovo server primario e Amazon FSx sostituisce il file server secondario.

Puoi monitorare l'avanzamento della richiesta di aggiornamento della capacità di throughput nella FSx console Amazon, nella CLI e nell'API. Una volta completato con successo l'aggiornamento, il file system è passato al server secondario e al 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](#)

Risorse del file system Single-AZ e Multi-AZ

I file system Single-AZ e Multi-AZ utilizzano le sottoreti e le interfacce di rete elastiche in modo diverso, come spiegato nelle sezioni seguenti.

Sottoreti

Quando si crea un cloud privato virtuale (VPC), si estende su tutte le zone di disponibilità (AZs) di Regione AWS. 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. Una sottorete è un intervallo di indirizzi IP nel VPC. Una sottorete deve risiedere in una singola zona di disponibilità.

FSx per Windows File Server I file system Single-AZ richiedono una sottorete specificata al momento della creazione. La sottorete scelta definisce la zona di disponibilità in cui viene creato il file system.

I file system Multi-AZ richiedono 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

Un'[interfaccia di rete elastica](#) è un componente di rete logico in un VPC che rappresenta una scheda di rete virtuale. Quando crei un FSx file system Amazon, Amazon FSx fornisce una o più interfacce di rete elastiche nel VPC associato al file system. L'elastic network interface consente ai client di comunicare e montare il file system. L'elastic network interface 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 modificate o eliminate le interfacce di rete elastiche associate ai 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 l'utilizzo delle risorse FSx per i file system Windows File Server Single-AZ e Multi-AZ:

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.

Lavorare con Microsoft Active Directory

Quando si crea un file system FSx per Windows File Server, lo si aggiunge al dominio Active Directory per fornire l'autenticazione degli utenti e il controllo degli accessi a livello di file e cartella. Amazon FSx collabora con Microsoft Active Directory per l'integrazione con gli ambienti Microsoft Windows esistenti. Amazon FSx offre due opzioni utilizzando FSx il file system Windows File Server con Active Directory: [Usare Amazon FSx con AWS Directory Service for Microsoft Active Directory](#) e [Utilizzo di un Microsoft Active Directory autogestito](#).

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.

Gli utenti possono quindi utilizzare le identità utente esistenti in Active Directory per autenticarsi e accedere al file system FSx per Windows File Server. 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 insieme alla loro configurazione della lista di controllo degli accessi di sicurezza (ACL) su Amazon FSx senza alcuna modifica.

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 con Microsoft Active Directory del nuovo file system. Per ulteriori informazioni, consulta [Ripristino dei backup su un nuovo file system](#).

 Note

Amazon non FSx supporta [Active Directory Connector](#) e [Simple Active Directory](#).

Il file server FSx per Windows potrebbe non essere configurato correttamente se viene apportata una modifica alla configurazione di Active Directory che interrompe la connessione al file system. Per riportare il file system allo stato Disponibile, seleziona il pulsante Attempt Recovery nella FSx console Amazon o usa il StartMisconfiguredStateRecovery comando nell' FSx API o nella console Amazon. Per ulteriori informazioni, consulta [Il file system è in uno stato configurato in modo errato](#).

Argomenti

- [Usare Amazon FSx con AWS Directory Service for Microsoft Active Directory](#)
- [Utilizzo di un Microsoft Active Directory autogestito](#)

Usare 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 tuo FSx file system Amazon con AWS Managed Microsoft AD. In questo modo, ottieni una soluzione chiavi in mano utilizzando Amazon FSx con AWS Managed Microsoft AD. 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 FSx console Amazon. Quando crei un nuovo file system FSx per Windows File Server nella console,

scegli AWS Managed Active Directory nella sezione Autenticazione di Windows. Scegliete anche la directory specifica che desiderate utilizzare. Per ulteriori informazioni, consulta [Fase 5. 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 FSx file system Amazon direttamente al tuo dominio Active Directory esistente e autogestito. Per ulteriori informazioni, consulta [Utilizzo di un Microsoft Active Directory autogestito](#).

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

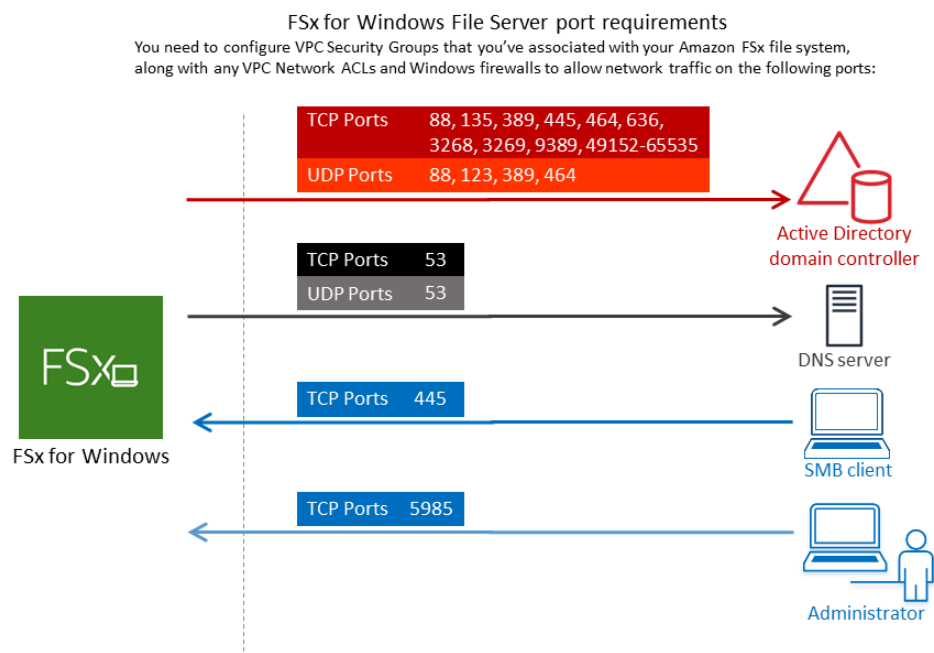
 Important

Per Single-AZ 2 e tutti i file system Multi-AZ, il nome di dominio completo (FQDN) di Active Directory non può superare i 47 caratteri.

Prerequisiti di rete

Prima di creare un file system FSx per Windows File Server aggiunto al dominio AWS Microsoft Managed Active Directory, assicurati 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 la rete VPC ACLs per le sottoreti in cui stai creando il FSx file system 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	Domains Name System (DNS)
TCP/UDP	88	Autenticazione Kerberos
TCP/UDP	464	Modifica reimpostazione della password

Protocollo	Porte	Ruolo
TCP/UDP	389	Lightweight Directory Access Protocol
UDP	123	Network Time Protocol (NTP)
TCP	135	Distributed Component Environment/End Point Mapper (DCE/EPMA P)
TCP	445	Condizione di file SMB di Servizio diretto

Protocollo	Porte	Ruolo
TCP	636	Lightweight Directory Access Protocol su TLS/SSL (LDAP)
TCP	3268	Catalogo globale Microsoft
TCP	3269	Microsoft Global Catalog tramite SSL
TCP	5985	WinRM 2.0 (gestione remota di Microsoft Windows)
TCP	9389	Servizio Web Microsoft AD DS, PowerShell

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 una rete VPC ACLs, devi anche consentire il traffico in uscita su porte dinamiche (49152-65535) dal tuo file system. FSx

- Se stai connettendo il tuo FSx file system Amazon a un Microsoft Active Directory AWS 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 AWS Managed Microsoft AD un 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, la rete VPC ACLs richiede che le porte siano aperte in entrambe le direzioni.

Utilizza lo [strumento Amazon FSx Network Validation](#) 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 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 AWS gestito. In uno scenario di autenticazione Kerberos, le richieste di autenticazione provenienti da un client aziendale vengono convalidate dal dominio aziendale, che quindi le rimanda al file system Windows File Server e infine il AWS Managed Microsoft AD client presenta il ticket di servizio al file system Windows File Server FSx utilizzato. Per ulteriori informazioni sui trust, consulta il post [Tutto quello che volevi sapere sui trust nel Security Blog. AWS Managed Microsoft AD](#) AWS

Verifica la configurazione di Active Directory

Prima di creare il tuo FSx file system Amazon, ti consigliamo di convalidare la connettività ai controller di dominio Active Directory utilizzando lo strumento Amazon FSx Network Validation. Per ulteriori informazioni, consulta [Convalida della connettività ai controller di dominio Active Directory](#).

Le seguenti risorse correlate possono esserti utili nell'utilizzo AWS Directory Service for Microsoft Active Directory di Windows File FSx Server:

- [Cosa contiene Directory Service](#) la Guida AWS Directory Service all'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

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

Puoi unire il tuo file system FSx per Windows File Server a una AWS Managed Microsoft AD directory che si trova in un altro VPC all'interno dello stesso account utilizzando il peering VPC. Puoi anche unire il tuo file system a una AWS Managed Microsoft AD directory che si trova in un AWS account diverso utilizzando la condivisione delle directory.

 Note

Puoi 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 un 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'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 VPCs

Un gateway di transito è un hub di transito di rete che puoi utilizzare per interconnettere le tue reti VPCs e quelle locali. Per ulteriori informazioni sull'utilizzo di VPC Transit Gateway, consulta l'argomento relativo alle [nozioni di base su Transit Gateway](#) nella Guida di Amazon VPC Transit Gateway.

Una connessione peering VPC è una connessione di rete tra due VPCs. Questa connessione consente di instradare il traffico tra di loro utilizzando indirizzi privati del protocollo Internet versione 4 (IPv4) o del protocollo Internet versione 6 (IPv6). Puoi utilizzare il peering VPC per connetterti VPCs all'interno dello stesso Regione AWS o tra di essi. 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 di 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 per Windows File Server aggiunto al tuo Active Directory, utilizza lo strumento di convalida di Amazon FSx Active Directory per convalidare la connettività al tuo dominio Active Directory. È possibile utilizzare questo test sia FSx per Windows File Server con Microsoft Active Directory AWS gestito che con una configurazione Active Directory autogestita. Il test di connettività di rete del controller di dominio (FSxADControllerTest-Connection) non esegue la suite completa di controlli della connettività di rete su tutti i controller di dominio del dominio. Utilizza 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 FSx il tuo file system per 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 Windows ad Active Directory. Per ulteriori informazioni, consulta [Aggiungere manualmente un'istanza di Windows](#) nella Guida all'AWS Directory Service amministrazione.
3. Connect alla tua EC2 istanza. Per ulteriori informazioni, consulta [Connecting to Your Windows Instance](#) nella Amazon EC2 User Guide.
4. Apri una PowerShell finestra Windows (usando Esegui come amministratore) sull' EC2 istanza.

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 FSx ADValidation modulo Amazon 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; Result=Listening; Description=Kerberos authentication}, @{Port=123; Result=Listening; Description=Kerberos authentication}}
Server	10.0.75.243
UdpDetails	{@{Port=88; Result=Timed Out; Description=Kerberos authentication}, @{Port=123; Result=Listening; Description=Kerberos authentication}}
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

```

 Note

In alternativa alla procedura precedente, è possibile utilizzare il `AWSSupport-ValidateFSxWindowsADConfig` runbook per convalidare la configurazione di Active Directory autogestita. Per ulteriori informazioni, consulta [AWSSupport-ValidateFSxWindowsADConfig](#) in Documentazione di riferimento del runbook di AWS Systems Manager Automation.

Utilizzo di un Microsoft Active Directory autogestito

Se la tua organizzazione gestisce identità e dispositivi utilizzando un Active Directory autogestito in locale o nel cloud, puoi aggiungere un file system FSx per Windows File Server al tuo dominio Active Directory al momento della creazione.

Quando si aggiunge il file system all'Active Directory autogestito, il file system FSx per Windows File Server 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, compresi i tuoi file system FSx Amazon, in una foresta Active Directory separata da quella in cui risiedono gli utenti. A tale scopo, collegate il vostro file system a un sistema Microsoft Active Directory AWS gestito e stabilite una relazione di trust forestale unidirezionale tra una AWS Microsoft Active Directory gestita da voi e la vostra Active Directory autogestita esistente.

- Nome utente e password per un account di servizio sul tuo dominio Active Directory, che Amazon può utilizzare FSx per aggiungere il file system al tuo dominio Active Directory. Puoi fornire queste credenziali come testo semplice o archivarle Gestione dei segreti AWS e fornire l'ARN segreto (consigliato).
- (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 di Windows, gestire gli elenchi di controllo degli accessi (ACLs) 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 per Windows File Server non creerà il gruppo di dominio 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 FSx file system Amazon a un dominio Microsoft Active Directory autogestito](#).

Argomenti

- [Prerequisiti](#)
- [Autorizzazioni dell'account di servizio](#)
- [Procedure consigliate per l'utilizzo di un Active Directory autogestito](#)
- [Account FSx di servizio Amazon](#)
- [Delegare le autorizzazioni all'account o al gruppo FSx di servizio Amazon](#)
- [Convalida della configurazione di Active Directory](#)
- [Unire un FSx file system Amazon a un dominio Microsoft Active Directory autogestito](#)
- [Ottenere gli indirizzi IP corretti del file system da utilizzare per le immissioni DNS manuali](#)
- [Aggiornamento di una configurazione di Active Directory autogestita](#)
- [Modifica dell'account del FSx servizio Amazon](#)
- [Monitoraggio degli aggiornamenti di Active Directory gestiti autonomamente](#)

Prerequisiti

Prima di aggiungere un file system FSx per Windows File Server al tuo dominio Microsoft Active Directory autogestito, esamina i seguenti prerequisiti per assicurarti di poter aggiungere correttamente il tuo FSx file system Amazon al tuo Active Directory autogestito.

Configurazioni locali

Questi sono i prerequisiti per il tuo Microsoft Active Directory autogestito, locale o basato sul cloud, a cui unirai il file system Amazon. FSx

- I controller di dominio Active Directory:
 - Deve avere un livello di funzionalità del dominio pari o superiore a Windows Server 2008 R2.
 - Deve essere scrivibile.
 - Almeno uno dei controller di dominio raggiungibili deve essere un catalogo globale della foresta.
- Il server DNS deve essere in grado di risolvere i nomi come segue:
 - Nel dominio in cui si sta entrando a far parte del file system
 - Nel dominio principale della foresta
- Gli indirizzi IP del server DNS e del controller di dominio Active Directory devono soddisfare i seguenti requisiti, che variano a seconda della data di creazione del FSx file system Amazon:

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 presenti nel file system. Regione AWS Per un elenco di indirizzi IP di AWS proprietà per regione, consulta gli intervalli di indirizzi AWS IP. • Indirizzi IP nell'intervallo di blocchi CIDR di 198.19.0.0/16

Se devi accedere a un file system FSx per Windows File Server creato prima del 17 dicembre 2020 utilizzando un intervallo di indirizzi IP non privato, puoi creare un nuovo file system ripristinando un backup del file system. Per ulteriori informazioni, consulta [Ripristino di un backup su un nuovo file system](#).

- Il nome di dominio dell'Active Directory autogestito deve soddisfare i seguenti requisiti:

- Il nome di dominio 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 non può superare i 47 caratteri.
- Tutti i siti di Active Directory che hai definito devono soddisfare i seguenti prerequisiti:
 - Le sottoreti nel VPC associato al file system devono essere definite in un sito di Active Directory.
 - Non vi sono conflitti tra le sottoreti VPC e le sottoreti del sito di Active Directory.

Amazon FSx richiede la connettività ai controller di dominio o ai siti di Active Directory che hai definito nel tuo ambiente Active Directory. Amazon FSx ignorerà qualsiasi controller di dominio con TCP e UDP bloccati sulla porta 389. Per i restanti controller di dominio presenti in Active Directory, assicurati che soddisfino i requisiti di FSx connettività di Amazon. Inoltre, verifica che tutte le modifiche al tuo account di servizio vengano propagate a tutti questi controller di dominio.

 Important

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

Puoi convalidare la configurazione di Active Directory, incluso il test della connettività di più controller di dominio, utilizzando lo strumento di [convalida di Amazon FSx Active Directory](#). 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

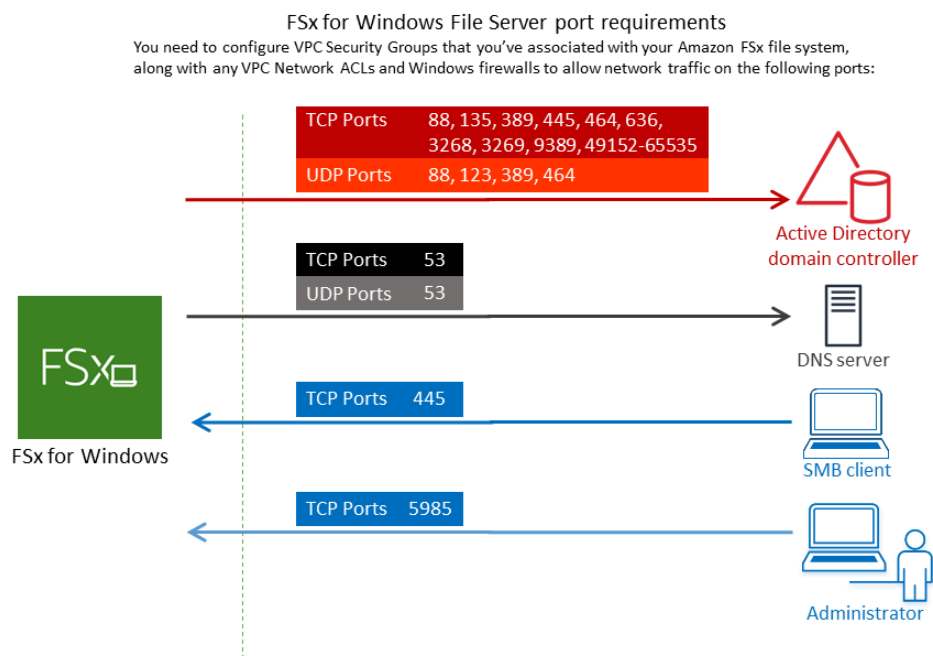
Amazon registra i record DNS per un file system FSx solo se utilizzi Microsoft DNS come servizio DNS predefinito. Se utilizzi un DNS di terze parti, dovrai configurare manualmente le voci dei record DNS per il tuo file system dopo averlo creato.

Configurazioni di rete

Questa sezione descrive i requisiti di configurazione di rete per aggiungere un file system all'Active Directory autogestito. Ti consigliamo vivamente di utilizzare lo [strumento di convalida di Amazon FSx](#)

[Active Directory](#) per testare le impostazioni di rete prima di tentare di aggiungere il tuo file system all'Active Directory autogestito.

- Assicurati che le regole del firewall consentano il traffico ICMP tra i controller di dominio Active Directory e Amazon. FSx
- 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 [Direct Connect](#), [AWS Virtual Private Network](#), il [peering VPC](#) o [AWS Transit Gateway](#)
- Il gruppo di sicurezza VPC predefinito per il tuo Amazon VPC predefinito deve essere aggiunto al tuo file system utilizzando la console Amazon. FSx Assicurati che il gruppo di sicurezza e la rete VPC ACLs per le sottoreti in cui crei il file system consentano il traffico sulle porte e nella direzione mostrata nel diagramma seguente.



La tabella seguente identifica il protocollo, le porte e il relativo ruolo.

Protocollo	Porte	Ruolo
TCP/UDP	53	Domain Name System (DNS)
TCP/UDP	88	Autenticazione Kerberos

Protocollo	Porte	Ruolo
TCP/UDP	464	Modifica/imposta la password
TCP/UDP	389	Lightweight Directory Access Protocol (LDAP)
UDP	123	Network Time Protocol (NTP)
TCP	135	Mappatore di Environment/End punti di calcolo distribuiti (DCE/EPMAP)
TCP	445	Condivisione di file SMB di Servizi directory
TCP	636	Lightweight Directory Access Protocol over (LDAPS) TLS/SSL
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  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.
TCP	49152 - 65535	Porte effimere per RPC

Queste regole di traffico devono essere rispecchiate anche sui firewall che si applicano a ciascuno dei controller di dominio, server DNS, client e amministratori di Active Directory. FSx FSx

 Note

Se utilizzi una rete VPC ACLs, devi anche consentire il traffico in uscita su porte dinamiche (49152-65535) dal tuo file system.

 Important

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

Autorizzazioni dell'account di servizio

È necessario disporre di un account di servizio nel proprio dominio Microsoft Active Directory autogestito con autorizzazioni delegate per aggiungere oggetti computer al dominio Active Directory autogestito. Un account di servizio è un account utente di Active Directory autogestito a cui sono state delegate determinate attività.

Di seguito è riportato il set minimo di autorizzazioni che devono essere delegate all'account di FSx servizio Amazon nell'unità organizzativa a cui ti stai unendo al file system.

- Se utilizzi Delegate Control nella MMC User and Computers di Active Directory:
 - Reimpostare le password
 - Leggi e scrivi le restrizioni relative all'account
 - Nome host DNS di scrittura convalidato
 - Nome principale del servizio di scrittura convalidato
- Se si utilizzano le funzionalità avanzate in MMC per utenti e computer di Active Directory:
 - Modifica le autorizzazioni
 - Creazione di oggetti computer
 - Eliminare gli oggetti del computer

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 sull'impostazione delle autorizzazioni richieste, vedere. [Delegare le autorizzazioni all'account o al gruppo FSx di servizio Amazon](#)

Procedure consigliate per l'utilizzo di un Active Directory autogestito

Argomenti

- [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#)

Ti consigliamo di seguire queste best practice quando unisci un file system Amazon FSx for Windows File Server al tuo Microsoft Active Directory autogestito. Queste best practice ti aiuteranno a mantenere la disponibilità continua e ininterrotta del tuo file system.

Usa un account di servizio separato per Amazon FSx

Utilizza un account di servizio separato per delegare [i privilegi richiesti](#) FSx ad Amazon per gestire completamente i file system aggiunti al tuo Active Directory autogestito. Non è consigliabile utilizzare Domain Admins per questo scopo.

Utilizzare un gruppo Active Directory

Utilizza un gruppo Active Directory per gestire le autorizzazioni e le configurazioni di Active Directory associate all'account del FSx servizio Amazon.

Separare l'unità organizzativa (OU)

Per semplificare la ricerca e la gestione degli oggetti FSx informatici Amazon, ti consigliamo di separare l'unità organizzativa (OU) che usi per i tuoi file system FSx per Windows File Server dagli altri controller di dominio.

Mantieni la configurazione di Active Directory up-to-date

È fondamentale mantenere la configurazione di Active Directory del file system up-to-date con eventuali modifiche. Ad esempio, se il tuo Active Directory autogestito utilizza una politica di reimpostazione della password basata sul tempo, non appena la password viene reimpostata, assicurati di aggiornare la password dell'account di servizio sul tuo file system. Per ulteriori informazioni, consulta [Aggiornamento di una configurazione di Active Directory autogestita](#).

Modifica dell'account del FSx servizio Amazon

Se aggiorni il file system con un nuovo account di servizio, quest'ultimo deve disporre delle autorizzazioni e dei privilegi necessari per accedere ad Active Directory e disporre delle

autorizzazioni di controllo completo per gli oggetti informatici esistenti associati al file system. Per ulteriori informazioni, consulta [Modifica dell'account del FSx servizio Amazon](#).

Assegnazione di sottoreti a un singolo sito di Microsoft Active Directory

Se il tuo ambiente Active Directory ha un numero elevato di controller di dominio, utilizza Active Directory Sites and Services per assegnare le sottoreti utilizzate dai tuoi FSx file system Amazon a un singolo sito Active Directory con la massima disponibilità e affidabilità. Assicurati che il gruppo di sicurezza VPC, l'ACL di rete VPC, le regole del firewall di Windows e tutti gli altri controlli di routing di rete presenti nella tua infrastruttura Active Directory consentano la comunicazione da Amazon sulle porte richieste. DCs FSx Ciò consente a Windows di tornare ad altri controller di dominio se non può utilizzare il sito Active Directory assegnato. Per ulteriori informazioni, consulta [Controllo degli accessi ai file system con Amazon VPC](#).

Utilizza le regole dei gruppi di sicurezza per limitare il traffico

Utilizza le regole dei gruppi di sicurezza per implementare il principio del privilegio minimo nel tuo cloud privato virtuale (VPC). Puoi limitare il tipo di traffico di rete in entrata e in uscita consentito per il tuo file utilizzando le regole del gruppo di sicurezza VPC. Ad esempio, consigliamo di consentire il traffico in uscita solo ai controller dei domini Active Directory autogestiti o all'interno della sottorete o del gruppo di sicurezza che state utilizzando. Per ulteriori informazioni, consulta [Controllo degli accessi ai file system con Amazon VPC](#).

Non spostare oggetti informatici creati da Amazon FSx

Important

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

Convalida la configurazione di Active Directory

Prima di tentare di aggiungere un file system FSx per Windows File Server ad Active Directory, ti consigliamo vivamente di convalidare la configurazione di Active Directory utilizzando lo strumento di [convalida di Amazon FSx Active Directory](#).

Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS

È possibile utilizzarlo per Gestione dei segreti AWS archiviare e gestire in modo sicuro le credenziali dell'account del servizio di accesso al dominio Microsoft Active Directory. Questo approccio elimina la necessità di archiviare credenziali sensibili in testo semplice nel codice dell'applicazione o nei file di configurazione, rafforzando il livello di sicurezza.

Puoi anche configurare le policy IAM per gestire l'accesso ai tuoi segreti e impostare policy di rotazione automatica per le tue password.

Archivia le credenziali di Active Directory in Gestione dei segreti AWS (Console)

Passaggio 1: creare una chiave KMS

Crea una chiave KMS per crittografare e decrittografare le credenziali di Active Directory in Secrets Manager.

Come creare una chiave

Note

Per la chiave di crittografia, crea una nuova chiave, non utilizzare la chiave KMS predefinita. AWS Assicurati di crearla AWS KMS key nella stessa regione che contiene il file system a cui desideri aggiungere ad Active Directory.

1. Apri la AWS KMS console in <https://console.aws.amazon.com/kms>.
2. Scegli Crea chiave.
3. In Tipo di chiave, scegli Simmetrica.
4. In Utilizzo delle chiavi, scegli Crittografia e decrittografia.
5. Per le opzioni avanzate, procedi come segue:
 - a. In Origine materiale chiave, scegli KMS.
 - b. Per Regionalità, scegli la chiave Single-Region e scegli Avanti.
6. Scegli Next (Successivo).
7. In Alias, fornisci un nome per la chiave KMS.

8. (Facoltativo) In Descrizione, immetti una descrizione per la chiave KMS.
9. (Facoltativo) Per i tag, fornisci un tag per la chiave KMS e scegli Avanti.
10. (Facoltativo) Per gli amministratori chiave, fornisci gli utenti e i ruoli IAM autorizzati a gestire questa chiave.
11. Per l'eliminazione della chiave, mantieni selezionata la casella Consenti agli amministratori chiave di eliminare questa chiave e scegli Avanti.
12. (Facoltativo) Per gli utenti chiave, fornisci gli utenti e i ruoli IAM autorizzati a utilizzare questa chiave nelle operazioni crittografiche. Scegli Next (Successivo).
13. Per Politica chiave, scegli Modifica e includi quanto segue nella dichiarazione sulla politica per consentire FSx ad Amazon di utilizzare la chiave KMS e scegli Avanti. Assicurati di *us-west-2* sostituirlo nel Regione AWS luogo in cui è distribuito il file system e nel tuo *123456789012* Account AWS ID.

```
{
  "Sid": "Allow FSx to use the KMS key",
  "Version": "2012-10-17",
  "Effect": "Allow",
  "Principal": {
    "Service": "fsx.amazonaws.com"
  },
  "Action": [
    "kms:Decrypt",
    "kms:DescribeKey"
  ],
  "Resource": "arn:aws:kms:us-west-2:123456789012:key/*",
  "Condition": {
    "StringEquals": {
      "kms:ViaService": "secretsmanager.us-west-2.amazonaws.com",
      "aws:SourceAccount": "123456789012"
    },
    "ArnLike": {
      "aws:SourceArn": "arn:aws:fsx:us-west-2:123456789012:file-system/*"
    }
  }
}
```

14. Scegli Fine.

 Note

Puoi impostare un controllo degli accessi più granulare modificando `aws:SourceArn` i campi `Resource` e in modo da indirizzarli a segreti e file system specifici.

Fase 2: Creare un segreto Gestione dei segreti AWS

Per creare un segreto

1. Apri la console Secrets Manager all'indirizzo <https://console.aws.amazon.com/secretsmanager/>.
2. Scegli Archivia un nuovo segreto.
3. Per Secret type (Tipo di segreto), scegli Other type of secret (Altro tipo di segreto).
4. Per le coppie chiave/valore, effettuate le seguenti operazioni per aggiungere le due chiavi:
 - a. Per la prima chiave, immetti `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`.
 - b. Per il valore della prima chiave, immetti solo il nome utente (senza il prefisso di dominio) dell'utente AD.
 - c. Per la seconda chiave, immetti `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`.
 - d. Per il valore della seconda chiave, immetti la password creata per l'utente AD nel dominio.
5. Per Chiave di crittografia, inserisci l'ARN della chiave KMS che hai creato in un passaggio precedente e scegli Avanti.
6. In Nome del segreto, inserisci un nome descrittivo che semplifichi l'individuazione del segreto in un secondo momento.
7. (Facoltativo) In Descrizione, inserisci una descrizione per il nome del segreto.
8. Per l'autorizzazione della risorsa, scegli Modifica.

Aggiungi la seguente politica alla politica di autorizzazione per consentire FSx ad Amazon di utilizzare il segreto, quindi scegli Avanti. Assicurati di *us-west-2* sostituirlo nel Regione AWS luogo in cui è distribuito il file system e *123456789012* nel tuo Account AWS ID.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
```

```

        "Service": "fsx.amazonaws.com"
    },
    "Action": [
        "secretsmanager:GetSecretValue",
        "secretsmanager:DescribeSecret"
    ],
    "Resource": "arn:aws:secretsmanager:us-west-2:123456789012:secret:*",
    "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "123456789012"
        },
        "ArnLike": {
            "aws:SourceArn": "arn:aws:fsx:us-west-2:123456789012:file-
system/*"
        }
    }
}

```

Note

Puoi impostare un controllo degli accessi più granulare modificando `aws:SourceArn` i campi `Resource` e in modo da indirizzarli a segreti e file system specifici.

9. (Facoltativo) È possibile configurare Secrets Manager per ruotare automaticamente le credenziali. Scegli Next (Successivo).
10. Scegli Fine.

Archivia le credenziali di Active Directory in Gestione dei segreti AWS (CLI)

Fase 1: Creare una chiave KMS

Crea una chiave KMS per crittografare e decrittografare le credenziali di Active Directory in Secrets Manager.

[Per creare una chiave KMS, usa il comando `create-key`. AWS CLI](#)

In questo comando, imposta il `--policy` parametro per specificare la politica chiave che definisce le autorizzazioni per la chiave KMS. La politica deve includere quanto segue:

- Il principale servizio per Amazon FSx, che è `fsx.amazonaws.com`.
- Azioni KMS richieste: `kms:Decrypt` e `kms:DescribeKey`.
- Schema ARN delle risorse per il tuo account Regione AWS .
- Chiavi condizionali che limitano l'utilizzo delle chiavi:
 - `kms:ViaService` per garantire che le richieste arrivino tramite Secrets Manager.
 - `aws:SourceAccount` da limitare al tuo account.
 - `aws:SourceArn` per limitarsi a specifici FSx file system Amazon.

L'esempio seguente crea una chiave KMS di crittografia simmetrica con una politica che consente ad Amazon FSx di utilizzare la chiave per le operazioni di decrittografia e descrizione delle chiavi. Il comando recupera automaticamente l' Account AWS ID e la regione, quindi configura la politica delle chiavi con questi valori per garantire controlli di accesso adeguati tra Amazon FSx, Secrets Manager e la chiave KMS. Assicurati che il tuo AWS CLI ambiente si trovi nella stessa regione del file system che entrerà a far parte di Active Directory.

```
# Set region and get Account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)

# Create Key
KMS_KEY_ARN=$(aws kms create-key --policy "{
  \"Version\": \"2012-10-17\",
  \"Statement\": [
    {
      \"Sid\": \"Enable IAM User Permissions\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"AWS\": \"arn:aws:iam::$ACCOUNT_ID:root\"
      },
      \"Action\": \"kms:*\",
      \"Resource\": \"*\"
    },
    {
      \"Sid\": \"Allow FSx to use the KMS key\",
      \"Effect\": \"Allow\",
      \"Principal\": {
        \"Service\": \"fsx.amazonaws.com\"
      },
      \"Action\": [
```

```

    \"kms:Decrypt\",
    \"kms:DescribeKey\"
  ],
  \"Resource\": \"*\",
  \"Condition\": {
    \"StringEquals\": {
      \"kms:ViaService\": \"secretsmanager.$REGION.amazonaws.com\",
      \"aws:SourceAccount\": \"$ACCOUNT_ID\"
    },
    \"ArnLike\": {
      \"aws:SourceArn\": \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\"
    }
  }
}
]
}" --query 'KeyMetadata.Arn' --output text)

echo "KMS Key ARN: $KMS_KEY_ARN"

```

Note

È possibile impostare un controllo degli accessi più granulare modificando `aws:SourceArn` i campi `Resource` and in modo da indirizzarli a segreti e file system specifici.

Fase 2: Creare un segreto Gestione dei segreti AWS

Per creare un codice segreto per consentire FSx ad Amazon di accedere al tuo Active Directory, usa il AWS CLI comando [create-secret](#) e imposta i seguenti parametri:

- `--name`: L'identificatore del tuo segreto.
- `--description`: Una descrizione dello scopo del segreto.
- `--kms-key-id`: L'ARN della chiave KMS che hai creato nel [passaggio 1](#) per crittografare il segreto inattivo.
- `--secret-string`: Una stringa JSON contenente le tue credenziali AD nel seguente formato:
 - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`: nome utente dell'account del servizio AD senza il prefisso del dominio, ad esempio. `svc-fsx` Non fornire il prefisso del dominio, ad esempio. `CORP\svc-fsx`

- `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD`: la password dell'account del servizio AD.
- `--region`: Il Regione AWS luogo in cui verrà creato il tuo FSx file system Amazon. Se non è impostata, l'impostazione predefinita `AWS_REGION` è la regione configurata.

Dopo aver creato il segreto, allega una politica delle risorse utilizzando il [put-resource-policy](#) comando e imposta i seguenti parametri:

- `--secret-id`: il nome o l'ARN del segreto a cui allegare la policy. L'esempio seguente utilizza **FSxSecret** come. `--secret-id`
- `--region`: Uguale Regione AWS al tuo segreto.
- `--resource-policy`: un documento di policy JSON che concede ad Amazon FSx l'autorizzazione ad accedere al segreto. La politica deve includere quanto segue:
 - Il principale servizio per Amazon FSx, che è **fsx.amazonaws.com**.
 - Azioni richieste di Secrets Manager: `secretsmanager:GetSecretValue` e `secretsmanager:DescribeSecret`.
 - Schema ARN delle risorse per il tuo account Regione AWS .
 - Le seguenti chiavi condizionali che limitano l'accesso:
 - `aws:SourceAccount` da limitare al tuo account.
 - `aws:SourceArn` per limitarsi a specifici FSx file system Amazon.

L'esempio seguente crea un segreto con il formato richiesto e allega una politica delle risorse che consente FSx ad Amazon di utilizzare il segreto. Questo esempio recupera automaticamente il tuo Account AWS ID e la tua regione, quindi configura la politica delle risorse con questi valori per garantire controlli di accesso adeguati tra Amazon FSx e il segreto.

Assicurati di sostituirlo `KMS_KEY_ARN` con l'ARN della chiave creata nel [passaggio 1](#) e `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD` con le credenziali `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME` dell'account del servizio Active Directory. Inoltre, verifica che l' AWS CLI ambiente sia configurato per la stessa regione del file system che entrerà a far parte di Active Directory.

```
# Set region and get account ID
REGION=${AWS_REGION:-$(aws configure get region)}
ACCOUNT_ID=$(aws sts get-caller-identity --query 'Account' --output text)
```

```

# Replace with your KMS key ARN from Step 1
KMS_KEY_ARN="arn:aws:kms:us-east-2:123456789012:key/1234542f-d114-555b-9ade-
fec3c9200d8e"

# Replace with your Active Directory credentials
AD_USERNAME="Your_Username"
AD_PASSWORD="Your_Password"

# Create the secret
SECRET_ARN=$(aws secretsmanager create-secret \
  --name "FSxSecret" \
  --description "Secret for FSx access" \
  --kms-key-id "$KMS_KEY_ARN" \
  --secret-string "{\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME\":\"$AD_USERNAME\",
\"CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD\":\"$AD_PASSWORD\"}" \
  --region "$REGION" \
  --query 'ARN' \
  --output text)

echo "Secret created with ARN: $SECRET_ARN"

# Attach the resource policy with proper formatting
aws secretsmanager put-resource-policy \
  --secret-id "FSxSecret" \
  --region "$REGION" \
  --resource-policy "{
    \"Version\": \"2012-10-17\",
    \"Statement\": [
      {
        \"Effect\": \"Allow\",
        \"Principal\": {
          \"Service\": \"fsx.amazonaws.com\"
        },
        \"Action\": [
          \"secretsmanager:GetSecretValue\",
          \"secretsmanager:DescribeSecret\"
        ],
        \"Resource\": \"$SECRET_ARN\",
        \"Condition\": {
          \"StringEquals\": {
            \"aws:SourceAccount\": \"$ACCOUNT_ID\"
          },
          \"ArnLike\": {

```

```
    \"aws:SourceArn\": \"arn:aws:fsx:$REGION:$ACCOUNT_ID:file-system/*\"  
  }  
}  
]  
}]  
}
```

```
echo "Resource policy attached successfully"
```

Note

È possibile impostare un controllo degli accessi più granulare modificando `aws:SourceArn` i campi `Resource` and in modo da indirizzarli a segreti e file system specifici.

Account FSx di servizio Amazon

I FSx file system Amazon uniti a un Active Directory autogestito richiedono un account di servizio valido per tutta la loro durata. Amazon FSx utilizza l'account di servizio per gestire completamente i tuoi file system ed eseguire attività amministrative che richiedono l'unione e il ricongiungimento degli oggetti del computer al tuo dominio Active Directory. Queste attività includono la sostituzione di un file server guasto e l'applicazione di patch al software Microsoft Windows Server. FSx Affinché Amazon possa eseguire queste attività, l'account di FSx servizio Amazon deve disporre almeno del set di autorizzazioni descritto in [Autorizzazioni dell'account di servizio](#) Delegato ad esso.

Sebbene i membri del gruppo Domain Admins abbiano privilegi sufficienti per eseguire queste attività, ti consigliamo vivamente di utilizzare un account di servizio separato per delegare i privilegi richiesti ad Amazon. FSx

Per ulteriori informazioni su come delegare i privilegi utilizzando le funzionalità Delegate Control o Advanced Features nello snap-in MMC Active Directory User and Computers, consulta. [Delegare le autorizzazioni all'account o al gruppo FSx di servizio Amazon](#)

Se si aggiorna il file system con un nuovo account di servizio, il nuovo account di servizio deve disporre delle autorizzazioni e dei privilegi necessari per accedere ad Active Directory e disporre delle autorizzazioni di controllo completo per gli oggetti informatici esistenti associati al file system. Per ulteriori informazioni, consulta [Modifica dell'account del FSx servizio Amazon](#).

Si consiglia di archiviare le credenziali dell'account del servizio Active Directory per una maggiore sicurezza Gestione dei segreti AWS . Ciò elimina la necessità di archiviare le credenziali sensibili

in testo semplice e si allinea alle migliori pratiche di sicurezza. Per ulteriori informazioni, consulta [Utilizzo di un Microsoft Active Directory autogestito](#).

Delegare le autorizzazioni all'account o al gruppo FSx di servizio Amazon

L'account o il gruppo di amministratori del FSx servizio Amazon deve disporre dei [privilegi necessari](#) FSx per accedere ai file system Windows File Server al tuo dominio Active Directory autogestito. Per delegare queste autorizzazioni, puoi utilizzare Delegate Control o Advanced Features nello Active Directory User and Computers MMC snap-in, come descritto nelle seguenti procedure.

Per assegnare le autorizzazioni utilizzando Delegate Control

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 FSx servizi Amazon, 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 committente e inserisci il nome del tuo account o gruppo di FSx servizi Amazon. Per Si applica a:, scegli Questo oggetto e tutti i computer discendenti. Assicuratevi che siano selezionati i seguenti elementi:
 - Modificare 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.

Convalida della configurazione di Active Directory

Prima di creare un file system FSx per Windows File Server unito ad Active Directory, ti consigliamo di convalidare la configurazione di Active Directory utilizzando lo strumento di convalida di 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**

- Preparate l'\$Credentialoggetto 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 Gestione dei segreti AWS risorsa, utilizzate il comando seguente.

```
$Secret = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
$AdminSecret).SecretString
$Credential = (New-Object PSredential($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 FSx file system Amazon (*SUBNET_1* ad *SUBNET_2* 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 README.md file incluso prima di eseguire lo strumento di convalida. DomainControllersMaxCount

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 con Amazon FSx](#)

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

Quando crei un nuovo file system FSx per Windows File Server, puoi configurare l'integrazione con Microsoft Active Directory in modo che venga aggiunto al tuo dominio Microsoft Active Directory autogestito. A tale scopo, fornisci le seguenti informazioni per Microsoft Active Directory:

- Il nome di dominio completo (FQDN) 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 del servizio Active Directory che Amazon FSx utilizza per aggiungere il file system al tuo dominio. Puoi fornirle in uno dei seguenti modi:
 - Opzione 1: ARN Gestione dei segreti AWS segreto: il segreto contenente il nome utente e la password per un account di servizio nel dominio Active Directory. Per ulteriori informazioni, consulta [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#).
 - Opzione 2: credenziali in chiaro
 - Nome utente dell'account di servizio: il nome utente dell'account di servizio nel Microsoft Active Directory esistente. Non includere un prefisso o un suffisso di dominio. Ad esempio `EXAMPLE\ADMIN`, solo per `ADMIN`
 - Password dell'account di servizio: la password per l'account di servizio.

È anche possibile specificare:

- Un'unità organizzativa (OU) specifica all'interno del dominio a cui desideri che il tuo FSx file system Amazon si unisca.
- Il nome del gruppo di dominio ai cui membri sono concessi i privilegi amministrativi per il FSx file system Amazon. Il nome del gruppo di dominio fornito deve essere univoco 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 registra i record DNS per un file system FSx 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 FSx file system Amazon 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 le immissioni DNS manuali](#)

Prima di iniziare

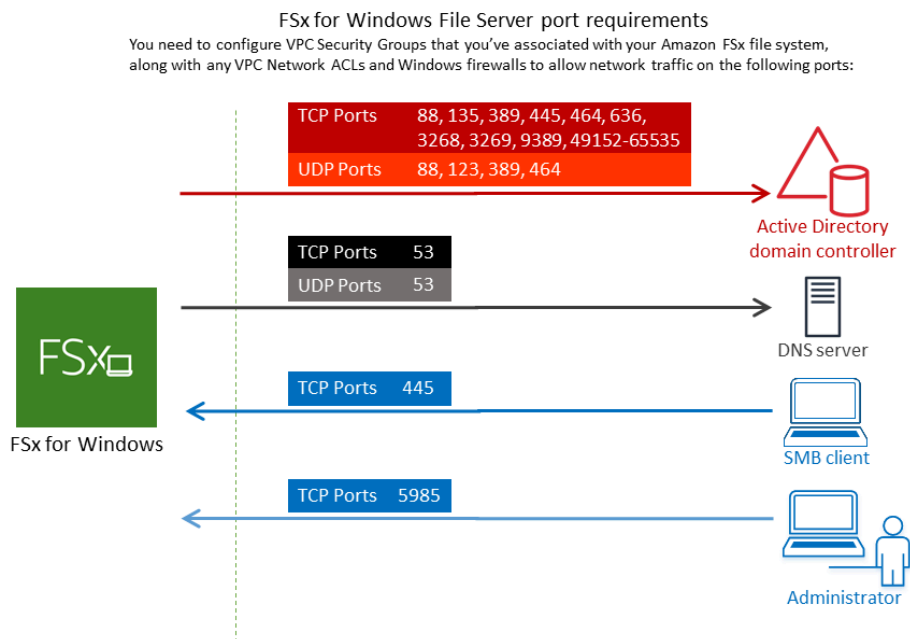
Assicurati di aver completato i [Prerequisiti](#) dettagli in [Utilizzo di un Microsoft Active Directory autogestito](#).

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

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Nel pannello di controllo, scegli Crea file system per avviare la procedura guidata di creazione del file system.
3. Scegli FSx 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 storage](#).
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 [FSx per le prestazioni di 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 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 la rete VPC ACLs per le sottoreti in cui stai creando il FSx file system 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

Protocollo	Porte	Ruolo
		System (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)
TCP	135	Distrib ed Comp Enviro nt/ End Point Mapp (DCE/ EPMA P)

Protocollo	Porte	Ruolo
TCP	445	Condizione di file SMB di Servizio direct
TCP	636	Lightweight Directory Access Protocol over TLS/SSL (LDAP)
TCP	3268	Catalogo globale Microsoft
TCP	3269	Microsoft Global Catalog tramite SSL

Protocollo	Porte	Ruolo
TCP	5985	WinRM 2.0 (gestione remota) di Microsoft Windows
TCP	9389	Servizio Web Microsoft Active Directory DS, Power I
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.

Note

Se utilizzi una rete VPC ACLs, 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, server DNS, client e amministratori di Active Directory. FSx FSx

Note

Se hai definito siti Active Directory, devi assicurarti che le sottoreti nel VPC associato al tuo file system FSx Amazon 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 delle reti VPC richiedono che le porte siano aperte in ACLs 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. Credenziali dell'account di servizio: scegli come fornire le credenziali del tuo account di servizio:
- Opzione 1: ARN Gestione dei segreti AWS segreto: il segreto contenente il nome utente e la password per un account di servizio nel dominio Active Directory. Per ulteriori informazioni, consulta [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#).
 - Opzione 2: credenziali in chiaro
 - Nome utente dell'account di servizio: il nome utente dell'account di servizio nel Microsoft Active Directory esistente. Non includere un prefisso o un suffisso di dominio. Ad esempio `EXAMPLE\ADMIN`, solo per. `ADMIN`
 - Password dell'account di servizio: la password per l'account di servizio.
 - Conferma password: la password per l'account di servizio.

 Important

NON includere un prefisso di dominio (`corp.com\ServiceAcct`) o un suffisso di dominio (`ServiceAcct@corp.com`) quando si immette 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`).

15. Per il gruppo Delegated file system administrators, 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 Domain Admins gruppo Builtin. Tieni presente che Amazon FSx non supporta la presenza di un contenitore Delegated file system administrators group (il Domain Admins gruppo o un gruppo personalizzato specificato) che si trova nel contenitore Builtin.

 Important

Se non fornisci un gruppo di amministratori di file system delegati, per impostazione predefinita Amazon FSx tenta di utilizzare il Domain Admins gruppo Builtin nel tuo dominio Active 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\ FSx Admins) 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= FSx Admins, OU=example, DC=corp, DC=com.

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

L'esempio seguente crea un file system FSx per Windows File Server con una SelfManagedActiveDirectoryConfiguration nella zona di us-east-2 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 FSx creati da Amazon nell'unità organizzativa dopo la creazione del file system. In questo modo il file system potrebbe essere configurato in modo errato.

Ottenere gli indirizzi IP corretti del file system da utilizzare per le immissioni DNS manuali

Amazon registra i record DNS per un file system FSx 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 FSx file system Amazon. 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. Nella <https://console.aws.amazon.com/fsx/>, scegli il file system di cui desideri 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 privato primario. IPv4
 - 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 privato secondario. IPv4
- 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 privato secondario. IPv4

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'IPv4 indirizzo privato primario per l'interfaccia di rete elastica per la sottorete Preferred. Per ulteriori informazioni, consulta [Utilizzo dell'Amazon FSx CLI per PowerShell](#).

Aggiornamento di una configurazione di Active Directory autogestita

Per garantire la disponibilità continua e ininterrotta del tuo FSx file system Amazon, devi aggiornare la configurazione di Active Directory del file system quando cambia una delle seguenti proprietà di Active Directory:

- Gli indirizzi IP del server DNS
- Le credenziali dell'account di servizio dell'Active Directory autogestito

Quando aggiorni la configurazione autogestita di Active Directory per il tuo FSx file system Amazon, 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.

 Important

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.

Per informazioni sulla risoluzione di possibili problemi relativi alle configurazioni di Active Directory autogestite, consulta [Il file system è in uno stato configurato in modo errato](#)

Puoi utilizzare Amazon FSx API o aggiornare le Console di gestione AWS credenziali dell'account AWS CLI 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 Console di gestione AWS 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 FSx console Amazon 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 autogestita di Active Directory.
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 (nome utente e password) o l'ARN segreto nella finestra di dialogo che appare. È possibile utilizzare Gestione dei segreti AWS per memorizzare le credenziali. Per ulteriori informazioni, consulta [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#).
5. Scegli Aggiorna per avviare l'aggiornamento della configurazione di Active Directory.

È possibile [monitorare l'avanzamento dell'aggiornamento](#) utilizzando Console di gestione AWS 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 per Windows File Server, utilizzare il comando. AWS CLI [update-file-system](#) Imposta i seguenti parametri:
 - `--file-system-id` dall'ID del file system che stai 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.
 - `DomainJoinServiceAccountSecret` il Gestione dei segreti AWS segreto contenente il nome utente e la password per un account di servizio nel dominio Active Directory

Note

Non puoi fornire entrambi username/password e un account segreto del servizio di accesso al dominio per connetterti ad Active Directory. Fornisci solo un set di credenziali.

- `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'`AdministrativeActions` oggetto nella risposta descrive la richiesta e il relativo stato.

Modifica dell'account del FSx servizio Amazon

Se aggiorni il file system con un nuovo account di servizio, il nuovo account di servizio deve disporre delle autorizzazioni e dei privilegi necessari per accedere ad Active Directory e disporre delle autorizzazioni di controllo completo per gli oggetti informatici esistenti associati al file system. Inoltre, assicurati che il nuovo account di servizio faccia parte degli account affidabili con l'impostazione dei Criteri di gruppo abilitata Controller di dominio: consenti il riutilizzo dell'account del computer durante l'aggiunta al dominio.

Consigliamo vivamente di utilizzare un gruppo Active Directory per gestire le autorizzazioni e le configurazioni di Active Directory associate agli account di servizio.

Quando modifichi l'account di servizio per Amazon FSx, assicurati che gli account di servizio abbiano le seguenti impostazioni:

- Il nuovo account di servizio (o il gruppo Active Directory di cui è membro) dispone delle autorizzazioni di controllo completo per gli oggetti informatici esistenti associati al file system.
- Gli account di servizio nuovi e precedenti (o il gruppo Active Directory di cui fanno parte) fanno parte degli account attendibili (o gruppo attendibile di Active Directory) con il controller di dominio: Consenti il riutilizzo degli account del computer durante l'aggiunta al dominio. L'impostazione Criteri di gruppo è abilitata su tutti i controller di dominio in Active Directory.

Se gli account di servizio non soddisfano questi requisiti, potrebbero verificarsi le seguenti condizioni:

- Per i file system Single-AZ, il file system potrebbe diventare [MISCONFIGURED_UNAVAILABLE](#).
- Per i file system Multi-AZ, il file system potrebbe non essere configurato correttamente e il nome dell'endpoint potrebbe [cambiare](#). RemotePowerShell

Configurazione dei criteri di gruppo di un controller di dominio

La seguente [procedura consigliata da Microsoft](#) descrive come utilizzare i Criteri di gruppo del controller di dominio per configurare i criteri di elenco consentiti.

Per configurare i criteri di elenco consentiti di un controller di dominio

1. Installa gli aggiornamenti di Microsoft Windows del 12 settembre 2023 o successivi su tutti i computer membri e i controller di dominio nel tuo Microsoft Active Directory autogestito.
2. In una politica di gruppo nuova o esistente che si applica a tutti i controller di dominio nell'Active Directory autogestito, configura le seguenti impostazioni.
 - a. Passa a Configurazione computer>Criteri>Impostazioni di Windows>Impostazioni di sicurezza> Criteri locali>Opzioni di sicurezza.
 - b. Fai doppio clic su Controller di dominio: consenti il riutilizzo dell'account del computer durante l'aggiunta al dominio.
 - c. <Edit Security ... >Seleziona Definisci questa impostazione dei criteri e.

- d. Utilizza il selettore di oggetti per aggiungere utenti o gruppi di creatori e proprietari di account di computer affidabili all'autorizzazione Consenti. (Come procedura consigliata, consigliamo vivamente di utilizzare i gruppi per le autorizzazioni.) Non aggiungere l'account utente che esegue l'aggiunta al dominio.

 Warning

Limita l'adesione alla policy agli utenti e agli account di servizio attendibili. Non aggiungere utenti autenticati, tutti o altri gruppi di grandi dimensioni a questa politica. Aggiungi invece utenti e account di servizio attendibili specifici ai gruppi e aggiungi tali gruppi alla politica.

3. Attendi l'intervallo di aggiornamento dei criteri di gruppo o esegui `gpupdate /force` su tutti i controller di dominio.
4. Verificate che la chiave di registro `HKLM\System\CCS\Control\SAM — «ComputerAccountReuseAllowList»` sia compilata con l'SDDL desiderato. Non modificate manualmente il registro.
5. Tentativo di accedere a un computer su cui sono installati gli aggiornamenti del 12 settembre 2023 o successivi. Assicurati che uno degli account elencati nella politica sia proprietario dell'account del computer. Assicurati inoltre che nel registro non sia abilitata la `NetJoinLegacyAccountReusechiave` (impostata su 1). Se l'aggiunta al dominio non riesce, controlla `c:\windows\debug\netsetup.log`.

Monitoraggio degli aggiornamenti di Active Directory gestiti autonomamente

Puoi monitorare lo stato di avanzamento di un aggiornamento della configurazione di Active Directory autogestito utilizzando Console di gestione AWS, l'API o il AWS CLI, come descritto nelle seguenti procedure.

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. Il completamento di un aggiornamento della configurazione di Active Directory può richiedere fino a diversi minuti.

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.

Updates (10)					
Filter updates					
					1
Update type ▼	Target value ▼	Status ▼	Progress % ▼	Request time ▲	
Storage capacity	154	✓ Completed	-	2020-05-22T12:14:58-04:00	
Throughput capacity	64	✓ Completed	-	2020-05-22T12:14:50-04:00	
Throughput capacity	128	✓ Completed	-	2020-05-21T13:55:58-04:00	
Storage capacity	140	✓ Completed	-	2020-05-21T13:55:30-04:00	
Storage capacity	122	✓ Completed	-	2020-05-18T11:36:33-04:00	

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 correttamente.
- 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 [describe-file-systems](#) AWS CLI comando e l'azione [DescribeFileSystems](#)API.

L'AdministrativeActionsarray 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 describe-file-systems.

L'output mostra due aggiornamenti del file system di 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."
            }
        },
    ],
    .
    .
    .
```

FSx per le prestazioni di Windows File Server

FSx per Windows File Server offre opzioni di configurazione del file system per soddisfare diverse esigenze di prestazioni. Di seguito è riportata una panoramica delle prestazioni del FSx file system di Amazon, con una discussione sulle opzioni di configurazione delle prestazioni disponibili e utili suggerimenti sulle prestazioni.

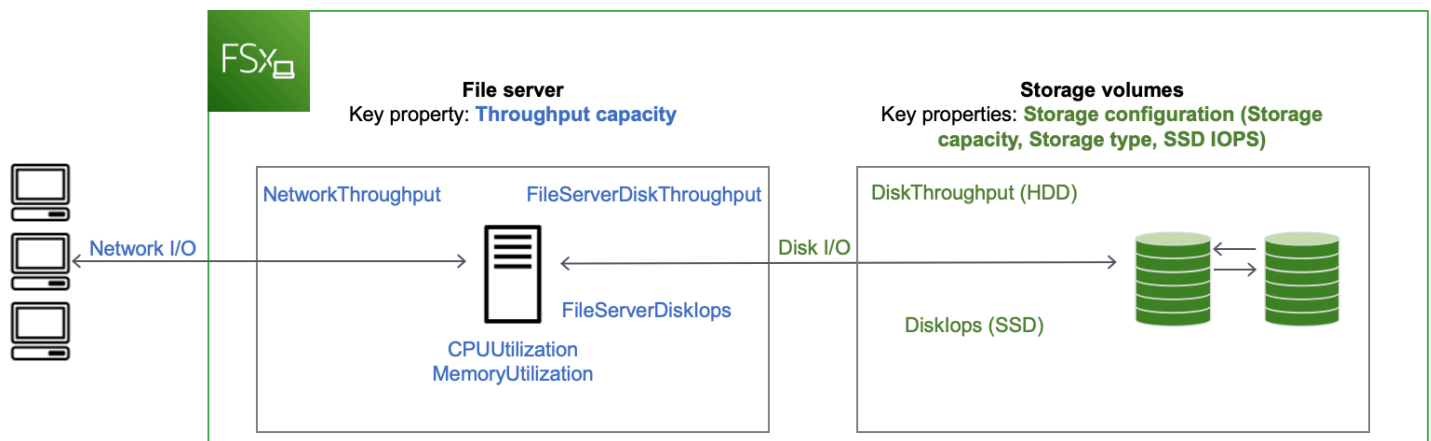
Argomenti

- [Prestazioni del file system](#)
- [Considerazioni aggiuntive sulle prestazioni](#)
- [Impatto della capacità di throughput sulle prestazioni](#)
- [Scelta del giusto livello di capacità di throughput](#)
- [Impatto della configurazione dello storage sulle prestazioni](#)
- [Esempio: capacità di archiviazione e capacità di throughput](#)
- [Misurazione delle prestazioni mediante metriche CloudWatch](#)
- [Risoluzione dei problemi di prestazioni del file system](#)

Prestazioni del file system

Ciascun 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 archiviazione, 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 per 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 I/O limiti 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 forniti dal file server al client come limiti di rete. I/O. The performance of this data access is determined by the network I/O limits as well as the disk I/O

I/O Le prestazioni di rete e la cache in memoria del file server sono determinate dalla capacità di trasmissione del file system. I/O Le prestazioni del disco sono determinate da una combinazione di capacità di throughput e configurazione di storage. Le I/O prestazioni massime del disco, che comprendono la velocità effettiva del disco e i livelli di IOPS del disco, che il file system è in grado di raggiungere sono le seguenti:

- Il livello di I/O prestazioni del disco fornito dal file server, in base alla capacità di trasmissione selezionata per il file system.
- Il livello di I/O prestazioni del disco fornito dalla configurazione di storage (la capacità di archiviazione, il tipo di storage e il 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 I/O alle operazioni al secondo (IOPS).

Latenza

FSx per i file server 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 eseguite 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 FSx file system di Amazon forniscono fino a 2 GBps e 80.000 IOPS in tutti i paesi in cui Regioni AWS Amazon FSx è disponibile e 12 GBps 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 la tecnologia multicanale per le piccole e medie imprese. Questa funzionalità consente di fornire fino a più GBps velocità effettiva 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 attività brevi e intensi, I/O con lunghi periodi di inattività tra un'interruzione e l'altra. Per supportare carichi di lavoro con picchi di lavoro, oltre alle velocità di base che un file system può supportare 24 ore su 24, 7 giorni su 7, Amazon FSx offre la possibilità di raggiungere velocità più elevate per periodi di tempo sia per le operazioni di rete che su disco. I/O Amazon FSx utilizza un meccanismo I/O di credito per allocare il throughput e gli IOPS in base all'utilizzo medio: i file system accumulano crediti quando il

loro throughput e l'utilizzo degli IOPS sono inferiori ai limiti di base e possono utilizzare questi crediti per eseguire operazioni. I/O

Impatto della capacità di throughput sulle prestazioni

La capacità di throughput determina le prestazioni del file system nelle seguenti categorie:

- Rete I/O : 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.
- Disco I/O : la velocità alla quale il file server è in grado di supportare la connessione I/O tra il file server e i volumi di archiviazione.

Le tabelle seguenti forniscono dettagli sui livelli massimi di rete I/O (throughput e IOPS) e disco I/O (throughput e IOPS) che è possibile gestire con ogni configurazione di capacità di throughput assegnata e sulla 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 utilizzi l'API FSx o la CLI di Amazon, 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).

Rete e memoria I/O

FSx capacità di trasmissione () MBps	Throughput di rete () MBps	IOPS di rete	Memoria (GB)
	Linea di base	Burst (per pochi minuti al giorno)	

FSx capacità di trasmissione () MBps	Throughput di rete () MBps		IOPS di rete	Memoria (GB)
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

FSx capacità di throughput () MBps	Velocità effettiva del disco () MBps		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

FSx capacità di throughput () MBps	Velocità effettiva del disco () MBps	IOPS del disco		
256	256	600	10.000	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 seleziona FSx 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 configurare una quantità specifica di capacità di throughput per soddisfare le esigenze del tuo carico di lavoro. Ad esempio, se il carico di lavoro richiede l'indirizzamento GBps dell'1% del traffico verso il file system, è necessario selezionare una capacità di throughput di almeno 1.024.

MBps La tabella seguente fornisce il livello minimo di capacità di throughput consigliato per un file system in base alla quantità di capacità di storage assegnata.

Capacità di archiviazione SSD (GiB)	Capacità di archiviazione HDD (GiB)	Capacità di throughput minima consigliata () MBps
Fino a 640	Fino a 3.200	32
641—1.280	3201—6.400	64
1281—2.560	6.401—12.800	128
2.561—5.120	12.801—25.600	256
5.121—10.240	25.601—51.200	512
10.241 — 20.480	> 51.200	1,024
>20.480	N/A	2.048

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 prestazionale disponibile. I/O 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 tuo 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 tua console Amazon FSx. Ti consigliamo di eseguire il test in un ambiente di preproduzione per assicurarti 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 alle metriche del file system](#).

Impatto della configurazione dello storage sulle prestazioni

La capacità di storage, il tipo di storage e il livello di IOPS SSD del file system influiscono tutti sulle I/O prestazioni del 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, consultare [Gestione della capacità di storage](#) 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 del file system](#).

Il file system fornisce i seguenti livelli predefiniti di velocità effettiva del disco e IOPS:

Storage Type (Tipo di storage)	Throughput del disco (MBps per TiB di storage)	IOPS su disco (per TiB di storage)
SSD	750	3.000 ¹
HDD	12 linee di base; 80 burst (fino a un massimo di 1 GBps per file system)	12 linee di base; 80 raffiche

Note

¹ 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 HDD, 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. Più crediti ha il volume, più a lungo può funzionare I/O a livello di burst.

La velocità effettiva disponibile di un volume di archiviazione HDD è espressa dalla seguente formula:

$$(\text{Volume size}) \times (\text{Credit accumulation rate per TiB}) = \text{Throughput}$$

Per un volume HDD da 1 TiB, il burst throughput è limitato a 80 MiBps, il bucket si riempie di crediti a 12 MiBps e può contenere fino a 1 TiB di crediti.

I volumi di storage HDD possono subire variazioni significative delle prestazioni a seconda del carico di lavoro. I picchi improvvisi degli IOPS o del throughput possono portare a un peggioramento delle prestazioni del disco. La [DiskThroughputBalance](#) metrica fornisce informazioni sul saldo dei crediti burst sia per la velocità effettiva del disco che per l'utilizzo degli IOPS del disco. Ad esempio, se il carico di lavoro supera i limiti di IOPS dell'HDD di base (12 IOPS per TiB di storage), l'utilizzo di IOPS su disco (HDD) sarà superiore al 100% e comporterà l'esaurimento del saldo del credito burst, come puoi vedere nella metrica. [DiskThroughputBalance](#) Affinché il carico di lavoro continui a generare elevati livelli di I/O, potrebbe essere necessario eseguire una delle seguenti operazioni:

- Riducete la I/O richiesta di carico di lavoro in modo da ricostituire il saldo del credito residuo.
- Aumentate la capacità di storage del file system per fornire un livello di base più elevato di IOPS su disco.
- Aggiorna il file system per utilizzare lo storage SSD, che fornisce un livello di base più elevato di IOPS su disco per soddisfare meglio i requisiti del carico di lavoro.

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 TiB di capacità MBps di throughput presenta i seguenti livelli di throughput:

- Throughput di rete: 32 linee di MBps base e 600 MBps burst (vedere la tabella sulla capacità di throughput)
- Throughput del disco: 24 linee di MBps base e 160 MBps burst, che è la più bassa tra:

- i livelli di velocità effettiva del disco, pari a 32 linee di MBps base e 260 MBps burst, supportati dal file server, in base alla capacità di trasmissione del file system
- i livelli di throughput del disco di 24 linee di MBps base (12 MBps per TB* 2 TiB) e 160 MBps burst (80 per TiB* 2 MBps 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 fino a 32 linee di MBps base e 600 MBps burst di velocità per le operazioni sui file eseguite sui dati ad accesso attivo memorizzati nella cache in memoria del file server e fino a 24 linee di MBps base e 160 MBps burst 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 con Amazon CloudWatch](#).

Risoluzione dei problemi di prestazioni del file system

Le prestazioni del file system FSx per Windows File Server dipendono da diversi fattori, tra cui il traffico indirizzato al file system, il modo in cui viene eseguito il provisioning del file system e le risorse utilizzate dalle funzionalità abilitate, come la deduplicazione dei dati o le copie shadow. Per informazioni sulla comprensione delle prestazioni del file system, vedere. [FSx per le prestazioni di Windows File Server](#)

Argomenti

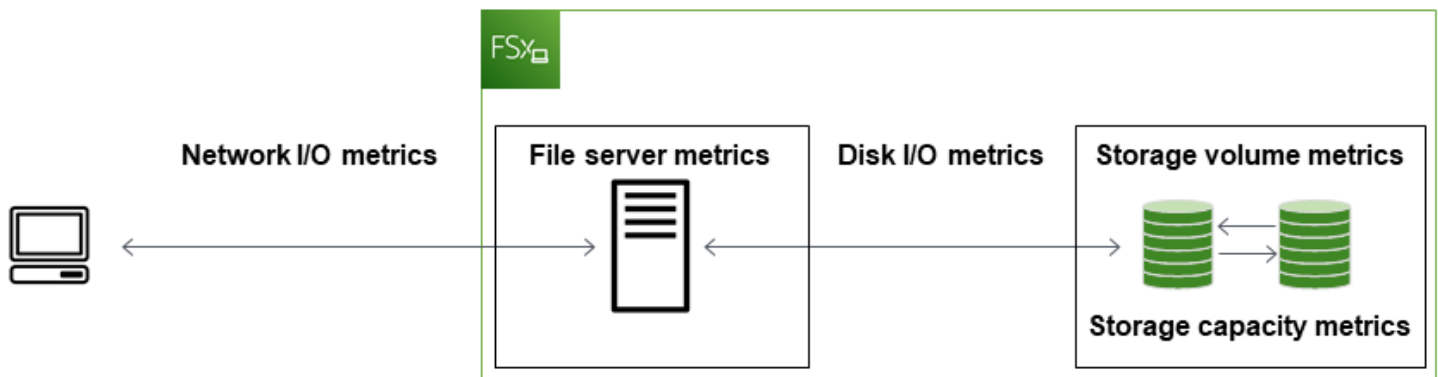
- [Come posso determinare il throughput e i limiti di IOPS per il mio file system?](#)
- [Qual è la differenza tra rete I/O e disco? I/O? Why is my network I/O different from my disk I/O](#)
- [Perché l'utilizzo della CPU o della memoria è elevato, anche quando la rete I/O è scarsa?](#)
- [Che cos'è lo scoppio? Quanta frammentazione viene utilizzata dal mio file system? Cosa succede quando i crediti burst si esauriscono?](#)
- [Nella pagina Monitoraggio e prestazioni viene visualizzato un avviso: devo modificare la configurazione del mio file system?](#)
- [Le mie metriche mancavano temporaneamente, devo preoccuparmi?](#)

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, fate riferimento alla [tabella che mostra i livelli di prestazioni](#) in base alla quantità di capacità di throughput di provisioning.

Qual è la differenza tra rete I/O e disco? I/O? Why is my network I/O different from my disk I/O

I FSx file system Amazon includono uno o più file server che forniscono dati in rete ai client che accedono al file system. Questa è la rete I/O. The file server has a fast, in-memory cache to enhance performance for the most frequently accessed data. The file servers also drives traffic to the storage volumes that host your file system data. This is the disk I/O. The following diagram illustrates network and disk I/O per un FSx file system Amazon.



Per ulteriori informazioni, consulta [Monitoraggio con Amazon CloudWatch](#).

Perché l'utilizzo della CPU o della memoria è elevato, anche quando la rete I/O è scarsa?

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 [Riduzione dei costi di storage con la 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 viene utilizzata dal mio file system? Cosa succede quando i crediti burst si esauriscono?

I carichi di lavoro basati su file sono in genere caratterizzati da picchi di attività brevi e intensi, I/O con tempi di inattività tra le interruzioni. 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 rete I/O che su disco. I/O

Amazon FSx utilizza un meccanismo I/O di credito per allocare la velocità effettiva e gli IOPS in base all'utilizzo medio: i file system accumulano crediti quando il loro throughput e l'utilizzo degli IOPS è inferiore 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 tuo file system, consulta [FSx per le prestazioni di 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 del disco e potenzialmente attivare avvisi I/O relativi alle prestazioni. 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 del disco. I/O 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 effettua FSx 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.

Amministrazione FSx per i file system Windows

Amazon FSx offre un'ampia gamma di funzionalità amministrative che ti aiutano a gestire e far crescere facilmente i tuoi file system Amazon FSx for Windows File Server per soddisfare i mutevoli requisiti dei carichi di lavoro e degli utenti e le esigenze normative e di conformità della tua organizzazione. Di seguito è riportato un elenco di alcune delle configurazioni del file system che puoi gestire utilizzando l'API Console di gestione AWS, l'Amazon FSx CLI per la gestione remota AWS CLI e le interfacce PowerShell grafiche native di Microsoft Windows Server.

- Capacità di archiviazione
- Storage Type (Tipo di storage)
- SSD IOPS
- Capacità effettiva di trasmissione
- Alias DNS
- Deduplicazione dei dati
- Copie shadow
- Quote di archiviazione
- Controllo dell'accesso ai file
- Condivisioni di file

Le seguenti sezioni forniscono informazioni sulle funzionalità e le impostazioni di amministrazione del file system disponibili. Abbiamo incluso delle linee guida per aiutarvi a determinare quali sono le opzioni migliori per la vostra situazione e le migliori pratiche, ove applicabili.

Argomenti

- [Stato FSx del file system Amazon](#)
- [Utilizzo dell'Amazon FSx CLI per PowerShell](#)
- [Avvio di una PowerShell sessione FSx remota Amazon](#)
- [Attività di configurazione del file system una tantum utilizzando l'Amazon FSx CLI per la gestione remota su PowerShell](#)
- [Risoluzione dei problemi di accesso all'Amazon FSx CLI su PowerShell](#)
- [Finestra di manutenzione del file system](#)

- [Modifica della finestra di manutenzione settimanale](#)
- [Gestione degli alias DNS](#)
- [Sessioni utente e file aperti](#)
- [File Server Resource Manager FSx attivo per Windows File Server](#)
- [Gestione dello storage FSx su Windows File Server](#)
- [Utilizzo dei namespace DFS](#)
- [Gestione della capacità di throughput](#)
- [Gestione del tipo di rete](#)
- [Taggare le tue risorse Amazon FSx](#)
- [Aggiornare un file system utilizzando AWS CLI](#)

Stato FSx del file system Amazon

Puoi visualizzare lo stato di un FSx file system Amazon utilizzando la FSx console Amazon, il AWS CLI comando [describe-file-systems](#) o l'operazione API [DescribeFileSystems](#).

Stato del file system	Description
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. II

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

Utilizzo dell'Amazon FSx CLI per PowerShell

Questo capitolo descrive come accedere all'Amazon FSx CLI per la gestione PowerShell remota per eseguire attività amministrative del file system FSx per i file system Windows. È inoltre possibile utilizzare l'interfaccia grafica utente (GUI) nativa di Microsoft Windows per eseguire alcune attività amministrative.

L'Amazon FSx CLI 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 tuo file system FSx per Windows File Server, devi prima soddisfare i seguenti prerequisiti:

- Essere in grado di connettersi a un'istanza di calcolo Windows con connettività di rete con il file system FSx per Windows File Server.
- Accedi all'istanza di calcolo di Windows come membro del gruppo di amministratori del file system. Se si utilizza AWS Managed Microsoft AD, si tratta del gruppo AWS FSxDelegated 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 consigliate per l'utilizzo di un Active Directory autogestito](#).

- Le regole in entrata del gruppo di sicurezza VPC del tuo file system consentono il traffico sulla porta 5985.

L'Amazon FSx CLI 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.

Hai due opzioni per eseguire i comandi CLI di gestione remota sul tuo FSx file system Amazon:

- 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'Amazon FSx CLI 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 per accedere al telecomando. PowerShell L'endpoint di amministrazione remota ha il formato, ad esempio `amznfsxctlyaa1k.ActiveDirectory-DNS-name`, di `amznfsxctlyaa1k.corp.example.com`. È possibile trovare il nome dell'endpoint utilizzando la Console di gestione AWS pagina dei dettagli del file system della scheda Rete e sicurezza. Usa il AWS CLI [describe-file-systems](#) comando per visualizzare la `RemoteAdministrationEndpoint` proprietà restituita nella risposta.

È possibile utilizzare il Get-Command cmdlet per recuperare informazioni sui cmdlet, le funzioni e gli alias disponibili in PowerShell. Per ulteriori informazioni, vedere la documentazione di Microsoft [Get-Command](#).

Puoi anche eseguire Amazon FSx CLI per la gestione remota della CLI 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 per Windows File Server, consulta [Avvio di una PowerShell sessione FSx remota Amazon](#)

Avvio di una PowerShell sessione FSx remota Amazon

In questo argomento vengono fornite istruzioni per avviare una PowerShell sessione remota di lunga durata sul file server FSx per Windows File Server.

Per avviare una PowerShell sessione remota sul file system

1. Connettiti a un'istanza di calcolo con connettività di rete con il tuo file system come utente membro del gruppo di FSx amministratori delegati che hai 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 FSx file system Amazon. 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. Inserisci le credenziali dell'utente che fa parte del gruppo Administrators. FSx Se la tua istanza è aggiunta al dominio, non ti verranno richieste le credenziali.

 Important

L' PowerShell endpoint Windows Remote potrebbe cambiare se si utilizza la configurazione di Active Directory autogestita e si modifica l'account del servizio senza le impostazioni appropriate dei criteri di gruppo di Active Directory. Per ulteriori informazioni, vedere [Modifica dell'account del FSx servizio Amazon](#) per ulteriori dettagli.

Attività di configurazione del file system una tantum utilizzando l'Amazon FSx CLI per la gestione remota su PowerShell

Utilizza la seguente Amazon FSx CLI for Remote Management sui PowerShell comandi per implementare rapidamente le attività di amministrazione del file system seguendo le nostre best practice.

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 [Riduzione dei costi di storage con la 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 [Gestione delle 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 applica 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, consultare [Gestione della crittografia in transito](#) e [Sessioni utente e file aperti](#).

Risoluzione dei problemi di accesso all'Amazon FSx CLI su 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, devi 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")
```

Finestra di manutenzione del file system

Amazon FSx for Windows File Server esegue patch software di routine per il software Microsoft Windows Server che gestisce. La finestra di manutenzione specifica il giorno della settimana e l'ora del giorno in cui inizia il processo di manutenzione. È possibile specificare il periodo di inizio della finestra di manutenzione durante la creazione del file system. Se non ne specificate uno, viene assegnata una finestra di inizio della manutenzione predefinita di 30 minuti. La durata della finestra di manutenzione dipende da diversi fattori, tra cui l'ambito della manutenzione e il processo di sincronizzazione di qualsiasi attività di lettura e scrittura dei file che si verifica durante la manutenzione tra i server primario e secondario per i file system Multi-AZ. Per ulteriori informazioni, consulta [Processo di failover](#).

FSx per Windows File Server consente di regolare l'ora di inizio della finestra di manutenzione per adattarla al carico di lavoro e ai requisiti operativi. È possibile spostare l'ora di inizio della finestra di manutenzione con la frequenza necessaria, a condizione che l'ora di inizio della finestra di manutenzione sia pianificata almeno una volta ogni 14 giorni. Se viene rilasciata una patch e non hai pianificato una finestra di manutenzione entro 14 giorni, FSx per Windows File Server procede alla manutenzione del file system per garantirne la sicurezza e l'affidabilità. Per ulteriori informazioni su come modificare l'ora di inizio della finestra di manutenzione del file system, consulta [Modifica della finestra di manutenzione settimanale](#).

Mentre è in corso l'applicazione delle patch, 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 eseguono automaticamente il failover e il failback tra il file server preferito e quello di standby. Per ulteriori informazioni, consulta [Processo di failover](#). Poiché l'applicazione delle patch per i file system Multi-AZ comporta il failover e il failback tra i file server, qualsiasi attività di lettura e scrittura dei file che si verifica durante questo periodo deve essere sincronizzata tra il file server preferito e quello di standby. Per ridurre i tempi di applicazione delle patch, 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.

Modifica della finestra di manutenzione settimanale

FSx per Windows File Server consente di modificare l'orario in cui inizia la finestra di manutenzione del file system in base al carico di lavoro e ai requisiti operativi. Puoi utilizzare l' FSx API Console di gestione AWS AWS CLI, e Amazon per modificare quando inizia la finestra di manutenzione settimanale, descritta nella procedura seguente.

Per modificare l'ora di inizio della finestra di manutenzione settimanale (console)

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Scegli File system nella colonna di navigazione a sinistra.
3. Scegli il file system per cui desideri modificare la finestra di manutenzione settimanale. Viene visualizzata la pagina dei dettagli del file system.
4. Scegliete Amministrazione per visualizzare il pannello Impostazioni di amministrazione del file system.
5. Scegliete Aggiorna per visualizzare la finestra Modifica manutenzione.
6. Inserisci il nuovo giorno e l'ora in cui desideri che inizi la finestra di manutenzione settimanale.
7. Scegli Salva per salvare le modifiche. La nuova ora di inizio della manutenzione viene visualizzata nel pannello Impostazioni di amministrazione.

Per modificare l'ora di inizio della finestra di manutenzione settimanale utilizzando il comando [update-file-system](#) CLI, vedere. [Aggiornare un file system utilizzando AWS CLI](#)

Gestione degli alias DNS

Oltre al nome DNS (Domain Name System) predefinito FSx fornito da Amazon, puoi anche associare alias DNS di tua scelta ai tuoi file system. 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 gli alias DNS a file system Windows File Server nuovi ed esistenti FSx e, quando ripristini un backup su un nuovo file system, utilizzando and. Console di gestione AWS AWS CLI È possibile associare fino a 50 alias DNS a un file system contemporaneamente.

Note

Il supporto per gli alias DNS è disponibile FSx per i file system 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 su un nuovo file system](#).

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 registra i record DNS per un file system FSx 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 FSx file system Amazon 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 le immissioni DNS manuali](#)

È possibile associare gli alias DNS ai file system esistenti FSx per Windows File Server, 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 dei servizi (SPNs) 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 [Accesso ai dati tramite alias DNS](#).

Un nome alias DNS per il tuo file system FSx per 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 memorizza i caratteri alfabetici come lettere minuscole (a-z), indipendentemente da come li specifichi: come lettere maiuscole, lettere minuscole o le lettere corrispondenti nei codici di escape.

Se provi ad associare un alias già associato al file system, 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 ricollegheranno automaticamente al file system. Tutti i file aperti dai client che mappavano una condivisione non-Continuously-Available (non CA) al momento della disconnessione devono essere riaperti dal client.

Argomenti

- [Stato dell'alias DNS](#)
- [Utilizzo di alias DNS con autenticazione Kerberos](#)

- [Visualizzazione degli alias DNS per file system e backup](#)
- [Associazione degli alias DNS ai file system](#)
- [Gestione degli alias DNS sui file system esistenti](#)

Stato dell'alias DNS

Gli alias DNS possono avere uno dei seguenti valori di stato:

- Disponibile: l'alias DNS è associato a un FSx file system Amazon.
- Creazione: Amazon FSx sta creando l'alias DNS e lo associa al file system.
- Eliminazione: Amazon FSx sta dissociando l'alias DNS dal file system e lo sta eliminando.
- Creazione non riuscita: Amazon non FSx è riuscito ad associare l'alias DNS al file system.
- Eliminazione non riuscita: Amazon non FSx è riuscita 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 tuo file system. Per abilitare l'autenticazione Kerberos per i client che accedono al tuo FSx file system Amazon utilizzando un alias DNS, devi configurare i nomi principali del servizio (SPNs) che corrispondono all'alias DNS sull'oggetto computer Active Directory del tuo file system.

Se avete SPNs configurato l'alias DNS assegnato a un altro file system su un oggetto computer in Active Directory, dovete prima rimuoverlo SPNs prima di aggiungerlo SPNs all'oggetto computer del vostro file system. Per ulteriori informazioni, consulta [Configura i nomi principali dei servizi \(SPNs\) per Kerberos](#).

Visualizzazione degli alias DNS per file system e backup

È possibile visualizzare gli alias DNS attualmente associati ai file system e FSx ai backup di Windows File Server utilizzando l'API Console di gestione AWS, the e AWS CLI, come descritto nelle procedure seguenti.

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

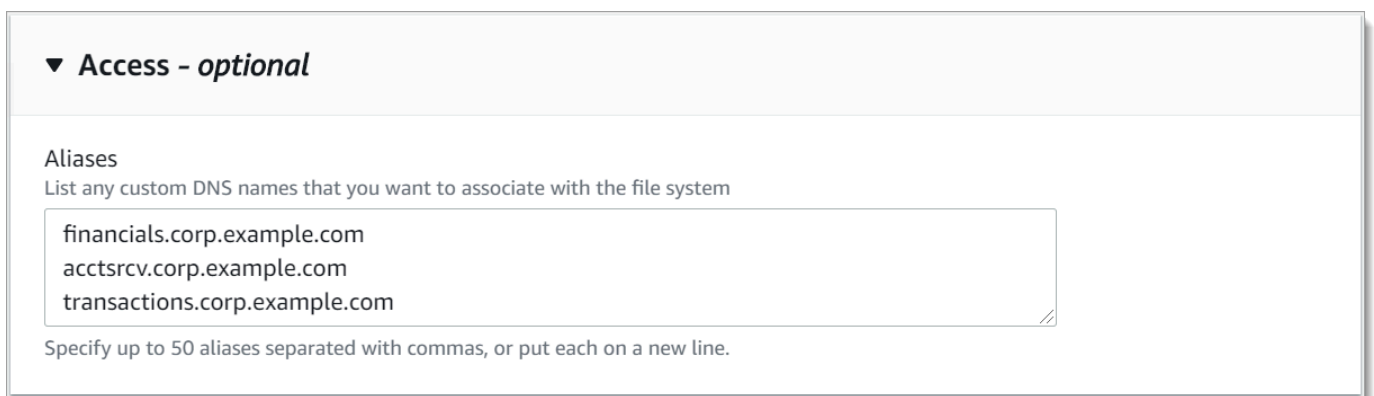
- Utilizzo della console: nel riquadro di navigazione, scegli Backup, quindi scegli il backup che desideri visualizzare. Nel riquadro Riepilogo, visualizza il campo Alias DNS.
- Utilizzo della CLI o dell'API: utilizza il comando `describe-backups` CLI o l'operazione API. [DescribeBackups](#)

Associazione degli alias DNS ai file system

È possibile associare gli alias DNS quando si crea da zero un nuovo file system FSx per Windows File Server o quando si ripristina un backup su un nuovo file system, utilizzando l'API, and Console di gestione AWS AWS CLI, descritta nelle seguenti procedure.

Per associare alias DNS durante la creazione di un nuovo file system (console)

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Segui la procedura per creare un nuovo file system descritta [Fase 5. 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.



▼ **Access - optional**

Aliases
List any custom DNS names that you want to associate with the file system

financials.corp.example.com
acctsrcv.corp.example.com
transactions.corp.example.com

Specify up to 50 aliases separated with commas, or put each on a new line.

4. Quando il file system è disponibile, è possibile accedervi utilizzando l'alias DNS configurando i nomi principali dei servizi (SPNs) e aggiornando o creando un record DNS CNAME per l'alias. Per ulteriori informazioni, consulta [Accesso ai dati tramite alias DNS](#).

Per associare alias DNS durante la creazione di un nuovo FSx file system Amazon (CLI)

1. Quando crei un nuovo file system, usa la proprietà [Alias](#) con l'operazione [CreateFileSystem](#) API 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 dei servizi (SPNs) e aggiornando o creando un record DNS CNAME per l'alias. Per ulteriori informazioni, consulta [Accesso ai dati tramite alias DNS](#).

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'[CreateFileSystemFromBackup](#) operazione 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 \  
  --aliases [alias1.corp.example.com,alias2.corp.example.com]
```

```
--windows-configuration Aliases=[transactions.corp.example.com,accts-rcv.corp.example.com]
```

- Quando il file system è disponibile, puoi accedervi utilizzando l'alias DNS configurando i nomi principali del servizio (SPNs) e aggiornando o creando un record DNS CNAME per l'alias. Per ulteriori informazioni, consulta [Accesso ai dati tramite alias DNS](#).

Gestione degli alias DNS sui file system esistenti

È possibile aggiungere e rimuovere alias su file system esistenti FSx per Windows File Server utilizzando Console di gestione AWS and AWS CLI, come descritto nelle procedure seguenti.

Per gestire gli alias DNS del file system (console)

- Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
- Passa a File system e scegli il file system Windows per cui desideri gestire gli alias DNS.
- Nella scheda Rete e sicurezza, scegli Gestisci alias DNS per visualizzare la finestra 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.

- Quando l'alias è disponibile, è possibile accedere al file system utilizzando l'alias DNS configurando i nomi principali dei servizi (SPNs) e aggiornando o creando un record DNS CNAME per l'alias. Per ulteriori informazioni, consulta [Accesso ai dati tramite alias DNS](#).

Per associare gli alias DNS ai file system esistenti (CLI)

- Utilizzate il comando `associate-file-system-aliases` CLI o l'operazione [AssociateFileSystemAliases](#) API 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 ([DescribeFileSystemAliases](#) è l'operazione API equivalente) per monitorare lo stato degli alias che stai associando.
3. Se `Lifecycle` ha il valore `AVAILABLE` (un processo che può richiedere fino a 2,5 minuti), è possibile accedere al file system utilizzando l'alias DNS configurando i nomi principali dei servizi (SPNs) e aggiornando o creando un record DNS CNAME per l'alias. Per ulteriori informazioni, consulta [Accesso ai dati tramite alias DNS](#).

Per dissociare gli alias DNS dai file system (CLI)

- Utilizzate il comando `disassociate-file-system-aliases` CLI o l'operazione [DisassociateFileSystemAliases](#) API 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 ([DescribeFileSystemAliases](#) è l'operazione API equivalente) per monitorare lo stato degli alias. L'eliminazione dell'alias richiede fino a 2,5 minuti.

Sessioni utente e file aperti

È possibile monitorare le sessioni utente connesse e aprire file sul FSx file system 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'Amazon FSx CLI per la gestione PowerShell remota per gestire le sessioni utente e aprire file sul tuo file system Windows File FSx Server.

Utilizzo della GUI per gestire utenti e sessioni

Le seguenti procedure descrivono in dettaglio come gestire le sessioni utente e aprire file sul FSx file system Amazon utilizzando lo strumento per le cartelle condivise di Microsoft Windows.

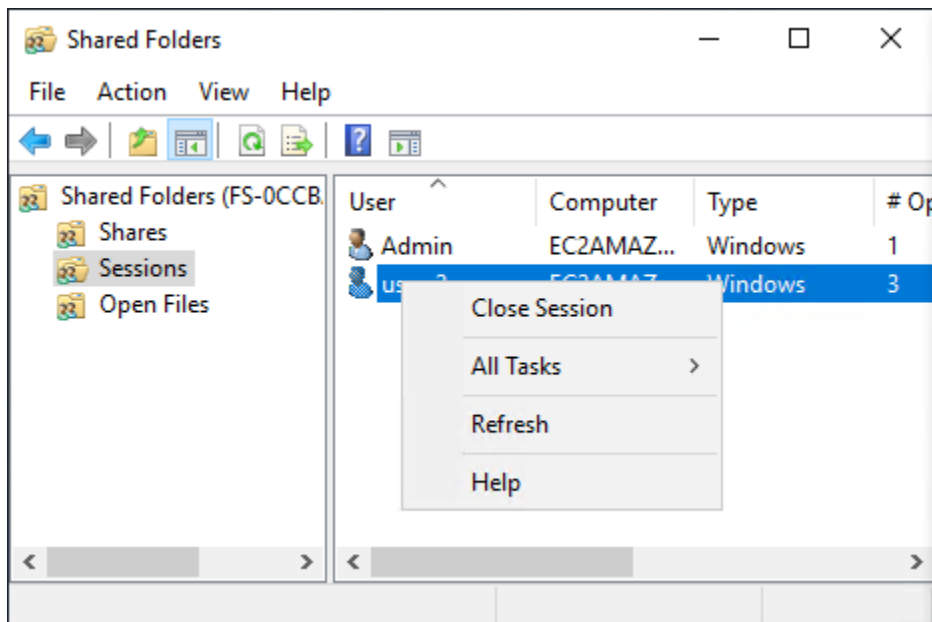
Per avviare lo strumento per le cartelle condivise

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

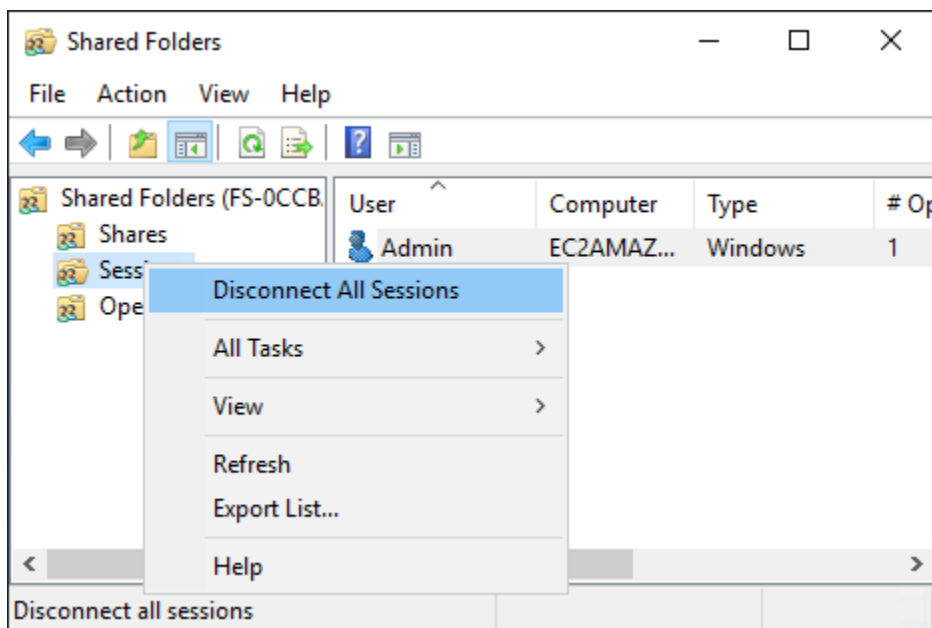
- [Unisciti senza problemi a un'istanza Windows EC2](#)
 - [Unisciti manualmente a un'istanza Windows](#)
2. Connect alla propria istanza come utente membro del gruppo di amministratori del file system. In AWS Managed Microsoft Active Directory, questo gruppo è denominato FSx Amministratori AWS delegati. 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 fs-*012345678901234567.ad-domain*.com il nome DNS del tuo FSx file system Amazon.
 6. Scegli OK. Viene quindi visualizzata una voce relativa al tuo FSx file system Amazon 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 FSx file system Amazon, questo snap-in mostra la sua sessione. Puoi disconnettere le sessioni aprendo il menu contestuale (fai clic con il pulsante destro del mouse) per una sessione e scegliendo Chiudi sessione.



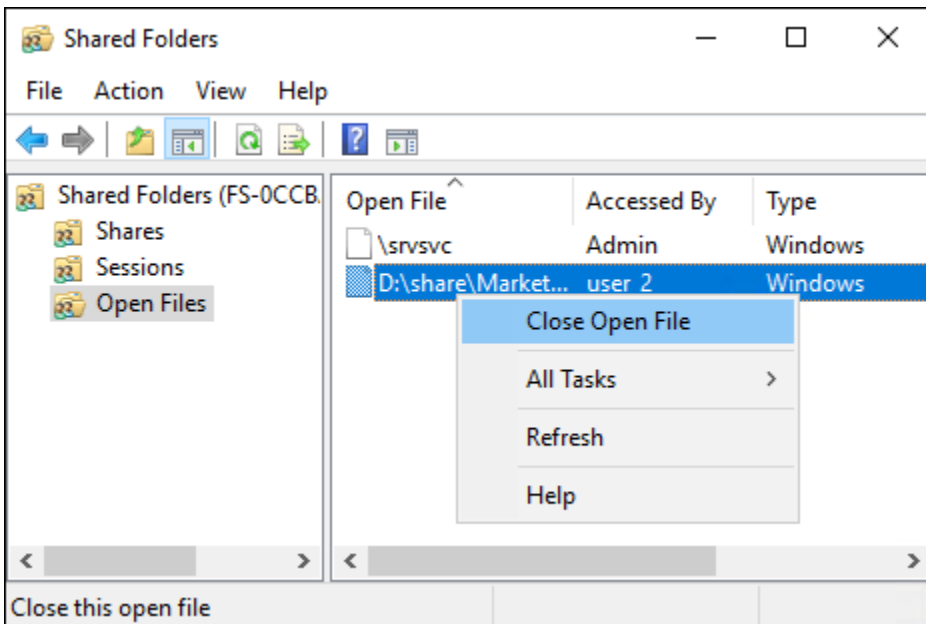
Per disconnettere tutte le sessioni aperte, apri il menu contestuale (fai clic con il pulsante destro del mouse) per Sessioni, scegli Disconnetti tutte le sessioni e conferma l'azione.



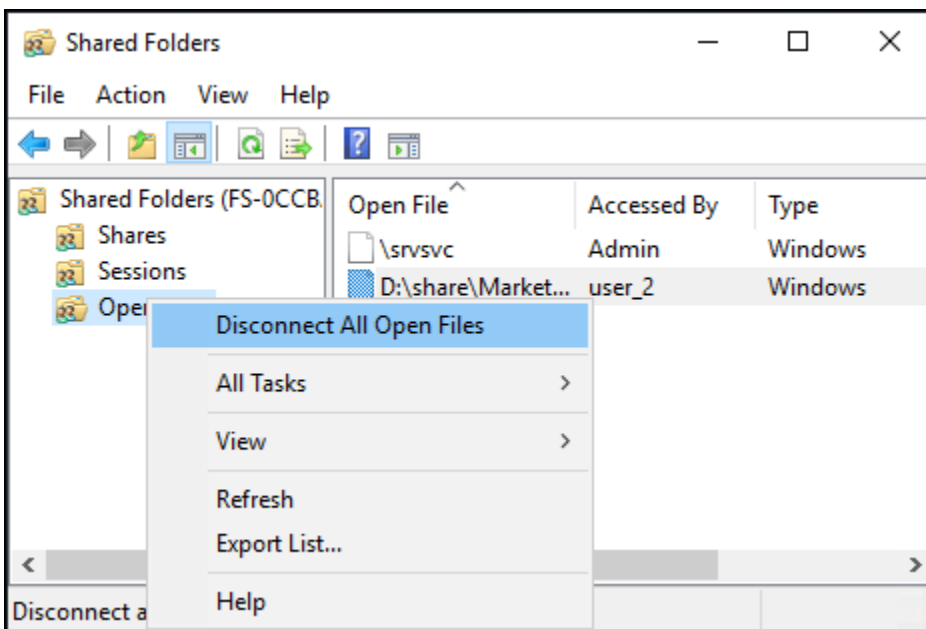
Per gestire i file aperti (GUI)

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'Amazon FSx CLI per PowerShell](#)

Di seguito sono riportati i comandi che è possibile utilizzare per la gestione delle sessioni utente e dei file aperti.

Comando	Description
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 esempio `Get-FSxSmbSession -?`.

File Server Resource Manager FSx attivo per Windows File Server

File Server Resource Manager (FSRM) è una funzionalità di Windows Server che ti aiuta a gestire e classificare i dati archiviati sul tuo file system Amazon FSx for Windows File Server. FSRM offre funzionalità automatizzate di applicazione delle policy e reportistica che consentono di controllare i costi di storage, mantenere la conformità alle politiche di gestione dei dati e organizzare i file in base alle regole aziendali.

Con FSRM, è possibile impostare limiti di archiviazione per impedire agli utenti di consumare uno spazio di archiviazione eccessivo, identificare e classificare automaticamente i dati sensibili, impedire il salvataggio di tipi di file non autorizzati nelle cartelle aziendali e generare report dettagliati sui modelli di utilizzo dello storage. Queste funzionalità consentono di mantenere un file system organizzato, efficiente e conforme senza richiedere l'intervento manuale per ogni file o cartella.

FSRM è particolarmente utile per le organizzazioni che devono:

- Controllate i costi di storage limitando la quantità di spazio su disco che gli utenti e i reparti possono archiviare
- Identifica dati sensibili come informazioni di identificazione personale o documenti finanziari

- Applica le politiche relative ai tipi di file consentiti in cartelle specifiche
- Genera report di conformità sulla conservazione dei dati, sulla proprietà dei file o sull'utilizzo dello storage
- Mantieni la visibilità su come viene utilizzato lo storage all'interno dell'organizzazione

Funzionalità chiave

- [Gestione delle quote](#)- Imposta limiti di archiviazione sulle cartelle per controllare la quantità di spazio che gli utenti e le applicazioni possono consumare. È possibile configurare quote rigide che impediscono agli utenti di superare i limiti o quote flessibili che consentono il superamento dei limiti durante l'invio delle notifiche. Le quote consentono di gestire i costi di archiviazione e impediscono agli utenti o ai reparti di consumare quantità sproporzionate di storage.
- [Screening dei file](#)- Controlla quali tipi di file gli utenti possono salvare in cartelle specifiche. È possibile bloccare tipi di file non autorizzati come file eseguibili, file multimediali o documenti personali nelle cartelle aziendali. Lo screening dei file consente di applicare le politiche di gestione dei dati, ridurre i rischi per la sicurezza e prevenire gli sprechi di archiviazione dovuti a file non aziendali.
- [Classificazione dei file](#)- Assegna automaticamente le proprietà dei metadati ai file in base al loro contenuto o alla loro posizione. La classificazione consente di organizzare i file, identificare i dati sensibili, applicare politiche di conservazione e generare report in base alle caratteristiche dei file. È possibile classificare i file in base alla sensibilità dei dati, al reparto, al periodo di conservazione o a qualsiasi altra proprietà personalizzata definita dall'utente.
- [Rapporti di archiviazione](#)- Genera report dettagliati sull'utilizzo del file system, inclusi file di grandi dimensioni, file duplicati, file per proprietario, file per tipo e utilizzo delle quote. I report sullo storage aiutano a capire come viene utilizzato lo storage, a identificare i file che possono essere archiviati o eliminati e a prendere decisioni informate sulla gestione dello storage.

Argomenti

- [Guida introduttiva a File Server Resource Manager](#)
- [Gestione delle quote](#)
- [Gruppi di file](#)
- [Screening dei file](#)
- [Classificazione dei file](#)

- [Rapporti di archiviazione](#)
- [Attività di gestione dei file](#)
- [Impostazioni FSRM](#)
- [Registri eventi](#)
- [Casi di utilizzo comune](#)

Guida introduttiva a File Server Resource Manager

Puoi abilitare File Server Resource Manager (FSRM) quando crei un nuovo file system Amazon FSx for Windows File Server oppure puoi aggiornare il file system esistente per abilitare FSRM.

FSRM è supportato solo sui file system Amazon FSx for Windows File Server con storage SSD e una capacità di throughput pari o superiore a 128. MB/s Puoi aggiornare il tipo di storage su SSD e modificare la capacità di throughput in qualsiasi momento dopo aver creato il file system. Per ulteriori informazioni, consultare [Aggiornamento del tipo di archiviazione di un file system FSx per Windows](#) e [Gestione della capacità di throughput](#).

Per abilitare FSRM durante la creazione di un file system (console)

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>
2. Nel pannello di controllo, scegli Crea file system per avviare la procedura guidata di creazione del file system.
3. Scegli Amazon FSx for Windows File Server, quindi scegli Avanti.
4. Seleziona l'opzione Standard Create
5. Fornisci le informazioni richieste
6. Apri il blocco File Server Resource Manager, scegli Enabled.
7. Per Destinazione del registro eventi, scegliete una delle seguenti opzioni:
 - CloudWatch Registri: selezionare un gruppo di CloudWatch registri per ricevere i registri degli eventi FSRM. Il nome del gruppo di CloudWatch log Logs deve iniziare con il prefisso. `' /aws/fsx/ '`
 - Kinesis Data Firehose: seleziona un flusso di distribuzione di Kinesis Data Firehose per ricevere i registri degli eventi FSRM
8. Completa le sezioni rimanenti e scegli Crea file system.

Per abilitare FSRM durante la creazione di un file system (CLI)

Per abilitare FSRM durante la creazione di un file system FSx per Windows File Server, utilizzate il comando CLI AWS `create-file-system`. Includete la seguente configurazione FSRM nel parametro: `--windows-configuration`

- `FsrmServiceEnabled`: imposta il valore su `true`
- `EventLogDestination`- L'Amazon Resource Name (ARN) che specifica la destinazione dei log degli eventi FSRM. Può essere un ARN del gruppo di log di CloudWatch Logs o un ARN del flusso di distribuzione di Kinesis Data Firehose.

```
aws fsx create-file-system \  
    --file-system-type WINDOWS \  
    --storage-capacity 300 \  
    --storage-type SSD \  
    --subnet-ids subnet-0123456789abcdef0 \  
    --windows-configuration  
    "ThroughputCapacity=128,WindowsFsrmConfiguration={FsrmServiceEnabled=true,EventLogDestination=  
east-1:123456789012:log-group:/aws/fsx/fsrm}"
```

Per modificare la configurazione FSRM su un file system esistente (console)

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Passa a File system e scegli il file system Windows che desideri modificare.
3. Scegli la scheda Amministrazione.
4. Nella sezione File Server Resource Manager, scegli Gestisci.
5. Apporta le modifiche richieste:
 - Per modificare la destinazione del registro degli eventi, selezionare un altro gruppo di log CloudWatch Logs o un flusso di distribuzione di Kinesis Data Firehose
 - Per abilitare FSRM, scegli Abilitato
 - Per disabilitare FSRM, scegliete Disabilitato

 Important

I file system Multi-AZ subiranno eventi automatici di failover e failback durante questo processo, mentre i file system Single-AZ subiranno un breve periodo di indisponibilità.

6. Scegli Save (Salva).

È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system, nella scheda Aggiornamenti.

Per modificare la configurazione FSRM su un file system esistente (CLI)

Per abilitare e disabilitare FSRM su un file system esistente FSx per Windows File Server, utilizzate il comando CLI AWS `update-file-system`

Attivazione di FSRM

Per abilitare FSRM, includi la seguente configurazione FSRM nel parametro: `--windows-configuration`

- `Fsrmserviceenabled`: imposta il valore su `true`
- `Eventlogdestination`- L'Amazon Resource Name (ARN) che specifica la destinazione dei log degli eventi FSRM. Può essere un ARN del gruppo di log di CloudWatch Logs o un ARN del flusso di distribuzione di Kinesis Data Firehose.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
  Fsrmserviceenabled=true,Eventlogdestination="arn:aws:logs:us-
east-1:123456789012:log-group:/aws/fsx/fsrm"
```

Disattivazione di FSRM

Per disabilitare FSRM:

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --windows-configuration Fsrmserviceenabled=false
```

 Important

I file system Multi-AZ subiranno eventi automatici di failover e failback durante questo processo, mentre i file system Single-AZ subiranno un breve periodo di indisponibilità.

FSx remoto PowerShell

Per configurare e utilizzare le funzionalità FSRM, devi utilizzare l'Amazon FSx CLI per la gestione remota su PowerShell. Per informazioni, consulta [Avvio di una PowerShell sessione FSx remota Amazon](#).

Gestione delle quote

È possibile utilizzare la gestione delle quote di File Server Resource Manager (FSRM) per controllare la quantità di spazio di archiviazione utilizzata dagli utenti sul file system FSx per Windows File Server. Le quote consentono di gestire la capacità di archiviazione limitando la quantità di dati che possono essere archiviati in cartelle specifiche e generando notifiche quando l'utilizzo dello storage si avvicina o supera le soglie definite.

Come funziona la gestione delle quote

La gestione delle quote offre due tipi di quote che è possibile applicare alle cartelle del file system:

Quote rigide

Impedisci agli utenti di salvare i file dopo il raggiungimento del limite di quota. Quando un utente tenta di salvare un file che supererebbe il limite di quota, l'operazione fallisce e l'utente riceve un messaggio di errore.

Quote flessibili

Consenti agli utenti di superare il limite di quota durante la registrazione della violazione. Le quote flessibili sono utili per monitorare l'utilizzo dello storage senza imporre limiti rigorosi.

Modelli di quote

I modelli di quote forniscono una configurazione riutilizzabile che definisce le impostazioni delle quote, inclusi i limiti di dimensione, il tipo di quota (rigido o flessibile) e le notifiche di soglia. Dopo

aver creato un modello di quote, puoi applicarlo a più cartelle senza dover riconfigurare ogni volta le stesse impostazioni. Quando aggiorni un modello di quote, puoi facoltativamente applicare le modifiche a tutte le quote create da quel modello.

L'utilizzo di modelli di quote offre diversi vantaggi:

- **Coerenza:** assicurati che cartelle simili abbiano configurazioni di quote identiche
- **Efficienza:** applica rapidamente le impostazioni delle quote a più cartelle
- **Manutenibilità:** aggiorna le impostazioni delle quote su più cartelle modificando il modello

Applica automaticamente le quote

Applica automaticamente le quote crea automaticamente le quote per le sottocartelle in base a un modello specificato. Quando si crea una quota di applicazione automatica su una cartella principale, FSRM genera automaticamente una quota per ogni sottocartella esistente e per tutte le nuove sottocartelle che gli utenti creeranno in futuro. Questo approccio è utile per gli scenari in cui si desidera applicare limiti di quota coerenti su più directory utente o cartelle dipartimentali.

Notifiche di soglia

Le soglie definiscono i livelli di utilizzo ai quali FSRM intraprende azioni specifiche. È possibile configurare più soglie per ogni quota, con ogni soglia impostata su una percentuale del limite di quota. Quando l'utilizzo dello storage raggiunge una percentuale di soglia, FSRM può eseguire le seguenti azioni:

Registrazione degli eventi

Registra un evento su Amazon CloudWatch o Amazon Kinesis Data Firehose per il monitoraggio e l'analisi. Puoi specificare il livello di gravità dell'evento (informazione, avviso o errore) e fornire un corpo del messaggio personalizzato. La registrazione degli eventi è utile per monitorare l'utilizzo delle quote e l'integrazione con i sistemi di monitoraggio esistenti.

Rapporti di archiviazione

Genera un rapporto sull'utilizzo dello storage che fornisca informazioni dettagliate sui file e le cartelle che occupano spazio di archiviazione. I report sullo storage consentono di identificare gli utenti o le applicazioni che utilizzano la maggior parte dello storage e di prendere decisioni informate sulla gestione dello storage. Per ulteriori informazioni, consulta [Rapporti di archiviazione](#).

È possibile configurare più soglie con azioni diverse per ogni quota. Ad esempio, è possibile configurare una quota con un evento informativo al 75% di utilizzo e un evento di avviso al 90% di utilizzo.

Comandi di gestione delle quote

È possibile accedere a tre famiglie di PowerShell comandi FSx remoti per la gestione delle quote:

1. Comandi di quota: crea, recupera, modifica, rimuovi e aggiorna le quote su cartelle specifiche. Utilizzate questi comandi quando è necessario gestire le quote su base individuale. folder-by-folder
2. Comandi del modello di quota: crea, recupera e modifica i modelli di quote che definiscono configurazioni di quote riutilizzabili. Utilizzate questi comandi per stabilire politiche di quota standard da applicare su più cartelle.
3. Comandi Quota automatica: crea, recupera, modifica, rimuovi e aggiorna le quote di applicazione automatica che generano automaticamente quote per le sottocartelle. Utilizzate questi comandi quando è necessario applicare limiti di quota coerenti su più sottocartelle senza creare manualmente quote individuali.

Elenco di comandi remoti di Quote Management FSx PowerShell

Note

Tutti gli esempi in questa pagina presuppongono che la `$FSxWindowsRemotePowerShellEndpoint` variabile sia stata definita con l' endpoint Windows Remote del file system. Puoi trovare questo endpoint nella FSx console Amazon nella pagina dei dettagli del tuo file system o utilizzando il AWS CLI `describe-file-systems` comando.

Comandi Quota

Nuovo- FSx FSRMQuota

Crea una nuova quota su una cartella. Una quota limita la quantità di dati che gli utenti possono archiviare in una cartella. Facoltativamente, puoi configurare la quota per generare notifiche quando gli utenti superano le soglie di quota.

Parametri:

- **Folder (string)**- Obbligatorio. Il percorso della cartella in cui verrà applicata la quota.
- **Size (string)**- Obbligatorio quando non si utilizza un modello: il limite di dimensione della quota.
- **Template (string)**- Facoltativo. Il nome di un modello di quote esistente da utilizzare. Quando si specifica un modello, è possibile utilizzare solo il parametro **Description**; tutte le altre impostazioni vengono ereditate dal modello.
- **Description (string)**- Facoltativo. Una descrizione della quota.
- **SoftLimit (boolean)**- Facoltativo. Se impostato su **true**, crea una quota flessibile che consente agli utenti di superare il limite durante la registrazione delle violazioni.
- **Disabled (boolean)**- Facoltativo. Se impostato su **true**, crea la quota in uno stato disabilitato.
- **ThresholdConfigurations (array)**- Facoltativo. Una serie di configurazioni di soglia che specificano le azioni da intraprendere a diversi livelli di utilizzo. Ogni configurazione ha le seguenti proprietà:
 - **ThresholdPercentage (number)**: La percentuale del limite di quota entro la quale attivare le azioni. Immettere un valore compreso tra 0 e 250.
 - **Action (array)**: Una o più azioni da intraprendere quando viene raggiunta la soglia. Ogni azione ha le seguenti proprietà:
 - **ActionType**: il tipo di azione da eseguire. Puoi specificare le seguenti valori:
 1. **Event**: registra un evento nel registro eventi del file system. Quando si specifica **Event**, è necessario specificare anche le seguenti proprietà:
 - **EventType**: Informazioni, avviso o errore
 - **MessageBody**: il testo del messaggio da registrare con l'evento.
 2. **Report**: genera un rapporto sull'utilizzo dello storage.

Esempi:

1. Crea una quota fissa di 5 GB senza utilizzare un modello di quote.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMQuota -Folder "share\test" -Size 5GB
}
```

2. Crea una quota flessibile con una notifica di soglia

```
$thresholds = [System.Collections.ArrayList]@()
$warning = @{
    ThresholdPercentage = 75
    Action = @(
        @{
            ActionType = "Event"
            EventType = "Warning"
            MessageBody = "Quota usage has reached 75%"
        }
    )
}

$thresholds.Add($warning)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
    FSxRemoteAdmin -ArgumentList ($thresholds) -ScriptBlock {
    param($thresholds)
    New-FSxFSRMQuota -Folder "share/test" -Size 1GB -Description "Test quota" -
    SoftLimit -ThresholdConfigurations $Using:thresholds
}
```

Ottieni- FSx FSRMQuota

Recupera una o più quote dal file system. Il comando restituisce dettagli sulle configurazioni delle quote, inclusi i limiti di dimensione, le soglie e l'utilizzo corrente.

Parametri:

- **Folder (string)**- Facoltativo. Il percorso della cartella da cui recuperare le quote. Se non si specifica il percorso della cartella, il comando restituisce tutte le quote sul file system.

Esempi:

1. Ottieni tutte le quote esistenti nel file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
    FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMQuota
}
```

Rimuovi- FSx FSRMQuota

Rimuove una quota da una cartella specificata del file system.

Parametri:

- **Folder (string)**- Obbligatorio. Il percorso della cartella da cui rimuovere la quota.
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto quota rimosso.

Esempi:

1. Rimuove una quota.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Remove-FSxFSRMQuota -Folder "share\test" -PassThru  
}
```

Impostare- FSx FSRMQuota

Modifica la configurazione di una quota esistente.

Parametri:

- **Folder (string)**- Obbligatorio. Il percorso della cartella che contiene la quota da modificare.
- **Description (string)**- Facoltativo. Una nuova descrizione per la quota.
- **Size (string)**- Facoltativo. Il nuovo limite di dimensione per la quota.
- **SoftLimit (boolean)**- Facoltativo. Se impostato su true, modifica la quota impostandola su un limite flessibile, che consente agli utenti di superare il limite durante la registrazione delle violazioni.
- **Disabled (boolean)**- Facoltativo. Se impostato su true, disabilita la quota. Se impostato su false, abilita la quota.
- **ThresholdConfigurations (array)**- Facoltativo. Una serie di nuove configurazioni di soglia. Ogni configurazione di soglia ha le seguenti proprietà:
 - **ThresholdPercentage (number)**: La percentuale del limite di quota entro la quale attivare le azioni. Immettere un valore compreso tra 0 e 250.
 - **Action (array)**: Una o più azioni da intraprendere quando viene raggiunta la soglia. Ogni azione ha le seguenti proprietà:

- **ActionType**: il tipo di azione da eseguire. Puoi specificare le seguenti valori:
 1. **Event**: registra un evento nel registro eventi del file system. Quando si specifica Event, è necessario specificare anche le seguenti proprietà:
 - **EventType**: Informazioni, avviso o errore
 - **MessageBody**: il testo del messaggio da registrare con l'evento.
 2. **Report**: genera un rapporto sull'utilizzo dello storage.
- **PassThru** (boolean)- Facoltativo. Se impostato su true, restituisce l'oggetto quota modificato.

Esempi:

1. Modifica la dimensione e la descrizione della quota.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuota -Folder "share\department" -Size 2GB -Description "Updated
quota for department share"
}
```

2. Disattiva una quota

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuota -Folder "share\department" -Disabled: $true
}
```

Aggiornamento- FSx FSRMQuota

Ricalcola le statistiche di utilizzo correnti per una quota scansionando la cartella per determinare la quantità effettiva di spazio utilizzato.

Parametri:

- **Folder** (string)- Obbligatorio. Il percorso della cartella che contiene la quota da aggiornare.
- **PassThru** (boolean)- Facoltativo. Se impostato su true, restituisce l'oggetto quota aggiornato.

Esempi:

1. Ricalcola le statistiche di utilizzo correnti per una quota specificata.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Update-FSxFSRMQuota -Folder "share\department" -PassThru  
}
```

Comandi del modello di quota

Nuovo- FSx FSRMQuota Modello

Crea un nuovo modello di quote che definisce una configurazione riutilizzabile per le quote.

Parametri:

- **Name (string)**- Obbligatorio. Un nome per il modello di quota.
- **Size (string)**- Obbligatorio. Il limite di dimensione applicato dal modello di quote.
- **Description (string)**- Facoltativo. Una descrizione del modello di quota.
- **SoftLimit (boolean)**- Facoltativo. Se impostato su true, crea un modello per le quote flessibili che segnalano l'utilizzo ma non applicano il limite.
- **ThresholdConfigurations (array)**- Facoltativo. Una serie di configurazioni di soglia che specificano le azioni da intraprendere a diversi livelli di utilizzo. Ogni configurazione ha le seguenti proprietà:
 - **ThresholdPercentage (number)**: La percentuale del limite di quota entro la quale attivare le azioni. Immettere un valore compreso tra 0 e 250.
 - **Action (array)**: Una o più azioni da intraprendere quando viene raggiunta la soglia. Ogni azione ha le seguenti proprietà:
 - **ActionType**: il tipo di azione da eseguire. Puoi specificare le seguenti valori:
 1. **Event**: registra un evento nel registro eventi del file system. Quando si specifica Event, è necessario specificare anche le seguenti proprietà:
 - **EventType**: Informazioni, avviso o errore
 - **MessageBody**: il testo del messaggio da registrare con l'evento.
 2. **Report**: genera un rapporto sull'utilizzo dello storage.

Esempi:

1. Crea un modello rigido con limite di 1 GB.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMQuotaTemplate -Name "1GB Hard Limit" -Size 1GB -Description "Standard
1GB hard limit template"
}
```

2. Crea un modello soft limit da 5 GB con una soglia di avviso al 90% di utilizzo

```
$threshold = @{
    ThresholdPercentage = 90
    Action = @(
        @{
            ActionType = "Event"
            EventType = "Warning"
            MessageBody = "Quota usage has reached 90% of the limit"
        }
    )
}

$thresholds = [System.Collections.ArrayList]@()
$thresholds.Add($threshold)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $thresholds -ScriptBlock {
    param($thresholds)

    New-FSxFSRMQuotaTemplate -Name "5GB Soft Limit" -Size 5GB -Description "5GB soft
limit with 90% warning" -SoftLimit -ThresholdConfigurations $Using:thresholds
}
```

Get- FSx FSRMQuota Template

Recupera uno o più modelli di quote dal file system.

Parametri:

- **Name (string)**- Facoltativo. Il nome di un modello di quote specifico da recuperare. Se non si specifica un nome, il comando restituisce tutti i modelli di quote.

Esempi:

1. Recupera tutti i modelli di quote sul file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMQuotaTemplate  
}
```

Set- Modello FSx FSRMQuota

Modifica le proprietà di un modello di quote.

Parametri:

- **Name (string)**- Obbligatorio. Il nome del modello di quota da modificare.
- **Description (string)**- Facoltativo. Una nuova descrizione per il modello.
- **Size (string)**- Facoltativo. Il nuovo limite di dimensione per il modello.
- **SoftLimit (boolean)**- Facoltativo. Se impostato su true, modifica il modello per creare quote flessibili che segnalano l'utilizzo ma non applicano il limite.
- **ThresholdConfigurations (array)**- Facoltativo. Una serie di configurazioni di soglia che specificano le azioni da intraprendere a diversi livelli di utilizzo. Ogni configurazione ha le seguenti proprietà:
 - **ThresholdPercentage (number)**: La percentuale del limite di quota entro la quale attivare le azioni. Immettere un valore compreso tra 0 e 250.
 - **Action (array)**: Una o più azioni da intraprendere quando viene raggiunta la soglia. Ogni azione ha le seguenti proprietà:
 - **ActionType**: il tipo di azione da eseguire. Puoi specificare le seguenti valori:
 1. **Event**: registra un evento nel registro eventi del file system. Quando si specifica Event, è necessario specificare anche le seguenti proprietà:
 - **EventType**: Informazioni, avviso o errore
 - **MessageBody**: il testo del messaggio da registrare con l'evento.
 2. **Report**: genera un rapporto sull'utilizzo dello storage.
- **UpdateDerived (boolean)**- Facoltativo. Se impostato su true, aggiorna tutte le quote create da questo modello.
- **UpdateDerivedMatching (boolean)**- Facoltativo. Se impostato su true, aggiorna solo le quote create da questo modello e che non sono state modificate dalla creazione.
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto modello modificato.

Esempi:

1. Modifica le dimensioni e la descrizione di un modello di quote.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuotaTemplate -Name "5GB Soft Limit" -Size 10GB -Description "Updated to
10GB soft limit"
}
```

2. Modifica un modello di quote e aggiorna tutte le quote create dal modello.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    Set-FSxFSRMQuotaTemplate -Name "1GB Hard Limit" -Size 2GB -UpdateDerived
}
```

Reimposta- FSx FSRMQuota

Reimposta una quota in modo che corrisponda alle impostazioni di un modello specificato.

Parameters

- **Folder (string)**- Obbligatorio. Il percorso della cartella che contiene la quota da reimpostare.
- **Template (string)**- Obbligatorio. Il nome del modello di quota da applicare.

Esempi

Esempi: reimpostare una quota in modo che corrisponda alle impostazioni definite in un modello di quote.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    Reset-FSxFSRMQuota -Folder "share\department" -Template "1GB Hard Limit"
}
```

Comandi di quota automatica

Nuova - FSx FSRMAuto Quota

Il New-FSxFSRMAutoQuota comando crea una quota di applicazione automatica su una cartella specificata. Una quota ad applicazione automatica genera automaticamente quote basate sul

modello specificato per ogni sottocartella esistente e per tutte le nuove sottocartelle create nella cartella specificata.

Parameters

- **Folder (string)**- Obbligatorio. Il percorso della cartella in cui verrà creata la quota di applicazione automatica.
- **Template (string)**- Facoltativo. Il nome di un modello di quote esistente da utilizzare per l'applicazione automatica della quota.
- **Disabled (boolean)**- Facoltativo. Se impostato su true, crea la quota di applicazione automatica in uno stato disabilitato.

Esempi

1. Crea una quota di applicazione automatica che applica automaticamente un modello specificato a tutte le sottocartelle.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    New-FSxFSRMAutoQuota -Folder "share\department" -Template "250 MB Extended Limit"  
}
```

Ottieni- Quota FSx FSRMAuto

Il `Get-FSxFSRMAutoQuota` comando recupera una o più quote di applicazione automatica dal file system.

Parameters

- **Folder (string)**- Facoltativo. Il percorso della cartella da cui recuperare le quote di applicazione automatica. È inoltre possibile utilizzare `...` alla fine del percorso per includere tutte le sottocartelle.

Se non si specifica un percorso di cartella, il comando restituisce tutte le quote di applicazione automatica sul file system.

Esempi

1. Recupera tutte le quote di applicazione automatica sul file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMAutoQuota  
}
```

Rimuovi- Quota FSx FSRMAuto

Il `Remove-FSxFSRMAutoQuota` comando rimuove una quota applicata automaticamente da una cartella specificata. Quando si rimuove una quota applicata automaticamente, il comando rimuove anche tutte le quote dalle sottocartelle derivate dal modello di quota associato.

Parameters

- `Folder (string)`- Obbligatorio. Il percorso della cartella da cui rimuovere la quota di applicazione automatica.
- `PassThru (boolean)`- Facoltativo. Se impostato su `true`, restituisce l'oggetto quota ad applicazione automatica rimosso.

Esempi

1. Rimuovi una quota applicata automaticamente da una cartella specifica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Remove-FSxFSRMAutoQuota -Folder "share\department" -PassThru  
}
```

Imposta- FSx FSRMAuto Quota

Il `Set-FSxFSRMAutoQuota` comando modifica le impostazioni di configurazione di una quota di applicazione automatica.

Parameters

- `Folder (string)`- Obbligatorio. Il percorso della cartella che contiene la quota di applicazione automatica da modificare.
- `Template (string)`- Facoltativo. Il nome di un modello di quota da applicare.
- `Disabled (boolean)`- Facoltativo. Se impostato su `true`, disabilita la quota di applicazione automatica. Se impostato su `false`, abilita la quota di applicazione automatica.

- **UpdateDerived** (boolean)- Facoltativo. Se impostato su true, aggiorna tutte le quote esistenti derivate da questa quota ad applicazione automatica.
- **UpdateDerivedMatching** (boolean)- Facoltativo. Se impostato su true, aggiorna solo le quote derivate che non sono state modificate dalla creazione.
- **PassThru** (boolean)- Facoltativo. Se impostato su true, restituisce l'oggetto quota modificato per l'applicazione automatica.

Esempi

1. Modifica il modello di quota utilizzato da una quota ad applicazione automatica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Set-FSxFSRMAutoQuota -Folder "share\department" -Template "100 MB Limit"  
}
```

2. Disattiva una quota ad applicazione automatica e aggiorna tutte le quote che ne sono derivate.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Set-FSxFSRMAutoQuota -Folder "share\department" -Disabled: $true -UpdateDerived  
}
```

Aggiorna - Quota FSx FSRMAuto

Il `Update-FSxFSRMAutoQuota` comando ricalcola le proprietà di una quota di applicazione automatica e le quote che ne derivano eseguendo la scansione della cartella per determinare la quantità effettiva di spazio utilizzata.

Parameters

- **Folder** (string)- Obbligatorio. Il percorso della cartella che contiene la quota di applicazione automatica da aggiornare.
- **PassThru** (boolean)- Facoltativo. Se impostato su true, restituisce l'oggetto quota aggiornato per l'applicazione automatica.

Esempi

1. Ricalcola le statistiche di utilizzo e restituisci l'oggetto quota ad applicazione automatica aggiornato.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Update-FSxFSRMAutoQuota -Folder "share\department" -PassThru  
}
```

Gruppi di file

I gruppi di file definiscono raccolte logiche di modelli di nomi di file che è necessario utilizzare durante la configurazione delle [schermate dei file](#) e che è possibile utilizzare facoltativamente per generare report di [archiviazione](#). Un gruppo di file contiene modelli di inclusione (file da abbinare) e modelli di esclusione (file da escludere dalle corrispondenze), a cui si fa riferimento tramite il nome del gruppo di file anziché specificare ogni volta modelli singoli.

Come vengono utilizzati i gruppi di file

I gruppi di file sono necessari per le seguenti funzionalità FSRM:

- Schermate dei file: è necessario specificare uno o più gruppi di file per definire quali tipi di file bloccare o monitorare.
- Eccezioni relative alla schermata dei file: è necessario specificare uno o più gruppi di file per definire quali tipi di file consentire nonostante il blocco delle schermate dei file nelle cartelle principali.
- Modelli di schermate dei file: è necessario specificare uno o più gruppi di file per definire quali tipi di file verranno bloccati o monitorati dal modello.

I gruppi di file sono opzionali per le seguenti funzionalità FSRM:

- Report di archiviazione: è possibile filtrare facoltativamente i report per gruppo di file per analizzare l'utilizzo dello storage per tipi di file specifici. Ad esempio, puoi generare un rapporto che mostri solo file audio e video.

Schemi dei nomi dei file

I gruppi di file utilizzano i caratteri jolly per abbinare i nomi dei file. È possibile specificare sia modelli di inclusione (file da abbinare) che modelli di esclusione (file da escludere dalle corrispondenze).

FSRM supporta i seguenti caratteri jolly:

- Asterisco (*): corrisponde a zero o più caratteri
- Punto interrogativo (?) - Corrisponde esattamente a un carattere

Ad esempio, il modello *.doc* corrisponde a file comereport.doc, e report.docxdocument.doc, mentre il modello di ~\$* esclusione esclude i file temporanei creati dalle applicazioni di Microsoft Office.

Gruppi di file predefiniti

Quando si abilita FSRM sul file system, vengono creati automaticamente i seguenti gruppi di file:

File audio e video

Corrisponde ai formati di file audio e video più comuni *.mp3, tra cui *.wav*.avi,*.mp4,*.mpeg,, e *.wmv

File di backup

Corrisponde ai formati di file di backup tra cui *.bak*.backup, e *.old

File compressi

Corrisponde ai formati di file di archivio e compressi *.zip, tra cui, *.rar,*.7z, e *.gz *.tar

File di posta elettronica

Corrisponde ai formati dei messaggi di posta elettronica e delle caselle di posta *.eml, tra cui *.msg, e *.pst

File eseguibili

Corrisponde ai formati di file eseguibili e di script *.exe *.dll, tra cui *.com,*.bat,*.cmd,, e *.vbs

File di immagine

Corrisponde ai formati di file di immagine più comuni tra cui *.jpg *.jpeg*.png,*.gif,*.bmp,, e *.tif

File di Office

Corrisponde ai formati di documenti di Microsoft Office tra cui *.doc
.docx.xls,*.xlsx,*.ppt, e *.pptx

File di sistema

Corrisponde ai formati di file di sistema Windows*.sys, tra cui *.dll*.ocx,, e *.drv

File temporanei

Corrisponde ai formati di file temporanei tra cui *.tmp*.temp, e ~*

File di testo

Corrisponde ai formati di file basati su testo*.txt, tra cui,*.log, e *.csv *.xml

File di pagine Web

Corrisponde ai formati di file di contenuto Web tra cui *.html *.htm*.asp,*.aspx,,*.php, e
*.js

È possibile utilizzare questi gruppi di file predefiniti immediatamente nelle schermate dei file e nei report di archiviazione oppure modificarli in base a requisiti specifici.

Comandi di gestione dei gruppi di file

FSRM fornisce PowerShell comandi per la creazione e la gestione di gruppi di file. Utilizzate questi comandi per definire gruppi di file personalizzati che corrispondano alle politiche di gestione dei file dell'organizzazione.

Note

Tutti gli esempi in questa pagina presuppongono che la `$FSxWindowsRemotePowerShellEndpoint` variabile sia stata definita con l' PowerShell endpoint Windows Remote del file system. Puoi trovare questo endpoint nella AWS FSx console nella pagina dei dettagli del tuo file system o utilizzando il comando `AWS describe-file-systems CLI`.

Nuovo- Gruppo FSx FSRMFile

Crea un gruppo di file che definisce una raccolta logica di modelli di nomi di file. Questi modelli possono essere utilizzati per schermate di file, eccezioni di schermate di file e report di archiviazione.

Parametri:

- **Name (string)**- Richiesto. Un nome per il gruppo di file.
- **Description (string)**- Facoltativo. Una descrizione per il gruppo di file.
- **IncludePattern (array)**- Facoltativo. Una serie di stringhe di pattern che specificano i file da includere.
- **ExcludePattern (array)**- Facoltativo. Una matrice di stringhe di pattern che specificano i file da escludere.

Esempi:

1. Crea un gruppo di file per file di testo.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    New-FSxFSRMFileGroup -Name "My Text Files" -IncludePattern "*.txt"  
}
```

2. Crea un gruppo di file per il codice sorgente con modelli di inclusione ed esclusione.

```
$includePatterns = @("*.cpp", "*.h", "*.cs", "*.py")  
$excludePatterns = @("*.tmp", "*.bak")  
  
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ArgumentList @($includePatterns, $excludePatterns) -ScriptBlock {  
    param($includePatterns, $excludePatterns)  
    New-FSxFSRMFileGroup -Name "Source Code" -Description "Programming source files"  
    -IncludePattern $includePatterns -ExcludePattern $excludePatterns  
}
```

Get- FSx FSRMFile Group

Recupera uno o più gruppi di file dal file system. I gruppi di file definiscono raccolte di modelli di file utilizzati per lo screening e il reporting dei file.

Parametri:

- **Name (array)**- Facoltativo. Una matrice di nomi di gruppi di file da recuperare. Se non si specifica un nome, il comando restituisce tutti i gruppi di file sul file system.

Esempi:

1. Recupera tutti i gruppi di file sul file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMFileGroup  
}
```

Rimuovi- Raggruppa FSx FSRMFile

Rimuove uno o più gruppi di file dal file system. Dopo la rimozione, il gruppo di file non può essere utilizzato nelle schermate dei file o nelle eccezioni delle schermate dei file.

Parametri:

- **Name (array)**- Richiesto. Un array di nomi di gruppi di file da rimuovere.
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto del gruppo di file rimosso.

Esempi:

1. Rimuove un singolo gruppo di file.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Remove-FSxFSRMFileGroup -Name "My Text Files" -PassThru  
}
```

Set- FSx FSRMFile Group

Modifica le proprietà dei gruppi di file esistenti.

Parametri:

- **Name (array)**- Obbligatorio. Una matrice di nomi di gruppi di file da modificare.
- **Description (string)**- Facoltativo. Una nuova descrizione per il gruppo di file.
- **IncludePattern (array)**- Facoltativo. Una nuova matrice di stringhe di pattern che specificano i file da includere.
- **ExcludePattern (array)**- Facoltativo. Una nuova matrice di stringhe di pattern che specificano i file da escludere.
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto del gruppo di file modificato.

Esempi:

1. Aggiorna la descrizione e i modelli per un gruppo di file.

```
$includePatterns = @("*.docx", "*.pdf", "*.rtf")  
$excludePatterns = @("~$*", "*.tmp")
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ArgumentList @($includePatterns, $excludePatterns) -ScriptBlock {  
    param($includePatterns, $excludePatterns)  
    Set-FSxFSRMFileGroup -Name "Documents" -Description "Updated document types" -  
    IncludePattern $includePatterns -ExcludePattern $excludePatterns -PassThru  
}
```

Screening dei file

Lo screening dei file controlla quali tipi di file gli utenti possono salvare nelle cartelle del file system. Lo screening dei file consente di applicare le politiche di archiviazione, prevenire tipi di file non autorizzati e mantenere la conformità ai requisiti organizzativi.

Note

Le schermate dei file utilizzano gruppi di file per definire quali tipi di file bloccare o monitorare. Per ulteriori informazioni sulla creazione e la gestione di gruppi di file, vedere [Gruppi di file](#).

FSRM supporta due tipi di schermate di file:

1. Schermate di file attive: impediscono agli utenti di salvare i file che corrispondono ai gruppi di file specificati e generano notifiche quando gli utenti tentano di salvare i file bloccati. Utilizzate le schermate di file attive quando è necessario applicare politiche rigorose sui tipi di file consentiti in cartelle specifiche.
2. Schermate passive per i file: monitorate e registrate quando gli utenti salvano file che corrispondono ai gruppi di file specificati, ma non impediscono l'operazione di salvataggio. Utilizzate schermate passive per tenere traccia dei modelli di utilizzo dei file senza interrompere i flussi di lavoro degli utenti.

Modelli di schermate di file

I modelli di schermate dei file forniscono una configurazione riutilizzabile che definisce le impostazioni di screening dei file, inclusi i gruppi di file bloccare o monitorare e le notifiche da generare. Dopo aver creato un modello di schermata dei file, è possibile applicarlo a più cartelle senza dover riconfigurare ogni volta le stesse impostazioni. Quando si aggiorna un modello di schermata dei file, è possibile facoltativamente applicare le modifiche a tutte le schermate dei file create a partire da tale modello.

L'utilizzo di modelli di schermate di file offre diversi vantaggi:

- **Coerenza:** assicuratevi che cartelle simili abbiano configurazioni di screening dei file identiche
- **Efficienza:** applica rapidamente le impostazioni di screening dei file a più cartelle
- **Manutenibilità:** aggiorna le impostazioni di screening dei file su più cartelle modificando il modello

Eccezioni relative alla schermata dei file

Le eccezioni relative allo schermo dei file hanno la precedenza sulle regole di screening dei file che altrimenti si applicherebbero a una cartella e a tutte le relative sottocartelle. Quando si crea un'eccezione per la schermata dei file, si specifica quali gruppi di file consentire nonostante le schermate dei file bloccate nelle cartelle principali. Le eccezioni relative alla schermata dei file sono utili quando è necessario consentire tipi di file specifici in determinate sottocartelle mantenendo al contempo restrizioni più ampie ai livelli più alti della gerarchia delle cartelle.

Ad esempio, è possibile bloccare i file eseguibili su un'intera condivisione ma creare un'eccezione per una sottocartella specifica in cui gli amministratori devono archiviare i file di installazione.

Notifiche di screening dei file

Quando gli utenti tentano di salvare file bloccati da una schermata di file attiva, FSRM può generare notifiche per avvisare gli amministratori o fornire informazioni agli utenti. È possibile configurare i seguenti tipi di notifiche:

- **Registrazione degli eventi:** registra un evento su Amazon CloudWatch o Amazon Kinesis Data Firehose per il monitoraggio e l'analisi. Puoi specificare il livello di gravità dell'evento (informazione, avviso o errore) e fornire un corpo del messaggio personalizzato. La registrazione degli eventi è utile per tenere traccia delle violazioni dello schermo dei file e per l'integrazione con i sistemi di monitoraggio esistenti.
- **Rapporti di archiviazione:** genera un rapporto sull'utilizzo dello storage che fornisce informazioni dettagliate sull'attività di screening dei file. I report sullo storage consentono di identificare i modelli nei tentativi di salvataggio dei file e di prendere decisioni informate sulle politiche di screening dei file. Per ulteriori informazioni, consulta [Rapporti di archiviazione](#).

Comandi per la gestione dello screening dei file

È possibile accedere a tre famiglie di PowerShell comandi FSx remoti per la gestione delle schermate dei file:

1. **Comandi della schermata dei file:** crea, recupera, modifica, rimuovi e ripristina le schermate dei singoli file su cartelle specifiche. Utilizzate questi comandi quando avete bisogno di gestire le schermate dei file su folder-by-folder base individuale.
2. **Comandi dei modelli di schermata dei file:** crea, recupera, modifica e rimuovi modelli di schermata dei file che definiscono configurazioni di screening dei file riutilizzabili. Utilizzate questi comandi per stabilire politiche standard di screening dei file da applicare a più cartelle.
3. **Comandi per le eccezioni relative allo screening dei file:** crea, recupera, modifica e rimuovi le eccezioni relative allo screening dei file che sostituiscono le regole di screening dei file nelle cartelle principali. Utilizzate questi comandi quando è necessario consentire tipi di file specifici in determinate sottocartelle mantenendo restrizioni più ampie.

Elenco di comandi remoti di File Screening FSx PowerShell

Note

Tutti gli esempi in questa pagina presuppongono che la `$FSxWindowsRemotePowerShellEndpoint` variabile sia stata definita con l' PowerShell endpoint Windows Remote del file system. Puoi trovare questo endpoint nella FSx console Amazon nella pagina dei dettagli del tuo file system o utilizzando il AWS CLI `describe-file-systems` comando.

Comandi sullo schermo del file

Nuova FSx FSRMFile schermata

Crea una schermata di file che impedisce agli utenti di salvare tipi di file specifici in una cartella.

Parametri:

- `Folder (string)`- Obbligatorio. Il percorso della cartella in cui verrà applicata la schermata del file.
- `Description (string)`- Facoltativo. Una descrizione per la schermata dei file.
- `IncludeGroup (array)`- Facoltativo. Un array di nomi di gruppi di file che specificano quali file bloccare o monitorare.
- `Active (boolean)`- Facoltativo. Se impostato su `true`, crea una schermata di file attiva che blocca i file. Se impostato su `false`, crea una schermata passiva che monitora solo i file. Il valore predefinito è `true`.
- `Template (string)`- Facoltativo. Il nome di un modello di schermata dei file esistente da utilizzare.
- `NotificationConfigurations (array)`- Facoltativo. Una serie di configurazioni per le notifiche quando gli utenti tentano di salvare file bloccati. Ogni configurazione ha le seguenti proprietà:
 - `ActionType (string)`: il tipo di azione da eseguire. Puoi specificare le seguenti valori:
 1. `Event`: registra un evento nel registro eventi del file system. Quando si specifica `Event`, è necessario specificare anche le seguenti proprietà:
 - `EventType (string)`: Informazioni, avviso o errore
 - `MessageBody (string)`: il testo del messaggio da registrare con l'evento.

2. **Report**: genera un rapporto sull'utilizzo dello storage. Quando si specifica **Report**, è necessario specificare anche:

- **ReportType** (string): il tipo di rapporto. È possibile specificare i seguenti valori: **DuplicateFiles**, **FilesByFileGroup**, **FilesByOwner**, **FilesByProperty**, **LargeFiles**, **Leases**, **oQuotaUsage**.

Esempi:

1. Crea una schermata di file attiva di base che blocchi i file audio.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMFileScreen -Folder "share\department" -IncludeGroup "Audio and Video
Files"
}
```

2. Crea una schermata di file che blocchi i file video e generi una voce nel registro degli eventi quando un utente tenta di salvare un file video.

```
$notifications = [System.Collections.ArrayList]@()
$eventNotification = @{
    ActionType = "Event"
    EventType = "Warning"
    MessageBody = "File screen violation detected"
}
$null = $notifications.Add($eventNotification)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    New-FSxFSRMFileScreen -Folder "share\projects" -IncludeGroup "Audio and Video
Files" -NotificationConfigurations $Using:notifications
}
```

Get- FSx FSRMFile Screen

Recupera una o più schermate di file dal file system.

Parametri:

- **Folder (string)**- Opzionale. Il percorso della cartella da cui recuperare le schermate dei file. Se non specificate il percorso della cartella, il comando restituisce tutte le schermate dei file sul file system.

Esempi:

1. Recupera tutte le schermate dei file sul file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMFileScreen  
}
```

Set- Screen FSx FSRMFile

Modifica le proprietà di una schermata di file esistente.

Parametri:

- **Folder (string)**- Obbligatorio. Il percorso della cartella che contiene la schermata del file da modificare.
- **Description (string)**- Facoltativo. Una nuova descrizione per la schermata dei file.
- **IncludeGroup (array)**- Facoltativo. Una nuova serie di nomi di gruppi di file che definiscono quali file bloccare o monitorare.
- **Active (boolean)**- Facoltativo. Se impostato su true, imposta la schermata del file in modalità attiva (blocco). Se impostato su false, imposta la schermata del file in modalità passiva (solo monitoraggio). Il valore predefinito è true.
- **NotificationConfigurations (array)**- Facoltativo. Una nuova gamma di configurazioni di notifica.
- **PassThru (boolean)**- Opzionale. Se impostato su true, restituisce l'oggetto modificato nella schermata del file.

Esempi:

1. Modifica la descrizione e i gruppi di file per una schermata di file.

```
$includeGroups = @("Audio and Video Files")
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
    param($includeGroups)
    Set-FSxFSRMFileScreen -Folder "share\projects" -Description "Updated screen" -
IncludeGroup $includeGroups
}
```

2. Imposta una schermata di file in modalità attiva e aggiungi notifiche.

```
$notifications = [System.Collections.ArrayList]@()
$eventNotification = @{
    ActionType = "Event"
    EventType = "Warning"
    MessageBody = "File screen violation detected"
}
$null = $notifications.Add($eventNotification)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    Set-FSxFSRMFileScreen -Folder "share\projects" -Active: $true -
NotificationConfigurations $Using:notifications -PassThru
}
```

Rimuovi- FSx FSRMFile Schermata

Rimuove una schermata di file da una cartella specificata.

Parametri:

- **Folder (string)**- Richiesto. Il percorso della cartella da cui rimuovere la schermata del file.
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto della schermata del file rimosso.

Esempi:

1. Rimuove una schermata di file da una cartella specifica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMFileScreen -Folder "share\projects" -PassThru
}
```

```
}
```

FSxFSRMFileSchermata di ripristino

Reimposta la schermata di un file in modo che corrisponda alle impostazioni di un modello specificato.

Parametri:

- **Folder (string)**- Obbligatorio. Il percorso della cartella che contiene la schermata del file da reimpostare.
- **Template (string)**- Obbligatorio. Il nome di un modello di schermata dei file esistente da applicare.

Esempi:

1. Reimposta una schermata di file in modo che corrisponda alle impostazioni definite in un modello di schermata dei file.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Reset-FSxFSRMFileScreen -Folder "share\department" -Template "Block Audio Files"  
}
```

Comandi del modello di file Screen

Ottieni- FSx FSRMFile ScreenTemplate

Il `Get-FSxFSRMFileScreenTemplate` comando recupera uno o più modelli di schermate di file dal file system.

Parameters

- **Name (array)**- Facoltativo. Una serie di nomi di modelli di schermate di file da recuperare. Se non si specifica un nome, il comando restituisce tutti i modelli di schermate di file presenti nel file system.

Esempi

1. Recupera tutti i modelli di schermate dei file.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMFileScreenTemplate  
}
```

Nuovo- FSx FSRMFile ScreenTemplate

Il `New-FSxFSRMFileScreenTemplate` comando crea un modello di schermata dei file che definisce una configurazione riutilizzabile per le schermate dei file. Il modello specifica quali gruppi di file bloccare e quali notifiche generare quando gli utenti tentano di salvare i file bloccati.

Parameters

- **Name (string)**- Obbligatorio. Un nome per il modello della schermata dei file.
- **Description (string)**- Facoltativo. Una descrizione del modello di schermata dei file.
- **IncludeGroup (array)**- Facoltativo. Un array di nomi di gruppi di file che specificano quali file bloccare o monitorare.
- **Active (boolean)**- Facoltativo. Se impostato su `true`, crea un modello di schermata dei file attivo che blocca i file. Se impostato su `false`, crea un modello passivo che monitora solo i file. Il valore predefinito è `true`.
- **NotificationConfigurations (array)**- Facoltativo. Una serie di configurazioni per le notifiche quando gli utenti tentano di salvare file bloccati. Ogni configurazione ha le seguenti proprietà:
 - **ActionType (string)**: il tipo di azione da eseguire. Puoi specificare le seguenti valori:
 1. **Event**: registra un evento nel registro eventi del file system. Quando si specifica **Event**, è necessario specificare anche le seguenti proprietà:
 - **EventType (string)**: Informazioni, avviso o errore
 - **MessageBody (string)**: il testo del messaggio da registrare con l'evento.
 2. **Report**: genera un rapporto sull'utilizzo dello storage. Quando si specifica **Report**, è necessario specificare anche:
 - **ReportType (string)**: il tipo di rapporto. È possibile specificare i seguenti valori:
`DuplicateFilesFilesByFileGroup,FilesByOwner,FilesByProperty,LargeFiles,Leas`
o `QuotaUsage`

Esempi

1. Crea un modello di schermata del file con notifiche.

```
$notifications = [System.Collections.ArrayList]@()
$eventNotif = @{
    ActionType = "Event"
    EventType = "Warning"
    MessageBody = "Blocked file detected"
}
$null = $notifications.Add($eventNotif)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {
    param($notifications)
    New-FSxFSRMFileScreenTemplate -Name "Block Executables" -Description
    "Blocks executable files" -IncludeGroup "Executable Files" -Active: $true -
    NotificationConfigurations $Using:notifications
}
```

Rimuovi- FSx FSRMFile ScreenTemplate

Il `Remove-FSxFSRMFileScreenTemplate` comando rimuove uno o più modelli di schermate di file dal file system. Quando rimuovete un modello, le schermate dei file create da quel modello rimangono invariate.

Parameters

- **Name (array)**- Obbligatorio. Una serie di nomi di modelli di schermate di file da rimuovere.
- **PassThru (boolean)**- Facoltativo. Se impostato su `true`, restituisce l'oggetto modello di schermata del file rimosso.

Esempi

1. Rimuove un singolo modello di schermata dei file.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    Remove-FSxFSRMFileScreenTemplate -Name "Block Executables" -PassThru
}
```

Imposta- FSx FSRMFile ScreenTemplate

Il Set-FSxFSRMFileScreenTemplate comando modifica le proprietà dei modelli di schermate di file esistenti. Aggiorna facoltativamente le schermate dei file create utilizzando i modelli modificati.

Parameters

- Name (array)- Obbligatorio. Una serie di nomi di modelli di schermate di file da modificare.
- Description (string)- Facoltativo. Una nuova descrizione per il modello.
- IncludeGroup (array)- Facoltativo. Una nuova serie di nomi di gruppi di file che definiscono quali file bloccare o monitorare.
- Active (boolean)- Facoltativo. Se impostato su true, imposta il modello in modalità attiva (blocco). Se impostato su false, imposta il modello in modalità passiva (monitoraggio). Il valore predefinito è true.
- NotificationConfigurations (array)- Facoltativo. Una nuova gamma di configurazioni di notifica.
- UpdateDerived (boolean)- Opzionale. Se impostato su true, aggiorna tutte le schermate dei file esistenti create da questo modello, indipendentemente dalle modifiche apportate a tali schermate di file.
- UpdateDerivedMatching (boolean)- Facoltativo. Se impostato su true, aggiorna solo le schermate dei file che non sono state modificate dopo la loro creazione da questo modello.
- PassThru (boolean)- Facoltativo. Se impostato su true, restituisce l'oggetto modello di schermata del file modificato.

Esempi

1. Aggiorna un modello di schermata dei file con nuovi gruppi di file.

```
$includeGroups = @("Audio and Video Files")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
    param($includeGroups)
    Set-FSxFSRMFileScreenTemplate -Name "Block Executables" -IncludeGroup
    $includeGroups
}
```

2. Aggiorna un modello di schermata dei file in modalità attiva e aggiorna tutte le schermate di file derivate.


```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Set-FSxFSRMFileScreenTemplate -Name "Block Executables" -Active: $true -  
UpdateDerived  
}
```

Comandi di eccezione per lo schermo dei file

Nuovo- FSx FSRMFile ScreenException

Il `New-FSxFSRMFileScreenException` comando crea un'eccezione relativa alla schermata dei file che sostituisce qualsiasi regola di screening dei file che altrimenti si applicherebbe a una cartella e a tutte le relative sottocartelle. Ciò consente di creare tipi di file specifici nella cartella delle eccezioni anche se sono bloccati dalle schermate dei file nelle cartelle principali.

Parameters

- **Folder (string)**- Obbligatorio. Il percorso della cartella in cui verrà applicata l'eccezione relativa alla schermata dei file. L'eccezione si applica a questa cartella e a tutte le relative sottocartelle.
- **Description (string)**- Facoltativo. Una descrizione dell'eccezione relativa allo schermo del file.
- **IncludeGroup (array)**- Facoltativo. Una serie di nomi di gruppi di file che specificano quali file consentire nonostante eventuali schermate di blocco dei file che altrimenti si applicherebbero alle cartelle principali.

Esempi

1. Crea un'eccezione per la schermata dei file per una cartella e un gruppo di file specifici.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    New-FSxFSRMFileScreenException -Folder "share\department" -IncludeGroup "Text  
Files"  
}
```

2. Crea un'eccezione per la schermata dei file con più gruppi di file.

```
$includeGroups = @("Audio and Video Files", "Documents")
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {
    param($includeGroups)
    New-FSxFSRMFileScreenException -Folder "share\projects" -Description "Allow media
files in project folder" -IncludeGroup $includeGroups
}
```

Ottieni- FSx FSRMFile ScreenException

Il `Get-FSxFSRMFileScreenException` comando recupera una o più eccezioni della schermata dei file dal file system.

Parameters

- **Folder (string)**- Facoltativo. Il percorso della cartella da cui recuperare le eccezioni della schermata dei file. Se non si specifica il percorso della cartella, il comando restituisce tutte le eccezioni della schermata dei file sul file system.

Esempi

1. Recupera tutte le eccezioni dello schermo del file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreenException
}
```

2. Recupera l'eccezione relativa alla schermata dei file per una cartella specifica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreenException -Folder "share\department"
}
```

Rimuovi- FSx FSRMFile ScreenException

Il `Remove-FSxFSRMFileScreenException` comando rimuove un'eccezione relativa alla schermata dei file da una cartella specificata. Dopo la rimozione, la cartella e le relative sottocartelle saranno soggette a tutte le regole di screening dei file delle cartelle principali che in precedenza erano state sostituite dall'eccezione.

Parameters

- **Folder (string)**- Obbligatorio. Il percorso della cartella da cui rimuovere l'eccezione relativa alla schermata del file.
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto di eccezione dello schermo del file rimosso.

Esempi

1. Rimuove un'eccezione relativa alla schermata dei file da una cartella specifica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Remove-FSxFSRMFileScreenException -Folder "share\projects" -PassThru  
}
```

Imposta- FSx FSRMFile ScreenException

Il Set-FSxFSRMFileScreenException comando modifica le proprietà di un'eccezione nella schermata del file.

Parameters

- **Folder (string)**- Obbligatorio. Il percorso della cartella che contiene l'eccezione della schermata del file da modificare.
- **Description (string)**- Facoltativo. Una nuova descrizione per l'eccezione relativa allo schermo del file.
- **IncludeGroup (array)**- Facoltativo. Una nuova serie di nomi di gruppi di file che definiscono quali file consentire nonostante eventuali schermate di file bloccanti che altrimenti si applicherebbero alle cartelle principali.
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto di eccezione modificato nella schermata del file.

Esempi

1. Aggiorna i gruppi di file consentiti per un'eccezione relativa allo screening dei file.

```
$includeGroups = @("Audio and Video Files")
```

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ArgumentList $includeGroups -ScriptBlock {  
    param($includeGroups)  
    Set-FSxFSRMFileScreenException -Folder "share\projects" -IncludeGroup  
$includeGroups -PassThru  
}
```

Classificazione dei file

La classificazione dei file assegna automaticamente le proprietà dei metadati ai file in base al contenuto, alla posizione o ad altri attributi. La classificazione consente di organizzare i file, applicare le politiche di gestione dei dati e soddisfare i requisiti di conformità identificando i file che contengono informazioni sensibili, appartengono a categorie aziendali specifiche o richiedono periodi di conservazione.

Come funziona la classificazione dei file

La classificazione dei file utilizza un processo in tre fasi:

1. Definizione delle proprietà: crea definizioni delle proprietà di classificazione che specificano i tipi di metadati da assegnare ai file, ad esempio o. "Data Sensitivity" "ContainsPII"
2. Crea regole: configura le regole di classificazione che assegnano automaticamente i valori delle proprietà ai file in base a criteri specificati, come i modelli di contenuto dei file o le posizioni delle cartelle. Ad esempio, i file che contengono uno schema come un numero di previdenza sociale (XXX-XX-XXXX) possono essere classificati automaticamente come ContainsPII=Yes.
3. Esegui la classificazione: esegui il processo di classificazione per scansionare i file e applicare le regole. È possibile eseguire la classificazione manualmente su richiesta, in base a una pianificazione o continuamente in background.

Una volta completata la classificazione, è possibile utilizzare le proprietà assegnate per generare report di archiviazione [Attività di gestione dei file](#), applicare o cercare file con caratteristiche specifiche.

Definizioni delle proprietà di classificazione

Le definizioni delle proprietà di classificazione specificano i tipi di metadati che possono essere assegnati ai file. Ogni definizione di proprietà ha un nome, un tipo di proprietà e, facoltativamente, un elenco di valori consentiti. Ad esempio, è possibile creare una proprietà chiamata "Data

Sensitivity" con un `OrderedList` Type e i valori possibili: `Public`, `InternalConfidential`, `eRestricted`.

Sono supportati i seguenti tipi di proprietà:

- `OrderedList`- Un elenco ordinato in cui i valori hanno una sequenza specifica (ad esempio, `Low`, `Medium`, `High`). Utilizzate questo tipo quando l'ordine dei valori è importante per la rendicontazione o le decisioni politiche.
- `MultiChoice`- Consente di selezionare più valori da un elenco (ad esempio, un file potrebbe essere etichettato con entrambe le categorie «Finanziario» e «Legale»).
- `SingleChoice`- Consente di selezionare un solo valore da un elenco.
- `String`- Un singolo valore di testo senza opzioni predefinite.
- `MultiString`- Valori di testo multipli senza opzioni predefinite.
- `Integer`- Un valore numerico.
- `YesNo`- Un valore booleano (vero o falso).
- `DateTime`- Un valore di data e ora.

Le definizioni delle proprietà sono riutilizzabili in più regole di classificazione. Dopo aver creato una definizione di proprietà, è possibile farvi riferimento in qualsiasi regola di classificazione che debba assegnare valori a tale proprietà.

Regole di classificazione

Le regole di classificazione definiscono la logica per l'assegnazione automatica dei valori delle proprietà ai file. Ogni regola specifica:

- Quale proprietà impostare
- Quale valore assegnare a quella proprietà
- Dove applicare la regola (quali cartelle)
- Come identificare i file che dovrebbero ricevere il valore della proprietà. È possibile utilizzare due meccanismi di classificazione:

Classificatore di contenuti

Content Classifier analizza il contenuto dei file alla ricerca di modelli di testo o espressioni regolari specifici. Utilizzate questo meccanismo per identificare i file in base a ciò che contengono. Content Classifier offre tre modi per abbinare il contenuto dei file:

- **ContentString-** Cerca stringhe di testo senza distinzione tra maiuscole e minuscole. Utilizzate questa opzione per trovare parole o frasi specifiche indipendentemente dalle maiuscole. Ad esempio, la ricerca di «riservato» corrisponderà a «Confidenziale», «CONFIDENZIALE» e «riservato».
- **ContentStringCaseSensitive-** Cerca stringhe di testo con distinzione tra maiuscole e minuscole. Utilizzate questa opzione quando le maiuscole sono importanti per la ricerca. Ad esempio, la ricerca di «SSN» corrisponderà a «SSN» ma non a «ssn» o «Ssn». Ciò è utile per acronimi, codici di prodotto o altri identificatori in cui le maiuscole e minuscole sono significative.
- **ContentRegularExpression-** Cerca modelli utilizzando espressioni regolari. Utilizzate questa opzione quando avete bisogno di abbinare modelli complessi o formati variabili. Ad esempio, puoi usare le espressioni regolari per rilevare:
 - Numeri di previdenza sociale nel formato 123-45-6789: `\b\d{3}-\d{2}-\d{4}\b`
 - Numeri di carte di credito con spazi o trattini opzionali: `\b\d{4}[\s-]?\d{4}[\s-]?\d{4}[\s-]?\d{4}\b`
 - Indirizzi e-mail, numeri di telefono o altri dati strutturati

È possibile specificare più stringhe o modelli in un'unica regola e i file verranno classificati se il loro contenuto corrisponde a uno dei valori specificati.

Classificatore di cartelle

Folder Classifier assegna i valori delle proprietà in base alla posizione in cui sono archiviati i file. Utilizzate questo meccanismo per classificare i file in base alla loro posizione nella gerarchia delle cartelle. Esempio:

- Imposta una proprietà del periodo di conservazione per tutti i file nella cartella Documenti legali
- Contrassegna tutti i file in una cartella di progetto specifica con un identificatore di progetto

Inoltre, è possibile utilizzare il `ReevaluateProperty` parametro per controllare cosa succede quando la classificazione viene eseguita su un file che ha già un valore per la proprietà. È possibile selezionare le seguenti configurazioni:

- **Never-** Classifica solo i file che non hanno un valore per questa proprietà
- **Overwrite-** Sostituisci i valori esistenti quando i file cambiano
- **Aggregate-** Combina nuovi valori con valori esistenti (per proprietà multivalore)

Proprietà di gestione

Le proprietà di gestione sono proprietà di classificazione che si applicano alle cartelle anziché ai file. Le proprietà di gestione vengono utilizzate per organizzare e classificare le cartelle nella gerarchia del file system. A differenza delle proprietà dei file che vengono assegnate automaticamente tramite regole di classificazione, le proprietà di gestione vengono impostate manualmente utilizzando il [Set- FSx FSRMMgmt Property](#) comando.

Per classificare le cartelle, utilizzare la `FolderUsage_MS` proprietà. Puoi specificare le seguenti valori:

- `User Files`
- `Group Share`
- `Application Files`
- `Backup and Archival`

Classificazione in corso

È possibile eseguire la classificazione dei file in tre modi:

1. **Classificazione manuale:** consente [Inizia- FSx FSRMClassification](#) di eseguire immediatamente la classificazione. Questo approccio è utile per testare nuove regole o eseguire attività di classificazione una tantum.
2. **Classificazione pianificata:** [Impostare- FSx FSRMClassification](#) consente di configurare una pianificazione per la classificazione automatica. È possibile pianificare la classificazione in modo che venga eseguita settimanalmente o mensilmente in orari specifici. La classificazione pianificata è appropriata per la maggior parte degli ambienti di produzione in cui si richiedono esecuzioni di classificazione regolari e prevedibili.
3. **Classificazione continua:** da utilizzare [Impostare- FSx FSRMClassification](#) con il `Continuous` parametro per abilitare la classificazione in background che viene eseguita in modo continuo. La classificazione continua classifica automaticamente i file nuovi e modificati subito dopo la loro

creazione o modifica. Questo approccio offre il massimo livello di up-to-date classificazione ma consuma più risorse di sistema.

Quando si avvia la classificazione, è possibile specificare `RunDuration` a per limitare la durata di esecuzione del processo. Se la classificazione non viene completata entro il tempo specificato, si interrompe e riprende durante la successiva esecuzione pianificata o quando la si riavvia manualmente.

Al termine della classificazione, è possibile visualizzare le proprietà di classificazione assegnate ai file facendo clic con il pulsante destro del mouse su un file in Windows File Explorer, selezionando Proprietà e scegliendo la scheda Classificazione. Questa scheda mostra tutte le proprietà di classificazione e i relativi valori per il file.

Gestione del processo di classificazione

È possibile monitorare e controllare il processo di classificazione con i seguenti comandi:

- [Ottieni- FSx FSRMClassification](#)- Verifica lo stato attuale della classificazione (Running, Queued, NotRunning, oUnknown)
- [Smettila... FSx FSRMClassification](#)- Interrompi un processo di classificazione in esecuzione o in coda
- [Aspetta... FSx FSRMClassification](#)- Sospende l'esecuzione dello script fino al completamento della classificazione o alla scadenza di un timeout

Utilizzate questi comandi per coordinare la classificazione con altre attività. Ad esempio, è possibile attendere il completamento della classificazione prima di generare un report di archiviazione che dipenda dalle proprietà dei file classificati.

Procedure consigliate di classificazione

Segui queste best practice per garantire una classificazione dei file efficiente ed efficace.

1. Considerazioni sulle prestazioni

La classificazione basata sui contenuti richiede molte risorse perché FSRM deve leggere e scansionare il contenuto dei file.

- Verifica innanzitutto le regole su un set di dati di piccole dimensioni: prima di applicare le regole di classificazione all'intero file system, testale su un campione rappresentativo di file per verificare che funzionino come previsto e per stimare il tempo necessario per la classificazione.
- Limita l'ambito di scansione dei contenuti: la classificazione basata sui contenuti richiede molte risorse perché richiede la lettura del contenuto dei file. Utilizzate il `Namespace` parametro per limitare le regole a cartelle specifiche anziché eseguire la scansione dell'intero file system.
- Usa la classificazione delle cartelle quando possibile: `Folder Classifier` è molto più veloce di `Content Classifier` perché non ha bisogno di leggere il contenuto dei file. Quando i file possono essere classificati in base alla loro posizione, utilizza `Folder Classifier` anziché `Content Classifier`.
- Pianifica la classificazione durante le ore non di punta: esegui la classificazione pianificata durante i periodi di scarsa attività del sistema per ridurre al minimo l'impatto sulle prestazioni degli utenti. Evita di eseguire la classificazione durante le finestre di backup o altre attività di manutenzione.
- Imposta `RunDuration` i limiti appropriati: utilizza il `RunDuration` parametro per evitare che la classificazione duri troppo a lungo e influisca sulle prestazioni del sistema. Se la classificazione non viene completata entro il limite di tempo, riprenderà durante la successiva esecuzione pianificata.
- Monitora le prestazioni di classificazione: `Get-FSxFSRMClassification` da utilizzare per verificare lo stato della classificazione e identificare se la classificazione sta impiegando più tempo del previsto. La classificazione a lungo termine può indicare che le regole devono essere ottimizzate o che il sistema necessita di più risorse.

2. Progettazione delle regole

- Usa espressioni regolari specifiche: durante l'uso `ContentRegularExpression`, scrivi modelli il più specifici possibile per evitare false corrispondenze. Prova a fondo le espressioni regolari prima di implementarle in produzione.
- Combina più modelli in modo efficiente: anziché creare regole separate per modelli simili, combinali in un'unica regola con `ContentRegularExpression` valori multipli `ContentString` o. Ciò riduce il numero di volte in cui FSRM deve scansionare ogni file.
- Escludi cartelle non necessarie: utilizza il `ExcludeNamespace` parametro in `Set-FSxFSRMClassification` per escludere le directory temporanee e altre posizioni che non richiedono una classificazione.

3. Gestione della proprietà

- Pianifica lo schema delle proprietà: progetta le proprietà di classificazione prima di creare regole. Considerate le proprietà necessarie per le politiche di reporting, conformità e gestione dei file.
- Definizioni delle proprietà del documento: utilizzate il campo Descrizione per spiegare il significato di ciascuna proprietà e come deve essere utilizzata. Questo aiuta gli altri amministratori a comprendere lo schema di classificazione.

4. Manutenzione continua

- Rivedi regolarmente i risultati della classificazione: genera report di archiviazione per verificare che la classificazione funzioni come previsto e che i file ricevano i valori di proprietà corretti.
- Aggiorna le regole secondo necessità: man mano che i requisiti di gestione dei dati dell'organizzazione cambiano, aggiorna le regole di classificazione per riflettere nuove politiche o requisiti di conformità.
- Pulisci le proprietà non utilizzate: rimuovi le definizioni e le regole delle proprietà che non sono più necessarie per mantenere gestibile la configurazione della classificazione.

Comandi di gestione della classificazione

È possibile accedere a quattro famiglie di PowerShell comandi FSx remoti per la gestione della classificazione dei file:

1. Comandi di definizione delle proprietà: crea e gestisce le definizioni delle proprietà di classificazione che specificano i tipi di metadati che è possibile assegnare ai file.
2. Comandi delle regole di classificazione: crea e gestisci regole di classificazione automatiche che assegnano valori alle proprietà in base al contenuto o alla posizione del file.
3. Comandi delle proprietà di gestione: impostano e recuperano le proprietà di classificazione sulle cartelle anziché sui file.
4. Comandi del processo di classificazione: avvia, arresta, monitora e configura il processo di classificazione.

Elenco di PowerShell comandi FSx remoti per la classificazione dei file

Note

Tutti gli esempi in questa pagina presuppongono che la `$FSxWindowsRemotePowerShellEndpoint` variabile sia stata definita con l' endpoint PowerShell Windows Remote del file system. Puoi trovare questo endpoint nella FSx console Amazon nella pagina dei dettagli del tuo file system o utilizzando il AWS CLI `describe-file-systems` comando.

Comandi di definizione delle proprietà

Nuovo- FSx FSRMClassification PropertyDefinition

`New-FSxFSRMClassificationPropertyDefinition`: crea una definizione di proprietà di classificazione che può essere utilizzata per classificare i file. Le definizioni delle proprietà definiscono gli attributi che possono essere assegnati ai file tramite regole di classificazione.

Parametri:

- `Name (string)`- Obbligatorio. Un nome per la definizione della proprietà.
- `DisplayName (string)`- Facoltativo. Un nome visualizzato per la definizione della proprietà.
- `Description (string)`- Facoltativo. Una descrizione per la definizione della proprietà.
- `Type (string)`- Obbligatorio. Il tipo di proprietà di classificazione. Puoi specificare le seguenti valori:
 - `OrderedList`: un elenco ordinato di valori possibili
 - `MultiChoice`: selezione a scelta multipla tra i valori possibili
 - `SingleChoice`: Scelta singola tra i valori possibili
 - `String`: stringa di testo singola
 - `MultiString`: stringhe di testo multiple
 - `Integer`: valore numerico
 - `YesNo`: valore booleano
 - `DateTime`: valore di data e ora

- **PossibleValueConfigurations (array)**- Facoltativo. Una serie di configurazioni per **OrderedList MultiChoice**, o tipi di **SingleChoice** proprietà. Ogni configurazione ha le seguenti proprietà:
 - **Name (string)**: nome del valore (obbligatorio)
 - **Description (string)**: Una descrizione del valore (opzionale)
- **Parameters (array)**- Facoltativo. Una serie di stringhe in "name=value" formato per una configurazione aggiuntiva.

Esempi:

1. Crea un elenco di proprietà per i dati PII.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "ContainsPII" -Type OrderedList -
PossibleValueConfigurations @(
    @{ Name = "Yes" },
    @{ Name = "No" })
}
```

2. Crea una proprietà di elenco ordinato per la sensibilità dei dati.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "DataSensitivity" -Type
OrderedList -PossibleValueConfigurations @(
    @{ Name = "Public" },
    @{ Name = "Internal" },
    @{ Name = "Confidential" },
    @{ Name = "Restricted" }
    )
}
```

Ottieni- FSx FSRMClassification PropertyDefinition

Get-FSxFSRMClassificationPropertyDefinition: recupera una o più definizioni delle proprietà di classificazione dal file system.

Parametri:

- **Name (array)**- Facoltativo. Una matrice di nomi di definizioni di proprietà da recuperare. Se non si specifica un nome, il comando restituisce tutte le definizioni di proprietà nel file system.

Esempi:

1. Recupera tutte le definizioni delle proprietà di classificazione sul file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMClassificationPropertyDefinition  
}
```

Imposta- FSx FSRMClassification PropertyDefinition

Modifica le proprietà di una definizione di proprietà di classificazione esistente.

Parameters

- **Name (array)**- Richiesto. Una matrice di nomi di proprietà da modificare.
- **DisplayName (string)**- Facoltativo. Un nuovo nome visualizzato per la definizione della proprietà.
- **Description (string)**- Facoltativo. Una nuova descrizione per la definizione della proprietà.
- **PossibleValueConfigurations (array)**- Facoltativo. Una nuova serie di configurazioni per **OrderedList** **MultiChoice**, o **SingleChoice** proprietà. Ogni configurazione ha le seguenti proprietà:
 - **Name (string)**: nome del valore (obbligatorio)
 - **Description (string)**: Una descrizione del valore (opzionale)
- **Parameters (array)**- Facoltativo. Un nuovo array di stringhe in formato «name=value».
- **PassThru (boolean)**- Facoltativo. Se impostato su **true**, restituisce l'oggetto di definizione della proprietà modificato.

Esempi:

1. Aggiorna i valori possibili con le descrizioni di una definizione di proprietà esistente.

```
$values = [System.Collections.ArrayList]@()  
$null = $values.Add(@{  
    Name = "High"
```

```
        Description = "High Risk Content"
    })
    $null = $values.Add(@{
        Name = "Medium"
        Description = "Medium Risk Content"
    })

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
    FSxRemoteAdmin -ArgumentList $values -ScriptBlock {
    param($values)
    Set-FSxFSRMClassificationPropertyDefinition -Name "RiskLevel" -
PossibleValueConfigurations $Using:values -PassThru
}
```

Rimuovi- FSx FSRMClassification PropertyDefinition

Rimuove una o più definizioni di proprietà di classificazione dal file system. È possibile rimuovere solo le definizioni di proprietà definite localmente.

Parameters

- **Name (array)**- Richiesto. Una serie di nomi di proprietà da rimuovere.
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto di definizione della proprietà rimosso.

Esempi:

1. Rimuove una singola definizione di proprietà.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
    FSxRemoteAdmin -ScriptBlock {
        Remove-FSxFSRMClassificationPropertyDefinition -Name "RiskLevel" -PassThru
    }
```

Comandi delle regole di classificazione

Nuova FSx FSRMClassification regola

Crea una regola di classificazione automatica che assegna i valori delle proprietà ai file in base a criteri specificati. Ogni regola imposta un valore per una singola proprietà.

Parameters

- **Name (string)**- Richiesto. Un nome per la regola di classificazione.
- **Description (string)**- Facoltativo. Una descrizione della regola di classificazione.
- **Property (string)**- Obbligatorio. Il nome della proprietà di classificazione da impostare. Deve essere un nome di definizione di proprietà esistente.
- **PropertyValue (string)**- Facoltativo. Il valore da assegnare alla proprietà. Deve essere valido per il meccanismo di classificazione specificato.
- **Namespace (array)**- Obbligatorio. Una serie di percorsi o tipi di cartelle a cui si applica la regola.
- **Disabled (boolean)**- Facoltativo. Se impostato su true, crea la regola in uno stato disabilitato.
- **ReevaluateProperty (string)**- Facoltativo. Specifica quando rivalutare i file. Puoi specificare le seguenti valori:
 - **Never**: valuta solo i file senza un valore di proprietà esistente
 - **Overwrite**: rivaluta quando i file cambiano e sovrascrivono il valore esistente
 - **Aggregate**: rivaluta quando i file cambiano e si combinano con il valore esistente
- **Flags (array)**- Facoltativo. Specifica comportamenti speciali per la regola. Puoi specificare le seguenti valori:
 - **ClearAutomaticallyClassifiedProperty**
 - **ClearManuallyClassifiedProperty**
 - **Deprecated**
- **ContentRegularExpression (array)**- Facoltativo. Una serie di espressioni regolari per corrispondere al contenuto del file.
- **ContentString (array)**- Facoltativo. Una serie di stringhe senza distinzione tra maiuscole e minuscole da cercare nel contenuto del file.
- **ClassificationMechanism (string)**- Obbligatorio. Il meccanismo da utilizzare per classificare i file. Puoi specificare le seguenti valori:
 - **Content Classifier**: analizza il contenuto dei file alla ricerca di stringhe o modelli di espressioni regolari specifici. Quando si specifica Content Classifier, è possibile utilizzare i ContentRegularExpression parametri ContentString ContentStringCaseSensitive, o per definire il contenuto da cercare.
 - **Folder Classifier**: classifica i file in base alla posizione della cartella

- **Parameters (array)**- Facoltativo. Una serie di "name=value" stringhe per una configurazione aggiuntiva.

Esempi:

1. Rileva i numeri di previdenza sociale utilizzando un'espressione regolare.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Detect_SSN" -Property "ContainsPII" -
Property "Yes" -Namespace "share" -ClassificationMechanism "Content Classifier" -
ContentRegularExpression "\b\d{3}-\d{2}-\d{4}\b"
}
```

2. Rileva i numeri delle carte di credito usando un'espressione regolare.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Detect_CreditCard" -Property "ContainsPII" -
Property "Yes" -Namespace "share" -ClassificationMechanism "Content Classifier" -
ContentRegularExpression "\b\d{4}[\s-]?\d{4}[\s-]?\d{4}[\s-]?\d{4}\b"
}
```

3. Classificate ogni file in una cartella con un periodo di conservazione di 7 anni Property.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Contracts_Records_7Year" -Property
"RetentionPeriod" -PropertyValue "7 years" -Namespace "share/Legal Documents" -
ClassificationMechanism "Folder Classifier"
}
```

Regola Get- FSx FSRMClassification

Recupera una o più regole di classificazione dal file system.

Parameters

- **Name (array)**- Facoltativo. Una serie di nomi di regole di classificazione da recuperare. Se non si specifica un nome, il comando restituisce tutte le regole sul file system.

Esempi:

1. Recupera tutte le regole di classificazione sul file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMClassificationRule  
}
```

Imposta - Regola FSx FSRMClassification

Modifica le proprietà delle regole di classificazione esistenti.

Parameters

- **Name (array)**- Obbligatorio. Una serie di nomi di regole di classificazione da modificare.
- **Description (string)**- Facoltativo. Una nuova descrizione della regola.
- **Property (string)**- Facoltativo. Il nome della proprietà di classificazione da impostare.
- **PropertyValue (string)**- Facoltativo. Un nuovo valore da assegnare alla proprietà.
- **Namespace (array)**- Facoltativo. Una nuova serie di percorsi o tipi di cartelle a cui si applica la regola.
- **Disabled (boolean)**- Facoltativo. Se impostato su true, disabilita la regola. Se impostato su false, abilita la regola.
- **ReevaluateProperty (string)**- Facoltativo. Modifica quando rivalutare i file. Puoi specificare le seguenti valori:
 - **Never**: valuta solo i file senza il valore della proprietà esistente
 - **Overwrite**: rivaluta quando i file cambiano e sovrascrivono il valore esistente
 - **Aggregate**: rivaluta quando i file cambiano e si combinano con il valore esistente
- **Flags (array)**- Facoltativo. Nuovi comportamenti speciali per la regola. Puoi specificare le seguenti valori:
 - **ClearAutomaticallyClassifiedProperty**
 - **ClearManuallyClassifiedProperty**
 - **Deprecated**
- **ContentRegularExpression (array)**- Facoltativo. Una nuova serie di espressioni regolari.
- **ContentString (array)**- Facoltativo. Una nuova serie di stringhe di ricerca senza distinzione tra maiuscole e minuscole.

- **ContentStringCaseSensitive (array)**- Facoltativo. Una nuova serie di stringhe di ricerca con distinzione tra maiuscole e minuscole.
- **ClassificationMechanism (string)**- Facoltativo. Un nuovo meccanismo di classificazione da utilizzare. Puoi specificare le seguenti valori:
 - **Content Classifier**: analizza il contenuto del file alla ricerca di stringhe o modelli di espressioni regolari specifici. Quando si specifica Content Classifier, è possibile utilizzare i ContentRegularExpression parametri ContentString ContentStringCaseSensitive, o per definire il contenuto da cercare.
 - **Folder Classifier**: classifica i file in base alla posizione della cartella
- **Parameters (array)**- Facoltativo. Una nuova serie di stringhe di "name=value" configurazione.
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto regola modificato.

Esempi:

1. Aggiorna le proprietà della regola e lo spazio dei nomi di una regola di classificazione esistente.

```
$namespaces = @("share\finance", "share\accounting")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $namespaces -ScriptBlock {
    param($namespaces)
    Set-FSxFSRMClassificationRule -Name "Detect_CreditCard" -Description "Updated PII
detection" -Namespace $Using:namespaces -ReevaluateProperty "Overwrite"
}
```

Rimuovi- Regola FSx FSRMClassification

Rimuove una o più regole di classificazione dal file system.

Parameters

- **Name (array)**- Obbligatorio. Una serie di nomi di regole di classificazione da rimuovere.
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto regola rimosso.

Esempi:

1. Rimuove una singola regola di classificazione.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Remove-FSxFSRMCClassificationRule -Name "Find Confidential Files" -PassThru  
}
```

Comandi delle proprietà di gestione

Get- FSx FSRMMgmt Property

Recupera le proprietà di gestione dalle cartelle specificate. Le proprietà di gestione sono proprietà di classificazione che si applicano alle cartelle anziché ai file.

Parameters

- **Namespace (string)**- Facoltativo. Un percorso verso una cartella.
- **Name (string)**- Facoltativo. Il nome di una proprietà di gestione da recuperare. Se non si specifica un nome, il comando recupera tutte le proprietà di gestione.
- **Recurse (boolean)**- Facoltativo. Se impostato su true, recupera le proprietà di gestione per tutte le cartelle all'interno del namespace. Richiede il parametro Namespace.
- **Effective (boolean)**- Facoltativo. Se impostato su true, recupera la proprietà di gestione per la cartella più vicina con il nome specificato. La ricerca include lo spazio dei nomi specificato e la relativa gerarchia principale. Richiede il parametro Name.

Esempi:

1. Recupera tutte le proprietà di gestione sul file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMMgmtProperty  
}
```

2. Recupera le proprietà di gestione per una cartella specifica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMMgmtProperty -Namespace "share\department"  
}
```

Rimuovi- Proprietà FSx FSRMMgmt

Rimuove le proprietà di gestione dalle cartelle specificate.

Parameters

- **Namespace (string)**- Facoltativo. Un percorso verso una cartella.
- **Name (string)**- Obbligatorio. Il nome della proprietà di gestione da rimuovere.
- **Recurse (boolean)**- Facoltativo. Se impostato su true, rimuove le proprietà di gestione per tutte le cartelle all'interno dello spazio dei nomi. Richiede il parametro Namespace.

Esempi:

1. Rimuove tutte le istanze di una proprietà di gestione.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Remove-FSxFSRMMgmtProperty -Name "FolderUsage_MS"  
}
```

2. Rimuove una proprietà di gestione da una cartella specifica.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Remove-FSxFSRMMgmtProperty -Name "FolderUsage_MS" -Namespace "share\department"  
}
```

Set- FSx FSRMMgmt Property

Modifica il valore di una proprietà di gestione per uno spazio dei nomi specificato. Le proprietà di gestione sono proprietà di classificazione che si applicano alle cartelle e non hanno il flag Secure impostato.

Parameters

- **Namespace (string)**- Facoltativo. Il percorso della cartella.
- **Name (string)**- Obbligatorio. Il nome della proprietà di gestione da modificare. Deve essere una proprietà di classificazione esistente applicabile alle cartelle.
- **Value (string)**- Obbligatorio. Il nuovo valore da assegnare alla proprietà di gestione.

Esempi:

1. Imposta una proprietà di utilizzo della cartella.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Set-FSxFSRMMgmtProperty -Namespace "share\department" -Name "FolderUsage_MS" -Value  
    "User Files"  
}
```

Comandi del processo di classificazione

Ottieni- FSx FSRMClassification

Recupera lo stato del processo di classificazione dei file in esecuzione. Lo stato può avere uno dei seguenti valori:

- Unknown: lo stato della classificazione non può essere determinato
- NotRunning: nessuna classificazione è attualmente in esecuzione
- Queued: La classificazione è in coda per iniziare
- Running: La classificazione è attualmente in corso

Parameters

Nessuno

Esempi:

1. Recupera lo stato corrente della classificazione.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMClassification  
}
```

Inizia- FSx FSRMClassification

Avvia il processo di classificazione dei file, che applica le regole di classificazione ai file e genera un rapporto di classificazione.

Parameters

- **Queue (boolean)**- Facoltativo. Se impostato su true, aggiunge l'attività di classificazione a una coda da eseguire entro i successivi 5 minuti. Tutte le attività in coda durante questo periodo verranno eseguite contemporaneamente. Se impostata su false o non specificata, la classificazione inizia immediatamente.
- **RunDuration (number)**- Facoltativo. Specifica per quante ore deve essere eseguito il processo di classificazione prima di essere annullato. Valori validi: da -1 a 2147483. Valori speciali:
 - -1: Esegui fino all'annullamento
 - 0: Esegui fino al completamento
 - Se non specificato, viene eseguito fino al completamento.

Esempi:

1. Inizia la classificazione senza limiti di tempo.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Start-FSxFSRMClassification -RunDuration 0  
}
```

Smettila... FSx FSRMClassification

Interrompe qualsiasi processo di classificazione in esecuzione o in coda sul file system.

Parameters

Nessuno

Esempi:

1. Interrompe una classificazione in corso.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Stop-FSxFSRMClassification  
}
```

Aspetta... FSx FSRMClassification

Attende il completamento del processo di classificazione dei file. Utilizzate questo comando quando è necessario eseguire azioni che dipendono dal completamento della classificazione, come la generazione di report basati su file classificati.

Parameters

- **Timeout (number)**- Facoltativo. Specificate il tempo di attesa, in secondi, per il completamento della classificazione. Se il timeout scade prima del termine della classificazione, il comando viene restituito ma la classificazione continua a essere eseguita in background. Valori validi: da -1 a 2147483. Valori speciali:
 - -1: Attendi indefinitamente fino al completamento della classificazione (impostazione predefinita)
 - 0: Controlla lo stato attuale e torna immediatamente senza aspettare

Esempi:

1. Attendi a tempo indeterminato il completamento della classificazione.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Wait-FSxFSRMClassification  
}
```

Impostare- FSx FSRMClassification

Modifica le impostazioni di configurazione per la classificazione dei file.

Parameters

- **ExcludeNamespace (array)**- Facoltativo. Una serie di cartelle aggiuntive da escludere dalla classificazione.
- **ScheduleConfigurations (hashtable)**- Facoltativo. Una tabella hash contenente la configurazione della pianificazione con le seguenti proprietà:
 - **Time (datetime)**: DateTime oggetto che specifica quando eseguire l'attività (obbligatorio)
 - **RunDuration (number)**: numero di ore di esecuzione dell'attività (opzionale)
 - **Weekly (array)**: matrice di giorni feriali (opzionale)
 - **Monthly (array)**: matrice di giorni del mese, usa -1 per l'ultimo giorno (opzionale)

- **Continuous** (boolean)- Facoltativo. Se impostato su true, consente la classificazione continua dello sfondo.
- **PassThru** (boolean)- Facoltativo. Se impostato su true, restituisce l'oggetto di configurazione della classificazione modificato.

Esempi:

1. Abilita la classificazione continua.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Set-FSxFSRMClassification -Continuous $true  
}
```

2. Imposta una pianificazione settimanale per eseguire la classificazione.

```
$schedule = @{  
    Time = ("12:00am")  
    Weekly = @('Monday', 'Wednesday', 'Friday')  
}  
  
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {  
    param($schedule)  
    Set-FSxFSRMClassification -ScheduleConfigurations $schedule  
}
```

3. Imposta una pianificazione mensile con esclusioni personalizzate.

```
$schedule = @{  
    Time = ("12:00am")  
    Monthly = @(1, 15, -1) # 1st, 15th, and last day  
    RunDuration = 4  
}  
$excludeNamespaces = @("share\folder /s")  
  
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ArgumentList @($schedule, $excludeNamespaces) -ScriptBlock {  
    param($schedule, $excludeNamespaces)  
    Set-FSxFSRMClassification -ScheduleConfigurations $schedule -ExcludeNamespace  
$excludeNamespaces
```


}

Rapporti di archiviazione

I report sullo storage forniscono un'analisi dettagliata dell'utilizzo del file system, aiutandoti a capire come viene utilizzato lo storage, a identificare i file che possono essere archiviati o eliminati e a monitorare la conformità con le politiche di gestione dei file. È possibile generare diversi tipi di report che analizzano la proprietà dei file, i tipi di file, i file duplicati, i file di grandi dimensioni, lo screening dei file e l'utilizzo delle quote.

Tipi di report

È possibile creare i seguenti tipi di report:

- **DuplicateFiles**

Identifica i file con contenuti identici in base alla dimensione dei file e al confronto degli hash. Utilizza questo rapporto per trovare file ridondanti che occupano spazio di archiviazione non necessario. Il rapporto raggruppa i file duplicati e mostra lo spazio totale che potrebbe essere recuperato rimuovendo i duplicati.

- **FilesByFileGroup**

[Raggruppa i file in base all'appartenenza ai gruppi di file](#) e mostra il consumo di spazio di archiviazione per ogni gruppo di file. Utilizza questo rapporto per capire quali tipi di file (documenti, supporti, eseguibili, ecc.) occupano più spazio di archiviazione.

- **FilesByOwner**

Raggruppa i file per proprietario e mostra la quantità di spazio di archiviazione utilizzata da ciascun utente o gruppo. Utilizza questo rapporto per identificare gli utenti che consumano la maggior parte dello spazio di archiviazione e per allocare i costi o le quote di archiviazione in modo appropriato.

- **FilesByProperty**

Raggruppa i file in base ai valori delle proprietà di classificazione e mostra il numero di file e il consumo di archiviazione per ogni valore di proprietà. Utilizza questo rapporto per analizzare i file in base alla loro classificazione, ad esempio il livello di sensibilità dei dati, il reparto o il periodo di conservazione. Questo rapporto richiede che i file siano stati classificati utilizzando [Regole di classificazione](#).

- **FileScreenAuditFiles**

Elenca [Screening dei file](#) le violazioni in cui gli utenti hanno tentato di salvare file bloccati dalle schermate di file attive. Utilizzate questo rapporto per monitorare la conformità alle politiche di screening dei file e identificare gli utenti che tentano frequentemente di salvare tipi di file non autorizzati.

- **FoldersByProperty**

Raggruppa le cartelle in base ai valori delle proprietà di gestione e mostra il consumo di spazio di archiviazione per ogni valore di proprietà. Utilizzate questo rapporto per analizzare l'utilizzo dello storage in base allo scopo della cartella, ad esempio file utente, condivisioni di gruppo o file di applicazioni.

- **LargeFiles**

Elenca i file che superano una soglia di dimensione specificata. Utilizzate questo rapporto per identificare i file che occupano molto spazio di archiviazione e che possono essere candidati all'archiviazione, alla compressione o all'eliminazione.

- **LeastRecentlyAccessed**

Elenca i file a cui non è stato effettuato l'accesso per un determinato numero di giorni. Utilizza questo report per identificare i file inattivi che possono essere archiviati o spostati su livelli di storage più economici.

- **MostRecentlyAccessed**

Elenca i file a cui è stato effettuato l'accesso entro un determinato numero di giorni.

- **QuotaUsage**

Mostra le statistiche sull'utilizzo delle quote per le cartelle con [quote](#) configurate. Utilizza questo rapporto per monitorare la conformità delle quote e identificare le cartelle che si avvicinano ai limiti di quota.

Formati dei report

È possibile generare report in più formati per soddisfare diversi casi d'uso:

- DHTML- Formato HTML dinamico con funzionalità interattive come l'ordinamento e il filtraggio.
- HTML- Formato HTML statico adatto per l'archiviazione o l'invio di e-mail.
- XML- Formato di dati strutturato per l'elaborazione programmatica.

- CSV- Formato di valori separati da virgole per l'importazione in applicazioni di fogli di calcolo.
- Text- Formato di testo semplice per una semplice visualizzazione o elaborazione.

È possibile specificare più formati per un singolo report.

Report interattivi e pianificati

È possibile creare due tipi di report di archiviazione:

1. Report interattivi: vengono eseguiti immediatamente al momento della creazione ed eseguiti una sola volta. Utilizza report interattivi per analisi o risoluzione dei problemi ad hoc. I report interattivi non hanno pianificazioni e non possono essere modificati dopo la creazione. Per eseguire un altro report interattivo, è necessario creare un nuovo report con un nome diverso.
2. Report pianificati: vengono eseguiti automaticamente in base a una pianificazione configurata. Utilizza i report pianificati per il monitoraggio regolare e la segnalazione della conformità. Puoi pianificare i report in modo che vengano eseguiti settimanalmente o mensilmente in orari specifici. I report pianificati possono essere modificati per cambiarne la configurazione ed è anche possibile eseguirli su richiesta utilizzando il [Inizia - FSx FSRMStorage Segnala](#) comando senza attendere l'ora pianificata.

Rapporti in esecuzione

Dopo aver creato un rapporto pianificato, puoi eseguirlo in diversi modi:

- Esecuzione automatica: i report pianificati vengono eseguiti automaticamente all'ora di pianificazione configurata.
- Esecuzione manuale: [Inizia - FSx FSRMStorage Segnala](#) consente di eseguire un rapporto pianificato su richiesta senza attendere l'ora pianificata.

È possibile monitorare l'esecuzione del report utilizzando [Ottieni un FSx FSRMStorage rapporto](#) per verificare lo stato.

Accesso ai report di archiviazione

Dopo che FSRM ha generato i report di archiviazione, i file di report vengono salvati in una posizione predefinita sul file system. Per accedere a questi report, è necessario mappare la quota amministrativa D\$ del file system.

Per accedere ai report di archiviazione

1. Mappare la condivisione D\$ amministrativa utilizzando il seguente formato di percorso:

```
\\file-system-dns-name\D$
```

Esempio:

```
\\amznfsxaa11bb22.corp.example.com\D$
```

2. Accedere alla StorageReports cartella. Questa cartella contiene sottocartelle organizzate per tipo di rapporto e data di esecuzione.

Note

L'accesso alla condivisione amministrativa D\$ richiede credenziali di amministratore.

Procedure ottimali per i report di archiviazione

Segui queste best practice per garantire una reportistica efficiente ed efficace sullo storage:

Considerazioni sulle prestazioni

La generazione di report di archiviazione richiede molte risorse perché FSRM deve scansionare grandi quantità di file.

- Limita l'ambito del rapporto: utilizza il Namespace parametro per limitare i report a cartelle specifiche anziché eseguire la scansione dell'intero file system. La scansione di strutture di directory di grandi dimensioni richiede molte risorse e può richiedere ore per essere completata.
- Pianifica i report durante le ore non di punta: esegui report pianificati durante i periodi di scarsa attività del sistema, per ridurre al minimo l'impatto sulle prestazioni. Evita di eseguire report durante le finestre di backup o altre attività di manutenzione.
- Imposta soglie ragionevoli: utilizza i parametri di soglia per limitare l'output dei report a dati utilizzabili. Ad esempio, impostate un valore che identifichi LargeFileMinimum i file che vale la pena esaminare, non tutti i file di dimensioni superiori a 1 MB.

- **RunDuration Limiti di utilizzo:** imposta il `RunDuration` parametro per evitare che i report vengano eseguiti troppo a lungo e influiscano sulle prestazioni del sistema. Se un report non viene completato entro il limite di tempo, riprenderà durante la successiva esecuzione pianificata.
- **Monitora le prestazioni dei report:** [Ottieni un FSx FSRMStorage rapporto](#) da utilizzare per verificare il tempo necessario per il completamento dei report. Se i report richiedono sempre troppo tempo, valuta la possibilità di restringerne l'ambito o di eseguirli meno frequentemente.

Progettazione dei report

- **Usa nomi descrittivi:** assegna ai report nomi chiari e descrittivi che indichino cosa analizzano e quando vengono eseguiti, ad esempio «Weekly Large Files - Finance Share» o «Monthly Duplicate Files - All Shares».
- **Combina analisi correlate:** quando generi più tipi di report per lo stesso namespace, crea un singolo report con più `ReportType` valori anziché report separati. Ciò è più efficiente perché FSRM deve scansionare la struttura delle directory una sola volta.
- **Filtra per modelli di file:** utilizza i parametri dei modelli di file per concentrare i report su tipi di file specifici. Ad esempio, quando si analizzano file di grandi dimensioni, è possibile creare report separati per file video, file di database e file di archivio per comprendere meglio i modelli di utilizzo dello spazio di archiviazione.
- **Sfrutta le proprietà di classificazione:** utilizza i `FilesByProperty` report per analizzare i file in base alla loro classificazione. Ciò fornisce informazioni più significative.

Gestione dei report

- **Rivedi i report regolarmente:** pianifica il tempo necessario per esaminare i risultati dei report e agire in base ai risultati. I report sono utili solo se vengono utilizzati per prendere decisioni sulla gestione dello storage.
- **Archivia i vecchi report:** i file di report si accumulano nel tempo e occupano spazio di archiviazione. Stabilisci una politica di conservazione per i file di report ed elimina o archivia i vecchi report che non sono più necessari.
- **Rapporti di test prima della pianificazione:** crea report interattivi per testare le configurazioni dei report e verificare che producano i risultati previsti prima di creare versioni pianificate.

Comandi per la gestione dei report di archiviazione

È possibile accedere a due famiglie di PowerShell comandi FSx remoti per la gestione dei report di archiviazione:

1. Comandi di definizione dei report: crea, recupera, modifica e rimuovi configurazioni dei report di archiviazione che specificano quali dati analizzare, quando eseguire i report e quali formati generare.
2. Comandi di esecuzione dei report: avvia, interrompi, monitora e attendi la generazione dei report di archiviazione. Utilizza questi comandi per eseguire report su richiesta o gestire processi di report di lunga durata.

Elenco di comandi remoti di Storage Report FSx PowerShell

Note

Tutti gli esempi in questa pagina presuppongono che la `$FSxWindowsRemotePowerShellEndpoint` variabile sia stata definita con l' endpoint PowerShell Windows Remote del file system. Puoi trovare questo endpoint nella FSx console Amazon nella pagina dei dettagli del tuo file system o utilizzando il AWS CLI `describe-file-systems` comando.

Comandi di definizione dei report

Nuovo- FSx FSRMStorage Rapporto

Nuovo - FSx FSRMStorage Rapporto: crea un rapporto di archiviazione che analizza le directory specificate per generare uno o più tipi di report.

Parametri:

- **Name (string)**- Obbligatorio. Un nome per il report di archiviazione.
- **Namespace (array)**- Obbligatorio. Una serie di percorsi o tipi di cartelle da analizzare. È possibile specificare percorsi in più formati:
 - Percorso della cartella
 - [Classificazione delle cartelle](#). Ad esempio, `[FolderUsage_ms="File utente "]`

- **ReportType (array)**- Obbligatorio. Una serie di tipi di report da generare. Puoi specificare le seguenti valori:
 - **DuplicateFiles**: identifica i file duplicati in base alle dimensioni e al contenuto dei file
 - **FilesByFileGroup**: raggruppa i file in base all'appartenenza al gruppo di file
 - **FilesByOwner**: raggruppa i file per proprietario
 - **FilesByProperty**: raggruppa i file in base alla proprietà di classificazione
 - **FileScreenAuditFiles**: elenca le violazioni relative allo screening dei file
 - **FoldersByProperty**: raggruppa le cartelle in base alla proprietà di gestione
 - **LargeFiles**: elenca i file al di sopra di una soglia di dimensione specificata
 - **LeastRecentlyAccessed**: elenca i file a cui non è stato effettuato l'accesso di recente
 - **MostRecentlyAccessed**: elenca i file a cui è stato effettuato l'accesso di recente
 - **QuotaUsage**: mostra le statistiche sull'utilizzo delle quote
- **ReportFormat (array)**- Facoltativo. Una serie di formati di output. Puoi specificare le seguenti valori:
 - **DHTML**: formato HTML dinamico
 - **HTML**: formato HTML statico
 - **XML**: formato XML
 - **CSV**: formato di valori separati da virgole
 - **Text**: formato di testo semplice
- **Interactive (boolean)**- Facoltativo. Se impostato su true, genera un rapporto interattivo. I report interattivi non possono essere modificati dopo la creazione.
- **ScheduleConfigurations (hashtable)**- Obbligatorio a meno che il rapporto non sia interattivo. Una tabella hash contenente la configurazione della pianificazione con le seguenti proprietà:
 - **Time (datetime)**: DateTime oggetto che specifica quando eseguire l'attività (obbligatorio)
 - **RunDuration (number)**: numero di ore di esecuzione dell'attività (opzionale)
 - **Weekly (array)**: matrice di giorni feriali (opzionale)
 - **Monthly (array)**: matrice di giorni del mese, da utilizzare -1 per l'ultimo giorno (opzionale)

Parametri specifici del rapporto:

- **FileScreenAuditDaysSince** (number)- Facoltativo. Per FileScreenAuditFiles i report, specifica quanti giorni fa includere gli eventi di controllo.
- **FileScreenAuditUser** (array)- Facoltativo. Per FileScreenAuditFiles i report, specifica una serie di account utente da includere nel rapporto. Verranno incluse solo le violazioni dello screening dei file da parte di questi utenti.
- **FileGroupIncluded** (array)- Facoltativo. Per FilesByFileGroup i report, specifica quali gruppi di file includere.
- **FileOwnerFilePattern** (string)- Facoltativo. Per i FilesByOwner report, specifica un modello di file per filtrare i risultati.
- **PropertyName** (string)- Facoltativo. Per i FilesByProperty report, specifica la proprietà di classificazione in base alla quale raggruppare.
- **FolderPropertyName** (string)- Facoltativo. Per i FoldersByProperty report, specifica la proprietà della cartella in base alla quale raggruppare.
- **PropertyFilePattern** (string)- Facoltativo. Per FilesByProperty and FoldersByProperty, specifica un modello di file per filtrare i risultati.
- **LargeFileMinimum** (number)- Facoltativo. Per i LargeFiles report, specifica la dimensione minima del file in byte.
- **LargeFilePattern** (string)- Facoltativo. Per i LargeFiles report, specifica un modello di file per filtrare i risultati.
- **LeastAccessedMinimum** (number)- Facoltativo. Per LeastRecentlyAccessed i report, specifica il numero minimo di giorni dall'ultimo accesso.
- **LeastAccessedFilePattern** (string)- Facoltativo. Per i LeastRecentlyAccessed report, specifica un modello di file per filtrare i risultati.
- **MostAccessedMaximum** (number)- Facoltativo. Per MostRecentlyAccessed i report, specifica il numero massimo di giorni dall'ultimo accesso.
- **MostAccessedFilePattern** (string)- Facoltativo. Per i MostRecentlyAccessed report, specifica un modello di file per filtrare i risultati.
- **QuotaMinimumUsage** (number)- Facoltativo. Per QuotaUsage i report, specifica la percentuale minima di utilizzo della quota da includere.

Esempi:

1. Crea un rapporto mensile sui file di grandi dimensioni.


```
$schedule = @{
    Time = ("3:00 AM")
    Monthly = @(1) # Run on first day
}

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {
    param($schedule)
    New-FSxFSRMStorageReport -Name "Monthly Large Files" -Namespace "share
\data" -ReportType "LargeFiles" -LargeFileMinimum 100MB -ReportFormat "HTML" -
ScheduleConfigurations $schedule
}
```

2. Crea un rapporto settimanale sui file duplicati con più namespace e formati.

```
$schedule = @{
    Time = ("12:00 AM")
    Weekly = @('Sunday')
    RunDuration = 4
}

$namespaces = @("share\docs", "[FolderUsage_MS=User Files]")
$reportFormats = @("HTML", "CSV")
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList @($schedule, $namespaces, $reportFormats) -ScriptBlock {
    param($schedule, $namespaces, $reportFormats)
    New-FSxFSRMStorageReport -Name "Weekly Duplicates" -Namespace $namespaces -
ReportType "DuplicateFiles" -ReportFormat $reportFormats -ScheduleConfigurations
$schedule
}
```

3. Crea un rapporto interattivo che viene eseguito immediatamente.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMStorageReport -Name "Find large files" -Namespace "share" -Interactive
$true -ReportType "QuotaUsage"
}
```

Ottieni un FSx FSRMStorage rapporto

Get- FSx FSRMStorage Report: recupera uno o più report di archiviazione dal file system. Restituisce dettagli sulle configurazioni e sullo stato dei report.

Parametri:

- Name (array)- Facoltativo. Una serie di nomi di report da recuperare. Se non si specifica un nome, il comando restituisce tutti i report di archiviazione sul file system.

Esempi:

1. Recupera tutti i report di archiviazione sul file system.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMStorageReport  
}
```

Rimuovi- FSx FSRMStorage Segnala

Rimuovi- FSx FSRMStorage Report: rimuove uno o più report di archiviazione dal file system. Non è possibile rimuovere i report attualmente in esecuzione.

Parametri:

- Name (array)- Obbligatorio. Una serie di nomi di report da rimuovere.
- PassThru (boolean)- Facoltativo. Se impostato su true, restituisce l'oggetto del report rimosso.

Esempi:

1. Rimuove un singolo report di archiviazione.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Remove-FSxFSRMStorageReport -Name "Monthly Report" -PassThru  
}
```

Set- FSx FSRMStorage Report

Parameters

- **Name (array)**- Richiesto. Una serie di nomi di report da modificare.
- **Namespace (array)**- Facoltativo. Una serie di percorsi o tipi di cartelle da analizzare. È possibile specificare percorsi in più formati:
 - Percorso della cartella
 - [Classificazione delle cartelle](#). Ad esempio, [FolderUsage_ms="File utente "]
- **ReportType (array)**- Facoltativo. Una serie di tipi di report da generare. Puoi specificare le seguenti valori:
 - **DuplicateFiles**: identifica i file duplicati in base alle dimensioni e al contenuto dei file
 - **FilesByFileGroup**: raggruppa i file in base all'appartenenza al gruppo di file
 - **FilesByOwner**: raggruppa i file per proprietario
 - **FilesByProperty**: raggruppa i file in base alla proprietà di classificazione
 - **FileScreenAuditFiles**: elenca le violazioni relative allo screening dei file
 - **FoldersByProperty**: raggruppa le cartelle in base alla proprietà di gestione
 - **LargeFiles**: elenca i file al di sopra di una soglia di dimensione specificata
 - **LeastRecentlyAccessed**: elenca i file a cui non è stato effettuato l'accesso di recente
 - **MostRecentlyAccessed**: elenca i file a cui è stato effettuato l'accesso di recente
 - **QuotaUsage**: mostra le statistiche sull'utilizzo delle quote
- **ReportFormat (array)**- Facoltativo. Una serie di formati di output. Puoi specificare le seguenti valori:
 - **DHTML**: formato HTML dinamico
 - **HTML**: formato HTML statico
 - **XML**: formato XML
 - **CSV**: formato di valori separati da virgole
 - **Text**: formato di testo semplice
- **ScheduleConfigurations (hashtable)**- Obbligatorio a meno che il rapporto non sia interattivo. Una tabella hash contenente la configurazione della pianificazione con le seguenti proprietà:

• **Time (datetime)**: DateTime oggetto che specifica quando eseguire l'attività (obbligatorio)

- **RunDuration (number)**: numero di ore di esecuzione dell'attività (opzionale)
- **Weekly (array)**: matrice di giorni feriali (opzionale)
- **Monthly (array)**: matrice di giorni del mese, da utilizzare -1 per l'ultimo giorno (opzionale)
- **PassThru (boolean)**- Facoltativo. Se impostato su true, restituisce l'oggetto del report modificato.

Parametri specifici del rapporto

- **FileScreenAuditDaysSince (number)**- Facoltativo. Per FileScreenAuditFiles i report, specifica quanti giorni fa includere gli eventi di controllo.
- **FileScreenAuditUser (array)**- Facoltativo. Per FileScreenAuditFiles i report, specifica una serie di account utente da includere nel rapporto. Verranno incluse solo le violazioni dello screening dei file da parte di questi utenti.
- **FileGroupIncluded (array)**- Facoltativo. Per FilesByFileGroup i report, specifica quali gruppi di file includere.
- **FileOwnerFilePattern (string)**- Facoltativo. Per i FilesByOwner report, specifica un modello di file per filtrare i risultati.
- **PropertyName (string)**- Facoltativo. Per i FilesByProperty report, specifica la proprietà di classificazione in base alla quale raggruppare.
- **FolderPropertyName (string)**- Facoltativo. Per i FoldersByProperty report, specifica la proprietà della cartella in base alla quale raggruppare.
- **PropertyFilePattern (string)**- Facoltativo. Per FilesByProperty and FoldersByProperty, specifica un modello di file per filtrare i risultati.
- **LargeFileMinimum (number)**- Facoltativo. Per i LargeFiles report, specifica la dimensione minima del file in byte.
- **LargeFilePattern (string)**- Facoltativo. Per i LargeFiles report, specifica un modello di file per filtrare i risultati.
- **LeastAccessedMinimum (number)**- Facoltativo. Per LeastRecentlyAccessed i report, specifica il numero minimo di giorni dall'ultimo accesso.
- **LeastAccessedFilePattern (string)**- Facoltativo. Per i LeastRecentlyAccessed report, specifica un modello di file per filtrare i risultati.
- **MostAccessedMaximum (number)**- Facoltativo. Per MostRecentlyAccessed i report, specifica il numero massimo di giorni dall'ultimo accesso.

- **MostAccessedFilePattern** (string)- Facoltativo. Per i **MostRecentlyAccessed** report, specifica un modello di file per filtrare i risultati.
- **QuotaMinimumUsage** (number)- Facoltativo. Per **QuotaUsage** i report, specifica la percentuale minima di utilizzo della quota da includere.

Esempi:

1. Aggiorna la pianificazione e il formato di un rapporto esistente.

```
$schedule = @{
    Time = ("3:00 AM")
    Monthly = @(1)
}
$reportFormats = @("HTML", "CSV")

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList @($schedule, $reportFormats) -ScriptBlock {
    param($schedule, $reportFormats)
    Set-FSxFSRMStorageReport -Name "Monthly Report" -ScheduleConfigurations $schedule -
ReportFormat $reportFormats -PassThru
}
```

Comandi di esecuzione dei report

Inizia - FSx FSRMStorage Segnala

Parameters

- **Name** (array)- Obbligatorio. Una serie di nomi di report per iniziare.
- **Queue** (boolean)- Facoltativo. Se impostato su true, aggiunge il rapporto a una coda da eseguire entro i prossimi 5 minuti. Tutti i report in coda durante questo periodo verranno eseguiti contemporaneamente. Se impostato su false o non specificato, il rapporto viene avviato immediatamente.
- **RunDuration** (number)- Facoltativo. Specifica per quante ore deve essere eseguito il rapporto prima di essere annullato. Valori validi: da -1 a 2147483. Valori speciali:
 - 0: Esegui fino al completamento
 - -1: Esegui fino all'annullamento

Se non specificato, viene eseguito fino al completamento.

Esempi

1. Avvia immediatamente un rapporto di archiviazione.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Start-FSxFSRMStorageReport -Name "Monthly Report"  
}
```

2. Metti in coda un rapporto di archiviazione con un limite di durata.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Start-FSxFSRMStorageReport -Name "Quarterly Report" -Queue: $true -RunDuration 4  
}
```

Stop - Segnala FSx FSRMStorage

Parameters

- Name (array)- Obbligatorio. Una serie di nomi di report da interrompere.

Esempi:

1. Interrompere un singolo report di archiviazione.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Stop-FSxFSRMStorageReport -Name "Monthly Report"  
}
```

Attendi- FSx FSRMStorage Segnala

Parameters

- Name (array)- Richiesto. Una serie di nomi di report da attendere.
- Timeout (number)- Facoltativo. Specificate il tempo di attesa, in secondi, per il completamento dei report. Se il timeout scade prima del termine dei report, il comando viene restituito ma la generazione dei report continua a essere eseguita in background. Valori validi: da -1 a 2147483. Valori speciali:

- -1: Attendi indefinitamente il completamento dei report (impostazione predefinita)
- 0: Controlla lo stato attuale e torna immediatamente senza aspettare

Esempi:

1. Attendi a tempo indeterminato il completamento di un rapporto di archiviazione.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Wait-FSxFSRMStorageReport -Name "Monthly Report"  
}
```

Attività di gestione dei file

Amazon FSx for Windows File Server non supporta le attività di gestione dei file FSRM. Tuttavia, è possibile ottenere casi d'uso comuni come le politiche di archiviazione e conservazione dei dati utilizzando PowerShell comandi nativi provenienti da macchine client che hanno accesso in rete al file system.

Ad esempio, è possibile utilizzare PowerShell gli script sui computer client per:

- Spostare o archiviare i file in base all'età o all'ora dell'ultimo accesso
- Eliminare i file classificati che superano un periodo di conservazione
- Copia i file nell'archivio di archiviazione in base alle proprietà di classificazione

È possibile accedere alle proprietà dei file utilizzando il `Get-FsrmClassification` comando e intraprendere azioni in base ai valori.

Per accedere alle proprietà di classificazione FSRM o ad altri metadati FSRM dagli PowerShell script lato client, sul computer client deve essere installato anche FSRM.

Impostazioni FSRM

Le impostazioni FSRM forniscono una configurazione a livello di sistema che consente di personalizzare il comportamento e semplificare la gestione delle funzionalità. Utilizzate queste impostazioni per controllare il funzionamento di FSRM nel file system e per impostare valori predefiniti che semplificano la creazione e la configurazione di funzionalità come i report di archiviazione e lo screening dei file.

Categorie di impostazioni

Le impostazioni FSRM sono organizzate in tre categorie:

Controllo dello schermo dei file

Il controllo delle schermate dei file registra quando gli utenti tentano di salvare file bloccati dalle schermate di file attive. Queste informazioni sono essenziali per monitorare la conformità alle politiche di screening dei file e identificare gli utenti che tentano frequentemente di salvare tipi di file non autorizzati.

- `ReportFileScreenAuditEnable`- Questa impostazione controlla se FSRM registra o meno le violazioni dello screening dei file. Se disattivata, FSRM non registra le violazioni dello schermo dei file e i `FileScreenAuditFiles` report non avranno dati da visualizzare. È necessario abilitare questa impostazione per utilizzare i report di controllo delle schermate dei file.
- `ReportFileScreenAuditDaysSince`- Questa impostazione fornisce l'intervallo di tempo predefinito per i report di controllo delle schermate dei file. Quando si crea un `FileScreenAuditFiles` report senza specificare a che distanza deve apparire, FSRM utilizza questo valore. L'impostazione di un'impostazione predefinita appropriata (ad esempio 30 giorni) garantisce che i report si concentrino sulle violazioni recenti senza includere dati storici eccessivi.
- `ReportFileScreenAuditUser`- Questa impostazione fornisce l'elenco predefinito di utenti da includere nei rapporti di controllo della schermata dei file. Quando si crea un `FileScreenAuditFiles` rapporto senza specificare quali utenti includere, FSRM utilizza questo elenco. Se vuoti, i report includono tutti gli utenti per impostazione predefinita. È possibile utilizzare questa impostazione per concentrare i report su gruppi di utenti o reparti specifici.

Filtri di report predefiniti

Le impostazioni predefinite del filtro dei report forniscono i valori che vengono utilizzati quando si creano report di archiviazione senza specificare determinati parametri. Queste impostazioni predefinite semplificano la creazione di report e garantiscono la coerenza tra report simili.

A ogni tipo di report sono associate impostazioni predefinite:

- Report con file di grandi dimensioni: `ReportLargeFileMinimum` imposta la dimensione minima predefinita del file e `ReportLargeFilePattern` imposta il filtro predefinito per il modello di file.

- Rapporti sui file con meno accesso: `ReportLeastAccessedMinimum` imposta il numero predefinito di giorni dall'ultimo accesso e `ReportLeastAccessedFilePattern` imposta il filtro predefinito per i modelli di file.
- Report sui file con più accesso: `ReportMostAccessedMaximum` imposta il numero massimo predefinito di giorni dall'ultimo accesso e `ReportMostAccessedFilePattern` imposta il filtro predefinito del modello di file.
- Rapporti relativi ai file per proprietario: `ReportFileOwnerFilePattern` imposta il filtro predefinito per lo schema dei file e `ReportFileOwnerUser` l'elenco predefinito degli utenti da includere.
- Rapporti relativi ai file per proprietà: `ReportPropertyName` imposta la proprietà di classificazione predefinita da analizzare e `ReportPropertyFilePattern` imposta il filtro predefinito del modello di file.
- Rapporti relativi ai gruppi di file: `ReportFileGroupIncluded` imposta l'elenco predefinito dei gruppi di file da includere.
- Rapporti sull'utilizzo delle quote: `ReportQuotaMinimumUsage` imposta la percentuale minima predefinita di utilizzo delle quote.

Quando si crea un rapporto, è possibile sovrascrivere qualsiasi di questi valori predefiniti specificando il parametro in modo esplicito nella configurazione del rapporto. Le impostazioni predefinite globali si applicano solo quando non si specifica un valore.

Limiti dei report

Le impostazioni dei limiti dei report controllano il numero massimo di elementi da includere nei report di archiviazione. Questi limiti servono a due scopi:

1. Gestione delle prestazioni: la limitazione del numero di elementi nei report impedisce che i report impieghino troppo tempo a generare o consumino risorse di sistema eccessive. Il completamento di report di grandi dimensioni che analizzano milioni di file può richiedere ore e influire sulle prestazioni del sistema.
2. Usabilità dei report: i report con migliaia di voci sono difficili da rivedere e analizzare. I limiti dei report garantiscono che i report rimangano incentrati sui dati più pertinenti.

Puoi impostare un controllo granulare sui limiti dei report:

- Limiti generali: `ReportLimitMaxFile` limita il numero totale di file in ogni rapporto, indipendentemente dal tipo.
- Per-report-type limiti: impostazioni come `ReportLimitMaxFileGroup` e `ReportLimitMaxPropertyValue` limita il numero di gruppi, proprietari o valori di proprietà da includere in tipi di report specifici. `ReportLimitMaxOwner`
- Limiti per gruppo: impostazioni come `ReportLimitMaxFilesPerFileGroup`, `ReportLimitMaxFilesPerOwner`, e `ReportLimitMaxFilesPerPropertyValue` limita il numero di file da mostrare all'interno di ciascun gruppo del rapporto.

Quando un report raggiunge un limite, FSRM include gli elementi che occupano più spazio di archiviazione o che sono più pertinenti al tipo di rapporto e indica nel rapporto che il limite è stato raggiunto.

Comandi di impostazione FSRM

È possibile accedere ai comandi per il recupero e la modifica delle impostazioni globali. Utilizzate questi comandi per configurare il comportamento FSRM a livello di sistema.

Elenco dei comandi remoti delle impostazioni FSRM FSx PowerShell

Note

Tutti gli esempi in questa pagina presuppongono che la `$FSxWindowsRemotePowerShellEndpoint` variabile sia stata definita con l'endpoint Windows Remote PowerShell del file system. Puoi trovare questo endpoint nella FSx console Amazon nella pagina dei dettagli del tuo file system o utilizzando il AWS CLI `describe-file-systems` comando.

Ottieni- FSx FSRMSetting

`Get-FSxFSRMSetting`: recupera le impostazioni correnti del File Server Resource Manager sul file system. Restituisce solo le impostazioni che possono essere modificate utilizzando `Set-FSxFSRMSetting`.

Parametri:

Nessuno

Esempi:

1. Recupera tutte le impostazioni FSRM correnti.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
  FSxRemoteAdmin -ScriptBlock {  
  Get-FSxFSRMSetting  
  }
```

Imposta- FSx FSRMSetting

Set-FSxFSRMSetting: modifica le impostazioni globali di File Server Resource Manager sul file system. Queste impostazioni forniscono valori predefiniti per i report di archiviazione e controllano il comportamento FSRM.

Parametri:

Impostazioni di controllo della schermata dei file:

- **ReportFileScreenAuditEnable (boolean)**- Facoltativo. Controlla se gli eventi di controllo dello screening dei file sono inclusi nei report FSRM.
- **ReportFileScreenAuditDaysSince (number)**- Facoltativo. Il numero predefinito di giorni per verificare eventuali violazioni dello screening dei file durante la generazione dei FileScreenAuditFiles report.
- **ReportFileScreenAuditUser (array)**- Facoltativo. Una matrice dell'elenco predefinito di account utente da includere nei FileScreenAuditFiles report.

Impostazioni predefinite del filtro dei report:

- **ReportFileGroupIncluded (array)**- Facoltativo. Una matrice di nomi di gruppi di file da includere nei report per impostazione predefinita.
- **ReportFileOwnerFilePattern (string)**- Facoltativo. Lo schema di file predefinito per i report dei file in base ai proprietari. Supporta i caratteri jolly (*e?).
- **ReportFileOwnerUser (array)**- Facoltativo. Una serie di utenti in formato Domain\ User per i report dei file ordinati dai proprietari.
- **ReportLargeFileMinimum (number)**- Facoltativo. La dimensione minima predefinita del file in byte per i report con file di grandi dimensioni.

- `ReportLargeFilePattern (string)`- Facoltativo. Lo schema di file predefinito per report con file di grandi dimensioni. Supporta i caratteri jolly (*e?).
- `ReportLeastAccessedFilePattern (string)`- Facoltativo. Lo schema di file predefinito per i report sui file a cui si accede meno. Supporta i caratteri jolly (*e?).
- `ReportLeastAccessedMinimum (number)`- Facoltativo. Il numero minimo predefinito di giorni dall'ultimo accesso per i report sui file a cui si accede meno.
- `ReportMostAccessedFilePattern (string)`- Facoltativo. Lo schema di file predefinito per la maggior parte dei report sui file a cui si accede. Supporta i caratteri jolly (*e?).
- `ReportMostAccessedMaximum (number)`- Facoltativo. Il numero massimo predefinito di giorni dall'ultimo accesso per la maggior parte dei report sui file a cui si accede.
- `ReportPropertyFilePattern (string)`- Facoltativo. Il modello di file predefinito per i report sulle proprietà. Supporta i caratteri jolly (*e?).
- `ReportPropertyName (string)`- Facoltativo. Il nome di proprietà predefinito per i report sulle proprietà.
- `ReportQuotaMinimumUsage (number)`- Facoltativo. La percentuale minima predefinita di utilizzo delle quote per i report sull'utilizzo delle quote.

Impostazioni dei limiti dei report:

- `ReportLimitMaxDuplicateGroup (number)`- Facoltativo. Il numero massimo di gruppi di file duplicati da includere nei report sui file duplicati.
- `ReportLimitMaxFile (number)`- Facoltativo. Il numero massimo di file da includere nei report di archiviazione.
- `ReportLimitMaxFileGroup (number)`- Facoltativo. Il numero massimo di gruppi di file da includere nei report.
- `ReportLimitMaxFileScreenEvent (number)`- Facoltativo. Il numero massimo di eventi relativi alla schermata dei file da includere nei rapporti di controllo delle schermate dei file.
- `ReportLimitMaxFilesPerDuplicateGroup (number)`- Facoltativo. Il numero massimo di file per gruppo duplicato nei report sui file duplicati.
- `ReportLimitMaxFilesPerFileGroup (number)`- Facoltativo. Il numero massimo di file per gruppo di file nei report file per gruppo di file.
- `ReportLimitMaxFilesPerOwner (number)`- Facoltativo. Il numero massimo di file per proprietario nei rapporti File per proprietario.

- `ReportLimitMaxFilesPerPropertyValue (number)`- Facoltativo. Il numero massimo di file per valore di proprietà nei file per rapporto sulle proprietà.
- `ReportLimitMaxOwner (number)`- Facoltativo. Il numero massimo di proprietari da includere nei file in base ai report dei proprietari.
- `ReportLimitMaxPropertyValue (number)`- Facoltativo. Il numero massimo di valori di proprietà da includere nei file in base ai report sulle proprietà.
- `ReportLimitMaxQuota (number)`- Facoltativo. Il numero massimo di quote da includere nei report sull'utilizzo delle quote.

Altre impostazioni:

- `PassThru (boolean)`- Facoltativo. Se impostato su `true`, restituisce l'oggetto delle impostazioni modificate.

Esempi:

1. Configura il controllo predefinito dello schermo dei file con una cronologia di 30 giorni.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Set-FSxFSRMSetting -ReportFileScreenAuditDaysSince 30 -PassThru  
}
```

2. Configura le impostazioni predefinite per i report su file di grandi dimensioni.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Set-FSxFSRMSetting -ReportLargeFileMinimum 100MB -ReportLargeFilePattern "*.iso"  
    -PassThru  
}
```

Registri eventi

Quando abiliti FSRM sul tuo file system, AWS FSx per Windows File Server genera registri degli eventi per le attività di gestione dei file e li invia alla destinazione configurata (AWS CloudWatch Logs o Kinesis Data AWS Firehose). Questi registri consentono di monitorare le operazioni FSRM, risolvere i problemi e mantenere gli audit trail delle attività di gestione dei file.

Quali registri FSRM

Quando si abilita FSRM sul file system, AWS FSx per Windows File Server registra gli eventi e li invia alla destinazione configurata. Verranno registrati i seguenti eventi:

- Violazioni relative allo screening dei file: quando gli utenti tentano di salvare file monitorati da schermate di file che prevedono azioni di notifica degli eventi
- Notifiche sulle soglie di quota: quando l'utilizzo delle quote raggiunge le soglie configurate che prevedono azioni di notifica degli eventi
- Eventi del servizio FSRM: conferma delle impostazioni di notifica, degli errori di servizio e degli errori operativi

Accesso ai registri FSRM

La posizione in cui si accede ai registri FSRM dipende dalla destinazione configurata durante l'attivazione di FSRM:

CloudWatch Registri

Visualizza i log nella console CloudWatch Logs accedendo al gruppo di log specificato. È possibile cercare, filtrare e analizzare i log utilizzando CloudWatch Logs Insights e impostare CloudWatch allarmi per notificare eventi specifici.

Kinesis Data Firehose

I log vengono consegnati alla destinazione configurata nel flusso di distribuzione di Kinesis Data Firehose, ad esempio Amazon S3 AWS , Redshift o Service. AWS OpenSearch Puoi elaborare e analizzare i log utilizzando gli strumenti e i servizi integrati nel tuo flusso di distribuzione.

Casi di utilizzo comune

Questo argomento fornisce step-by-step esempi di attività comuni di File Server Resource Manager. Questi esempi dimostrano come utilizzare e implementare le funzionalità FSRM per risolvere le problematiche tipiche della gestione dei file.

Note

Tutti gli esempi in questa pagina presuppongono che la `$FSxWindowsRemotePowerShellEndpoint` variabile sia stata definita con l'endpoint

Windows Remote PowerShell del file system. Puoi trovare questo endpoint nella FSx console Amazon nella pagina dei dettagli del tuo file system o utilizzando il AWS CLI `describe-file-systems` comando.

Impostazione di una quota fissa su una cartella

Questo esempio mostra come creare una quota fissa che impedisca agli utenti di archiviare più di 10 GB in una cartella «reparto».

Per impostare una quota su una cartella:

1. Crea una quota fissa con un limite di 10 GB:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMQuota -Folder "share\department" -Size 10GB -Description "10 GB hard
limit for department folder"
}
```

2. (Facoltativo) Modifica la quota per aggiungere una notifica di soglia con un utilizzo dell'85%:

```
$thresholds = [System.Collections.ArrayList]@()
$threshold = @{
    ThresholdPercentage = 85
    Action = @(
        @{
            ActionType = "Event"
            EventType = "Warning"
            MessageBody = "Department folder has reached 85% of quota limit"
        }
    )
}

$null = $thresholds.Add($threshold)

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
FSxRemoteAdmin -ArgumentList ($thresholds) -ScriptBlock {
    param($thresholds)
    Set-FSxFSRMQuota -Folder "share\department" -ThresholdConfigurations
$Using:thresholds
}
```

3. Verifica che la quota sia stata creata:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
  FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMQuota -Folder "share\department"  
  }
```

Limitazione di tipi di file specifici utilizzando gruppi di file

Questo esempio mostra come impedire agli utenti di salvare file audio e video in una cartella di documenti aziendali utilizzando il gruppo di file Audio and Video Files "" predefinito.

Per limitare i tipi di file utilizzando gruppi di file:

1. Crea una schermata di file attiva che blocchi i file audio e video:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
  FSxRemoteAdmin -ScriptBlock {  
    New-FSxFSRMFileScreen -Folder "share\business-documents" -IncludeGroup "Audio and  
    Video Files" -Description "Block media files in business documents folder"  
  }
```

2. (Facoltativo) Aggiorna la schermata dei file per aggiungere una notifica quando gli utenti tentano di salvare file bloccati:

```
$notifications = [System.Collections.ArrayList]@()  
  
$eventNotification = @{  
    ActionType = "Event"  
    EventType = "Warning"  
    MessageBody = "User attempted to save blocked media file"  
}  
$null = $notifications.Add($eventNotification)  
  
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
  FSxRemoteAdmin -ArgumentList $notifications -ScriptBlock {  
    param($notifications)  
    Set-FSxFSRMFileScreen -Folder "share\business-documents" -  
    NotificationConfigurations $Using:notifications  
  }
```


3. Verifica che la schermata dei file sia stata creata:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
  FSxRemoteAdmin -ScriptBlock {
    Get-FSxFSRMFileScreen -Folder "share\business-documents"
  }
```

Identifica e classifica i dati PII

Questo esempio mostra come identificare automaticamente i file contenenti numeri di previdenza sociale e classificarli come contenenti informazioni di identificazione personale (PII).

Per identificare e classificare i dati PII:

1. Crea una proprietà di classificazione per PII:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
  FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationPropertyDefinition -Name "ContainsPII" -Type
    OrderedList -PossibleValueConfigurations @(
      @{ Name = "Yes" },
      @{ Name = "No" })
  }
```

2. Crea una regola di classificazione per rilevare i numeri di previdenza sociale:

Note

La seguente espressione regolare cercherà nei file il testo con lo schema XXX-XX-XXXX. Per l'uso in produzione, prendete in considerazione l'utilizzo di modelli più sofisticati o la combinazione di più metodi di rilevamento.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
  FSxRemoteAdmin -ScriptBlock {
    New-FSxFSRMClassificationRule -Name "Detect_SSN" -Property "ContainsPII"
    -PropertyValue "Yes" -Namespace "share" -ClassificationMechanism "Content
    Classifier" -ContentRegularExpression "\b\d{3}-\d{2}-\d{4}\b"
  }
```

3. Esegui la classificazione:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Start-FSxFSRMClassification  
}
```

4. (Facoltativo) Configura la classificazione continua per classificare automaticamente i nuovi file:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Set-FSxFSRMClassification -Continuous $true  
}
```

5. Verifica lo stato (1 significa completato):

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMClassification  
}
```

6. Al termine della classificazione, è possibile visualizzare le proprietà di classificazione assegnate ai file facendo clic con il pulsante destro del mouse su un file in Esplora file di Windows, selezionando Proprietà e scegliendo la scheda Classificazione. Questa scheda mostra tutte le proprietà di classificazione e i relativi valori per il file.

Creazione di una politica di conservazione per i file

Questo esempio mostra come classificare i file in base al periodo di conservazione in base alla posizione della cartella, che è quindi possibile utilizzare con PowerShell script lato client per archiviare o eliminare i file.

Per creare una politica di conservazione dei file:

1. Crea una proprietà di classificazione per il periodo di conservazione:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    New-FSxFSRMClassificationPropertyDefinition -Name "RetentionPeriod" -Type  
    String -Description "File retention period"
```

```
}
```

2. Crea regole di classificazione per diversi periodi di conservazione:

- Conservazione di 7 anni per i documenti legali nella cartella Documenti legali:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -  
ConfigurationName FSxRemoteAdmin -ScriptBlock {  
    New-FSxFSRMClassificationRule -Name "Legal_7Year" -Property  
    "RetentionPeriod" -PropertyValue "7 years" -Namespace "share/Legal Documents" -  
    ClassificationMechanism "Folder Classifier"  
}
```

- Conservazione di 3 anni per i registri finanziari nella cartella Finanza:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -  
ConfigurationName FSxRemoteAdmin -ScriptBlock {  
    New-FSxFSRMClassificationRule -Name "Finance_3Year" -Property  
    "RetentionPeriod" -PropertyValue "3 years" -Namespace "share/Finance" -  
    ClassificationMechanism "Folder Classifier"  
}
```

Puoi anche classificare per contenuto del file e cercare stringhe come «Periodo di conservazione: sette anni». Per raggiungere questo obiettivo, usa `and`.
`ClassificationMechanism "Content Classifier" ContentString "Retention seven years"`

3. Esegui la classificazione per applicare le proprietà di conservazione:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Start-FSxFSRMClassification  
}
```

4. (Facoltativo) Configura la classificazione continua per classificare automaticamente i nuovi file:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Set-FSxFSRMClassification -Continuous $true  
}
```

5. Verifica lo stato (1 significa completato):

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Get-FSxFSRMClassification  
}
```

6. Al termine della classificazione, è possibile visualizzare le proprietà di classificazione assegnate ai file facendo clic con il pulsante destro del mouse su un file in Esplora file di Windows, selezionando Proprietà e scegliendo la scheda Classificazione. Questa scheda mostra tutte le proprietà di classificazione e i relativi valori per il file.
7. Una volta classificati i file in base ai periodi di conservazione, è possibile utilizzare PowerShell script lato client per archiviare o eliminare i file in base alla loro *RetentionPeriod* proprietà e alla loro età. Ad esempio, è possibile eseguire la scansione del file system e confrontare l'età dei file con la classificazione del periodo di conservazione. Per ulteriori informazioni, consulta [Attività di gestione dei file](#).

Configurazione di report di archiviazione comuni

Questa sezione mostra come creare due report di archiviazione di uso comune: un report sui file di grandi dimensioni e un rapporto sui file per proprietario.

Rapporto su file di grandi dimensioni

Questo esempio crea un rapporto mensile che identifica i file di dimensioni superiori a 200 MB.

Per creare un rapporto su file di grandi dimensioni:

1. Crea un rapporto pianificato su file di grandi dimensioni:

```
$schedule = @{  
    Time = "2:00 AM"  
    Monthly = @(1) # Run on the 1st of each month  
}  
  
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {  
    param($schedule)  
    New-FSxFSRMStorageReport -Name "Monthly Large Files Report" -Namespace "share"  
    -ReportType "LargeFiles" -LargeFileMinimum 200MB -ReportFormat "HTML","CSV" -  
    ScheduleConfigurations $schedule
```

```
}
```

2. (Facoltativo) Esegui immediatamente il rapporto per testare:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Start-FSxFSRMStorageReport -Name "Monthly Large Files Report"  
}
```

Rapporto «File per proprietario»

Questo esempio crea un rapporto settimanale che mostra il consumo di storage per utente.

Per creare un rapporto sui file in base al proprietario:

1. Crea un rapporto pianificato relativo ai file per proprietario:

```
$schedule = @{  
    Time = "3:00 AM"  
    Weekly = @('Sunday')  
}  
  
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ArgumentList $schedule -ScriptBlock {  
    param($schedule)  
    New-FSxFSRMStorageReport -Name "Weekly Files by Owner Report" -  
    Namespace "share" -ReportType "FilesByOwner" -ReportFormat "HTML","CSV" -  
    ScheduleConfigurations $schedule  
}
```

2. (Facoltativo) Esegui immediatamente il rapporto per testare:

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName  
FSxRemoteAdmin -ScriptBlock {  
    Start-FSxFSRMStorageReport -Name "Weekly Files by Owner Report"  
}
```

Accedi ai report generati mappando la condivisione amministrativa D\$. Per ulteriori informazioni, consulta [Accesso ai report di archiviazione](#).

Gestione dello storage FSx su Windows File Server

La configurazione di storage del file system include la quantità di capacità di storage assegnata, il tipo di storage e, se il tipo di storage è un'unità a stato solido (SSD), la quantità di IOPS SSD. È possibile configurare queste risorse, insieme alla capacità di throughput del file system, durante la creazione di un file system e dopo la sua creazione, per ottenere le prestazioni desiderate per il carico di lavoro. Scopri come gestire lo storage del tuo file system e le prestazioni correlate allo storage utilizzando Amazon FSx CLI per la gestione remota PowerShell esplorando i seguenti argomenti. Console di gestione AWS AWS CLI

Argomenti

- [Ottimizzazione dei costi di archiviazione](#)
- [Gestione della capacità di storage](#)
- [Gestione del tipo di storage del file system](#)
- [Gestione degli IOPS SSD](#)
- [Riduzione dei costi di storage con la deduplicazione dei dati](#)
- [Gestione delle quote di archiviazione](#)
- [Aumento della capacità di archiviazione del file system](#)
- [Monitoraggio dell'aumento della capacità di archiviazione](#)
- [Aumento dinamico della capacità di archiviazione di un file system FSx per Windows File Server](#)
- [Aggiornamento del tipo di archiviazione di un file system FSx per Windows](#)
- [Monitoraggio degli aggiornamenti dei tipi di archiviazione](#)
- [Aggiornamento degli IOPS SSD di un file system](#)
- [Monitoraggio degli aggiornamenti IOPS degli SSD forniti](#)
- [Gestione della deduplicazione dei dati](#)
- [Risoluzione dei problemi di deduplicazione dei dati](#)

Ottimizzazione dei costi di archiviazione

Puoi ottimizzare i costi di storage utilizzando le opzioni di configurazione dello storage disponibili in Windows. FSx

Opzioni relative ai tipi di archiviazione: FSx per Windows File Server offre due tipi di storage, unità disco rigido (HDD) e unità a stato solido (SSD), per consentire l'ottimizzazione in base cost/

performance alle esigenze di carico di lavoro. L'archiviazione HDD è pensata per un ampio spettro di carichi di lavoro, che comprende home directory, condivisioni tra utenti e dipartimenti, nonché sistemi per la gestione dei contenuti. L'archiviazione SSD è progettata per i carichi di lavoro più performanti e sensibili alla latenza, inclusi database, carichi di lavoro di elaborazione multimediale e applicazioni di analisi dei dati. Per ulteriori informazioni sui tipi di storage e sulle prestazioni del file system, vedere.

[FSx per le prestazioni di Windows File Server](#)

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 utente 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. È possibile ridurre i costi di archiviazione dei dati attivando la deduplicazione dei dati per il 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 FSx file system Amazon, consulta. [Riduzione dei costi di storage con la deduplicazione dei dati](#)

Gestione della capacità di storage

È possibile aumentare la capacità di storage del file system FSx per Windows man mano che i requisiti di archiviazione cambiano. Puoi farlo utilizzando la FSx console Amazon, l' FSx API Amazon o AWS Command Line Interface (AWS CLI). I fattori da considerare quando si pianifica un aumento della capacità di storage includono sapere quando è necessario aumentare la capacità di storage, comprendere in che modo Amazon FSx elabora gli aumenti di capacità di storage e monitorare lo stato di avanzamento di una richiesta di aumento dello storage. Puoi solo aumentare la capacità di storage di un file system, non puoi ridurla.

Note

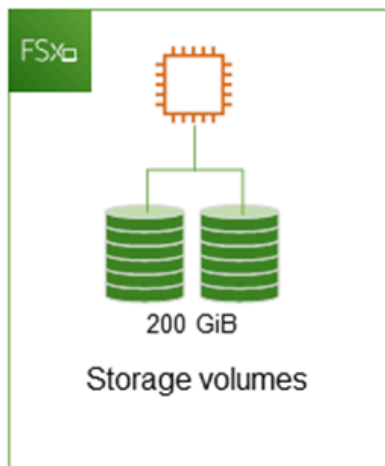
Non è possibile aumentare la capacità di archiviazione per i file system creati prima del 23 giugno 2019 o per i file system ripristinati da un backup appartenente a un file system creato prima del 23 giugno 2019.

Quando aumenti la capacità di archiviazione del tuo FSx file system Amazon, Amazon FSx aggiunge un nuovo set di dischi più grande al tuo file system dietro le quinte. Amazon esegue FSx 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 diversi

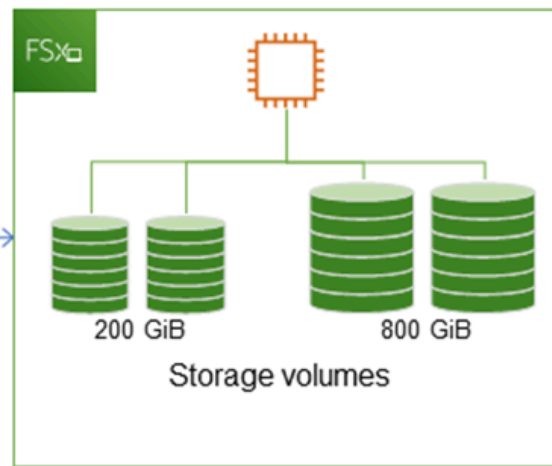
giorni, a seconda del tipo di storage e di altri fattori, con un impatto minimo evidente sulle prestazioni del carico di lavoro. Durante questa ottimizzazione, l'utilizzo del backup è temporaneamente maggiore, poiché sia i vecchi che i nuovi volumi di storage sono inclusi nei backup a livello di file 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 FSx utilizzato da Amazon per aumentare la capacità di storage di un file system.

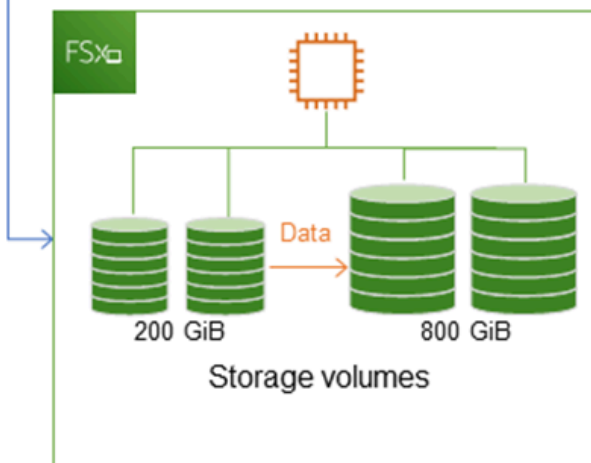
Step 1: Storage capacity increase request to 800 GiB.



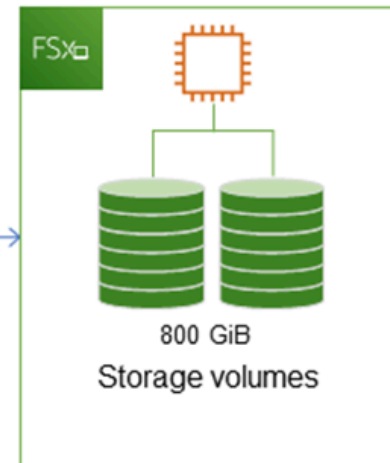
Step 2: Amazon FSx adds the new, larger disks.



Step 3: Amazon FSx migrates data to larger disks.



Step 4: Amazon FSx removes smaller disks.



Puoi monitorare i progressi dell'ottimizzazione dello storage, gli aumenti della capacità di archiviazione 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](#).

Cosa sapere sull'aumento della capacità di storage di un file system

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 storage, un file system deve avere una capacità di throughput minima di 16. MBps. 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 delle prestazioni del disco I/O . 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 raccomandazioni sulle prestazioni](#).

Sapere quando aumentare la capacità di archiviazione

Aumenta la capacità di storage del file system quando la capacità di storage disponibile sta per esaurirsi. Utilizza la `FreeStorageCapacity` CloudWatch metrica per monitorare la quantità di spazio di archiviazione gratuito disponibile sul file system. Puoi creare un CloudWatch allarme Amazon in base a questa metrica e ricevere una notifica quando scende al di sotto di una soglia specifica. Per ulteriori informazioni, consulta [Monitoraggio con Amazon CloudWatch](#).

Ti consigliamo di mantenere sempre almeno il 20% 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 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. Tuttavia, i file system con tipo di storage HDD e carichi di lavoro 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 potrebbero subire temporaneamente una riduzione delle prestazioni. In questi casi, si consiglia di aumentare innanzitutto la capacità di throughput del file system prima di aumentare la capacità di archiviazione. Per questi tipi di carichi di lavoro, consigliamo inoltre di modificare la capacità di throughput durante i periodi di inattività, quando il carico sul file system è minimo. 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](#).

Gestione del tipo di storage del file system

È possibile modificare il tipo di storage del file system da HDD a SSD utilizzando and. Console di gestione AWS AWS CLI Quando modifichi il tipo di archiviazione in SSD, 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, consigliamo di aggiornare il tipo di archiviazione quando il traffico sul file system è minimo. Per ulteriori informazioni, consulta [Aggiornamento del tipo di archiviazione di un file system FSx per Windows](#).

Non puoi modificare il tipo di storage del file system da SSD a HDD. Se desideri modificare il tipo di archiviazione di un file system da SSD a HDD, dovrai ripristinare un backup del file system su un nuovo file system configurato per utilizzare l'archiviazione su HDD. Per ulteriori informazioni, consulta [Ripristino dei backup su un nuovo file system](#).

Informazioni sui tipi di storage

È possibile configurare il file system FSx per Windows File Server in modo che utilizzi il tipo di archiviazione su unità a stato solido (SSD) o su disco rigido magnetico (HDD).

Lo storage SSD è appropriato per la maggior parte dei carichi di lavoro di produzione con 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.

Lo storage su HDD è progettato per un'ampia gamma di carichi di lavoro, tra cui home directory, condivisioni di file tra utenti e dipartimenti e sistemi di gestione dei contenuti. Lo storage su HDD ha un costo inferiore rispetto allo storage SSD, ma presenta 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 I/O requisiti bassi, 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](#).

Gestione degli IOPS SSD

Per i file system configurati con l'archiviazione SSD, la quantità di IOPS SSD determina la quantità di disco I/O disponibile quando il file system deve leggere e scrivere dati su disco, a differenza dei dati che si trovano nella cache. È possibile selezionare e scalare la quantità di IOPS SSD 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 selezionata 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 ottenere quel livello di IOPS SSD. Per ulteriori informazioni, consultare [FSx per le prestazioni di Windows File Server](#) e [Gestione della capacità di throughput](#).

Ecco alcuni elementi importanti da sapere sull'aggiornamento degli IOPS SSD forniti da un file system:

- Scelta di una modalità IOPS: sono disponibili due modalità IOPS tra cui scegliere:

- **Automatico:** scegli questa modalità e Amazon FSx ridimensionerà 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:** scegli questa modalità in modo da poter specificare il numero di IOPS SSD nell'intervallo compreso tra 96 e 400.000. Specificare un numero compreso tra 3 e 50 IOPS per GiB di capacità di storage per tutti i paesi in cui Regioni AWS Amazon FSx è disponibile 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 si sceglie la modalità di provisioning dall'utente e la quantità di IOPS SSD specificata non è di 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 archiviazione:** se aumenti la capacità di storage del file system e tale quantità richiede per impostazione predefinita una quantità di IOPS SSD superiore al livello di IOPS SSD attualmente fornito dall'utente, Amazon passa FSx automaticamente il file system alla modalità Automatica e il file system avrà un minimo di 3 IOPS SSD per GiB di capacità di storage.
- **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, FSx Amazon passa automaticamente il file system alla modalità Automatica.
- **Aumento della frequenza degli IOPS SSD:** non è possibile effettuare ulteriori aumenti degli IOPS SSD, aumentare la capacità di throughput o aggiornare il tipo di storage su un file system fino a 6 ore dopo la richiesta dell'ultimo 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

Si noti che i livelli di capacità di throughput pari o superiori a 4.608 MBps sono supportati solo nei seguenti paesi Regioni AWS: 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 su come aggiornare la quantità di IOPS SSD assegnati per il file system per Windows File Server, consulta. FSx [Aggiornamento degli IOPS SSD di un file system](#)

Riduzione dei costi di storage con la deduplicazione dei dati

La deduplicazione dei dati, spesso denominata in breve Dedup, aiuta gli amministratori di storage a ridurre i costi associati alla duplicazione dei dati. Con FSx for Windows File Server, puoi utilizzare 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.

Esempio:

- Le condivisioni di file degli utenti possono avere molte copie dello stesso file o di file simili.
- Le condivisioni di sviluppo software possono avere molti file binari che rimangono invariati da una build all'altra.

È possibile ridurre i costi di archiviazione dei dati abilitando 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. Quando si abilita la deduplicazione dei dati, la compressione dei dati è abilitata per impostazione predefinita, comprimendo i dati dopo la deduplicazione per ulteriori risparmi. La deduplicazione dei dati ottimizza le ridondanze senza compromettere la fedeltà o l'integrità dei dati. 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 per cento per i documenti degli utenti al 70-80 per cento per i set di dati di sviluppo software. È possibile misurare i potenziali risparmi derivanti dalla deduplicazione utilizzando il comando remoto descritto di seguito. `Measure-FSxDedupFileMetadata PowerShell`

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. `Get-FSxDedupStatus`

Per informazioni sulla configurazione della deduplicazione dei dati sul file system, vedere. [Gestione della deduplicazione dei dati](#)

Per informazioni sulla risoluzione dei problemi relativi alla deduplicazione dei dati, vedere.

Utilizza le seguenti informazioni per risolvere alcuni problemi comuni relativi alla configurazione e all'utilizzo della deduplicazione dei dati.

Argomenti

- [La deduplicazione dei dati non funziona](#)
- [I valori di deduplicazione sono inaspettatamente impostati su 0](#)
- [Dopo l'eliminazione dei file non viene liberato spazio sul file system](#)

La deduplicazione dei dati non funziona

Per visualizzare lo stato corrente della deduplicazione dei dati, esegui il `Get-FSxDedupStatus` PowerShell 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 350 MB per 1 TB di dati logici). Utilizza la [tabella FSx delle prestazioni di Amazon](#) per determinare la memoria associata alla capacità di throughput del tuo file system e assicurati che le risorse di memoria siano sufficienti per le dimensioni dei tuoi dati. In caso contrario, devi [aumentare la capacità di throughput del file system](#) al livello che soddisfi i requisiti di memoria di 1 GB per 1 TB di dati logici.
- I processi di deduplicazione sono configurati con l'impostazione predefinita consigliata da Windows, che prevede l'allocazione della memoria al 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 comando con parametro). `Set-FSxDedupSchedule -Memory` Tieni presente che l'utilizzo di un'allocazione di memoria più elevata per la deduplicazione può influire sulle prestazioni del file system.
- È possibile modificare la configurazione dei processi di deduplicazione per ridurre la quantità di memoria richiesta. 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 storage](#)

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 l'esecuzione del processo di raccolta dei rifiuti 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.

Per ulteriori informazioni sulla deduplicazione dei dati, consulta la documentazione di Microsoft [Understanding Data Deduplication](#).

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 FSx delle prestazioni di Amazon](#) per determinare la memoria associata alla capacità di throughput del tuo 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 affinché venga eseguita su tipi di file o cartelle specifici oppure impostare una dimensione e una data minime del file per l'ottimizzazione. Per ulteriori informazioni, consulta [Riduzione dei costi di storage con la deduplicazione dei dati](#).

Gestione delle 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.

Puoi gestire le quote di storage degli utenti 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'Amazon FSx CLI per PowerShell](#).

Di seguito sono riportati i comandi che è possibile utilizzare per gestire le quote di archiviazione degli utenti.

Comando User Storage Quotas	Description
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 esempio `Enable-FSxUserQuotas -?`.

Aumento della capacità di archiviazione del file system

È possibile aumentare la capacità FSx di storage del file system Windows File Server man mano che i requisiti di storage cambiano. Usa la FSx console Amazon AWS CLI, o l'FSx API Amazon per aumentare la capacità di storage di un file system come descritto nelle seguenti procedure. Per ulteriori informazioni, consulta [Gestione della capacità di storage](#).

Per aumentare la capacità di archiviazione di un file system (console)

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

2. Passa a File system e scegli il file system Windows per cui desideri aumentare la capacità di archiviazione.
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 per cento 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 per Windows File Server, utilizzare il AWS CLI comando [update-file-system](#). 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 per cento rispetto al valore corrente.

È possibile monitorare l'avanzamento dell'aggiornamento utilizzando il AWS CLI comando [describe-file-systems](#). Cerca il `administrative-actions` nell'output.

Per ulteriori informazioni, consulta [AdministrativeAction](#).

Monitoraggio dell'aumento della capacità di archiviazione

Dopo aver aumentato la capacità di storage del file system, puoi monitorare l'avanzamento dell'aumento della capacità di storage utilizzando la FSx console Amazon, l'API o AWS CLI come descritto nelle seguenti procedure.

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 archiviazione 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-systems](#) AWS CLI comando e l'azione [DescribeFileSystems](#) API. L'AdministrativeActions array elenca le 10 azioni di aggiornamento più recenti per ogni tipo di azione amministrativa. Quando si aumenta la capacità di archiviazione di un file system, AdministrativeActions ne vengono generate due: una FILE_SYSTEM_UPDATE e un STORAGE_OPTIMIZATION azione.

L'esempio seguente mostra un estratto della risposta di un comando CLI describe-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_OPTIMIZATION`azione 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, vedere [Gli aggiornamenti della capacità di storage o di throughput non riescono](#).

Aumento dinamico della capacità di archiviazione di un file system FSx per Windows File Server

In alternativa all'aumento manuale della capacità di storage del file system FSx for Windows File Server all'aumentare della quantità di dati archiviati, è possibile utilizzare un CloudFormation modello per aumentare automaticamente lo storage. La soluzione presentata in questa sezione aumenta dinamicamente la capacità di storage di un file system quando la quantità di capacità di storage disponibile 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 archiviazione gratuita, l' CloudWatch allarme Amazon basato su questa soglia e la AWS Lambda funzione che aumenta la capacità di archiviazione del file system.

La soluzione include 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

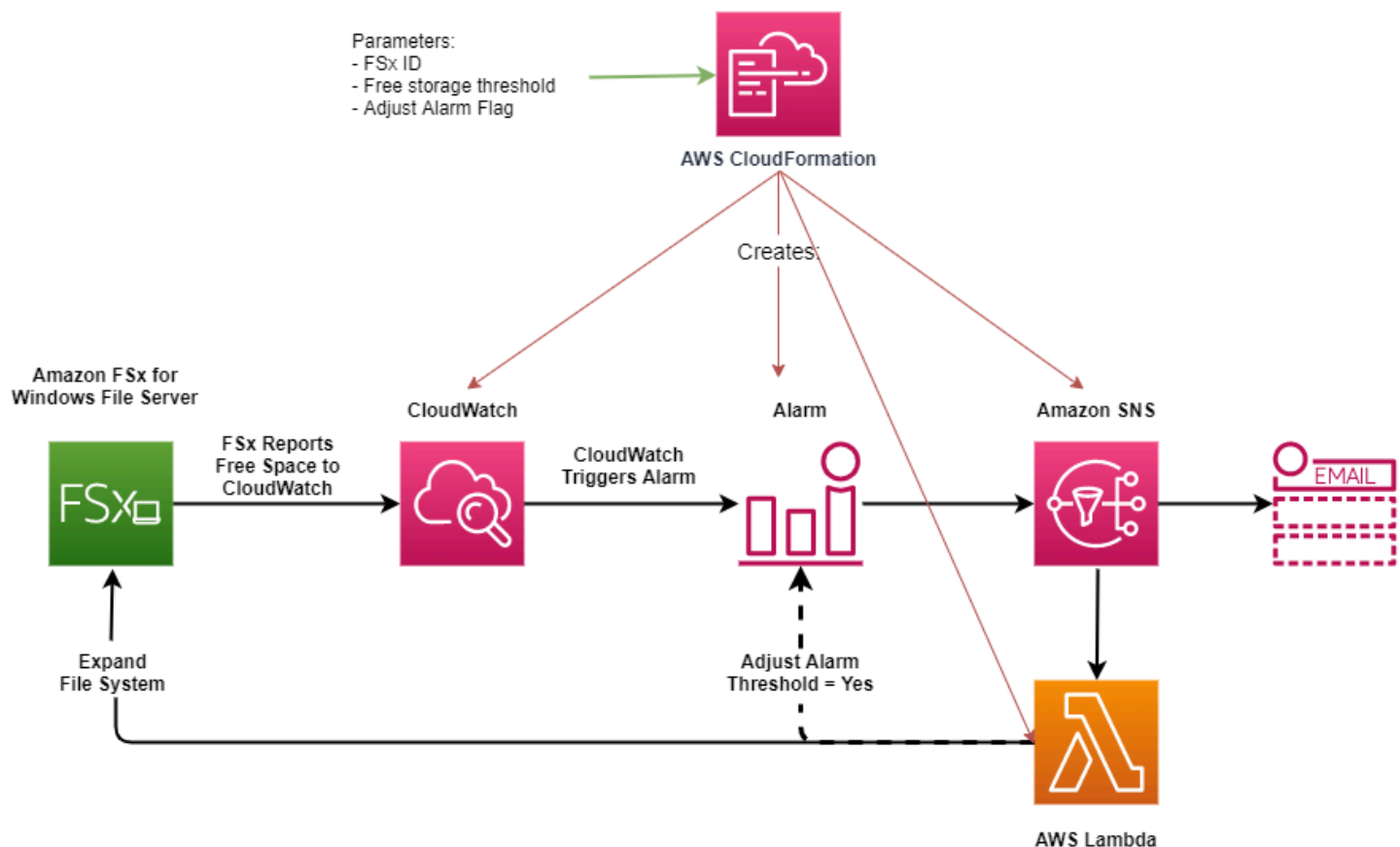
- Regola la soglia di allarme (Sì/No)

Argomenti

- [Panoramica dell'architettura](#)
- [CloudFormation modello](#)
- [Implementazione automatizzata con CloudFormation](#)

Panoramica dell'architettura

L'implementazione di questa soluzione crea le seguenti risorse nel cloud. AWS



Il diagramma illustra i passaggi seguenti:

1. Il CloudFormation modello distribuisce un CloudWatch allarme, una AWS Lambda funzione, una coda Amazon Simple Notification Service (Amazon SNS) e tutti i ruoli richiesti (IAM). AWS Identity and Access Management Il ruolo IAM fornisce alla funzione Lambda il permesso 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.

CloudFormation modello

Questa soluzione consente CloudFormation di automatizzare la distribuzione dei componenti utilizzati per aumentare automaticamente la capacità di archiviazione di un file system FSx per Windows File Server. Per utilizzare questa soluzione, scarica il modello [Increase FSx Size](#) 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. Specifica 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 perLowFreeDataStorageCapacityThreshold, 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. Specifica l'indirizzo e-mail da utilizzare per l'abbonamento SNS e riceve avvisi sulla soglia di capacità di archiviazione.

PercentIncrease

Nessun valore predefinito. Specifica la quantità di cui aumentare la capacità di archiviazione, espressa come percentuale della capacità di archiviazione corrente.

Implementazione automatizzata con CloudFormation

La procedura seguente configura e implementa uno CloudFormation stack per aumentare automaticamente la capacità di archiviazione di un file system FSx per 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 FSx file system Amazon in esecuzione in un Amazon Virtual Private Cloud (Amazon VPC) nel tuo AWS account. Per ulteriori informazioni sulla creazione di FSx risorse Amazon, consulta [Guida introduttiva ad Amazon FSx per Windows File Server](#).

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

1. Scarica il CloudFormation modello [Increase FSx Size](#). Per ulteriori informazioni sulla creazione di uno CloudFormation stack, consulta [Creazione di uno stack sulla AWS CloudFormation console nella Guida](#) per l'AWS CloudFormation utente.

 Note

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

2. In Specificare i dettagli dello stack, inserisci i valori per la tua soluzione di aumento automatico della capacità di archiviazione.

Specify stack details

Stack name

Stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

File System Parameters

FileSystemId
Amazon FSx file system ID

Alarm Notification

LowFreeDataStorageCapacityThreshold
Low free data storage capacity threshold (GiB or %)

LowFreeDataStorageCapacityThresholdUnit
Specify the Storage Capacity threshold Unit (GiB or %)

EmailAddress
The email address for alarm notification.

Other parameters

AlarmModificationNotification
Would you like to adjust the percent increase for the next FSx storage increase event proportionate to the requested increase?

PercentIncrease
Provide the percent increase for File System Storage. This value should be between 10 and 100

Cancel Previous **Next**

- Immettete il nome dello stack.
- Per Parametri, esaminate i parametri del modello e modificateli in base alle esigenze del file system. Quindi scegli Successivo.
- Immettete le impostazioni delle opzioni desiderate per la soluzione personalizzata, quindi scegliete Avanti.
- 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. Scegli Crea per distribuire lo stack.

Puoi visualizzare lo stato dello stack nella CloudFormation console nella colonna Status. Dovresti vedere lo stato di CREATE_COMPLETE tra circa 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 CloudFormation utente.

Aggiornamento del tipo di archiviazione di un file system FSx per Windows

È possibile modificare il tipo di archiviazione di un file system che utilizza l'archiviazione su HDD per utilizzare l'archiviazione SSD. Puoi utilizzare la FSx console Amazon AWS CLI, o l' FSx API Amazon per modificare il tipo di storage di un file system, come illustrato nelle seguenti procedure. Per ulteriori informazioni, consulta [Gestione del tipo di storage del file system](#).

Per aggiornare il tipo di storage di un file system (console)

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Passa a File system e scegli il file system 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 Aggiorna tipo di archiviazione.
4. Per Tipo di archiviazione desiderato, scegli SSD. Scegli Aggiorna per avviare l'aggiornamento del tipo di archiviazione.

È possibile [monitorare l'avanzamento](#) dell'aggiornamento del tipo di archiviazione utilizzando la console e la CLI.

Per aggiornare il tipo di storage di un file system (CLI)

Per aggiornare il tipo di archiviazione FSx per un file system Windows File Server, utilizzare il AWS CLI comando [update-file-system](#). Imposta i seguenti parametri:

- `--file-system-id` dall'ID del file system che desideri aggiornare.
- `--storage-type` su SSD. Non è possibile passare dal tipo di archiviazione SSD al tipo di archiviazione HDD.

È possibile monitorare l'avanzamento dell'aggiornamento utilizzando il AWS CLI comando. [describe-file-systems](#) Cerca il `administrative-actions` nell'output.

Per ulteriori informazioni, consulta [AdministrativeAction](#).

Monitoraggio degli aggiornamenti dei tipi di archiviazione

Dopo aver aggiornato il tipo di storage del tuo file system da HDD a SSD, puoi monitorare l'avanzamento dell'aggiornamento del tipo di storage utilizzando la FSx console Amazon AWS CLI, l'API, come descritto nelle seguenti procedure.

Monitoraggio degli aggiornamenti del file system nella console

Nella scheda Aggiornamenti della finestra dei dettagli del file system, è possibile 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 di archiviazione SSD sono disponibili per le operazioni di scrittura. L'aggiornamento entra in uno stato di ottimizzazione Aggiornato, che in genere dura alcune ore, durante il quale le operazioni di lettura 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-systems](#) AWS CLI comando e l'azione [DescribeFileSystems](#) API. L'AdministrativeActionsarray 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_OPTIMIZATIONazione.

Aggiornamento degli IOPS SSD di un file system

Per i file system configurati con storage SSD, il livello di IOPS SSD assegnati determina la quantità di disco I/O disponibile quando il file system deve leggere e scrivere dati su disco, anziché leggere o scrivere dati nella cache. Puoi aggiornare gli IOPS SSD per un file system utilizzando la FSx console Amazon AWS CLI, o l' FSx API Amazon, come descritto nelle seguenti procedure. Per ulteriori informazioni sulla gestione degli IOPS SSD, consulta. [Gestione degli IOPS SSD](#)

Per aggiornare gli IOPS SSD per un file system (console)

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Vai a File system e scegli 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, scegliete Automatico o Provisionato dall'utente. Se scegli Automatic, Amazon fornisce FSx 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 per Windows File Server, utilizzate 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 aumenti automaticamente FSx gli IOPS dei tuoi SSD, usa `Mode=AUTOMATIC` e non utilizzare il `Iops` parametro. Amazon mantiene FSx automaticamente 3 IOPS SSD per GiB di capacità di storage sul file system, fino a un massimo di 400.000 nelle regioni supportate. AWS

Puoi monitorare lo stato di avanzamento dell'aggiornamento utilizzando il comando. AWS CLI [describe-file-systems](#) Cerca il `administrative-actions` nell'output.

Per ulteriori informazioni, consulta [AdministrativeAction](#).

Monitoraggio degli aggiornamenti IOPS degli SSD forniti

Dopo aver aggiornato la quantità di IOPS SSD assegnati per il tuo file system, puoi monitorare l'avanzamento dell'aggiornamento degli IOPS SSD utilizzando la FSx console Amazon, l'API e l'API AWS CLI, come descritto nelle seguenti procedure.

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-systems](#) AWS CLI comando e l'azione [DescribeFileSystems](#)API.

L'AdministrativeActionsarray 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 deduplicazione dei dati

Puoi gestire le [impostazioni di deduplicazione dei dati](#) del tuo file system utilizzando l'Amazon FSx CLI per la gestione remota su PowerShell. Per ulteriori informazioni sull'utilizzo della gestione remota Amazon FSx CLI su PowerShell, consulta [Utilizzo dell'Amazon FSx CLI per PowerShell](#)

Di seguito sono riportati i comandi che puoi utilizzare per la deduplicazione dei dati.

Comando di deduplicazione dei dati	Description
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 deduplicazione, tra cui la dimensione e la data minime del file per l'ottimizzazione, le impostazioni di compressione e i tipi di file e le cartelle esclusi.
Set-FSxDedupConfiguration	Modifica le impostazioni di configurazione della deduplicazione, tra cui dimensione e età minime dei file per l'ottimizzazione, le impostazioni di compressione e i tipi di file e le cartelle esclusi.
Get-FSxDedupStatus	Recupera lo stato della deduplicazione e includi proprietà di sola lettura che descrivono i risparmi e lo stato di ottimizzazione del file system, i tempi e lo stato di completamento degli ultimi processi di deduplicazione 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.
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.

Comando di deduplicazione dei dati	Description
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	Eliminare una pianificazione di deduplicazione.
Get-FSxDedupJob	Ottieni lo stato e le informazioni per tutti i processi di deduplicazione attualmente in esecuzione o in coda.
Stop-FSxDedupJob	Annula 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 esempio `Enable-FSxDedup -?`.

Abilitare la deduplicazione dei dati

Puoi abilitare la deduplicazione dei dati su una condivisione di file Amazon FSx for Windows File Server utilizzando il `Enable-FSxDedup` comando, come segue.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxxxxxxx.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

Sebbene la pianificazione predefinita funzioni correttamente 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 amznfsxxxxxxxxx.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 amznfsxxxxxxxxx.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 amznfsxxxxxxxxx.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, come segue.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxxxxxxx.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

Utilizza le seguenti informazioni per risolvere alcuni problemi comuni relativi alla configurazione e all'utilizzo della deduplicazione dei dati.

Argomenti

- [La deduplicazione dei dati non funziona](#)
- [I valori di deduplicazione sono inaspettatamente impostati su 0](#)
- [Dopo l'eliminazione dei file non viene liberato spazio sul file system](#)

La deduplicazione dei dati non funziona

Per visualizzare lo stato corrente della deduplicazione dei dati, esegui il `Get-FSxDedupStatus` PowerShell 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 350 MB per 1 TB di dati logici). Utilizza la [tabella FSx delle prestazioni di Amazon](#) per determinare la memoria associata alla capacità di throughput del tuo file system e assicurati che le risorse di memoria siano sufficienti per le dimensioni dei tuoi dati. In caso contrario, devi [aumentare la capacità di throughput del file system](#) al livello che soddisfi i requisiti di memoria di 1 GB per 1 TB di dati logici.
- I processi di deduplicazione sono configurati con l'impostazione predefinita consigliata da Windows, che prevede l'allocazione della memoria al 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 comando con parametro). `Set-FSxDedupSchedule -Memory` Tieni presente che l'utilizzo di un'allocazione di memoria più elevata per la deduplicazione può influire sulle prestazioni del file system.
- È possibile modificare la configurazione dei processi di deduplicazione per ridurre la quantità di memoria richiesta. 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 storage](#).

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 l'esecuzione del processo di raccolta dei rifiuti 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.

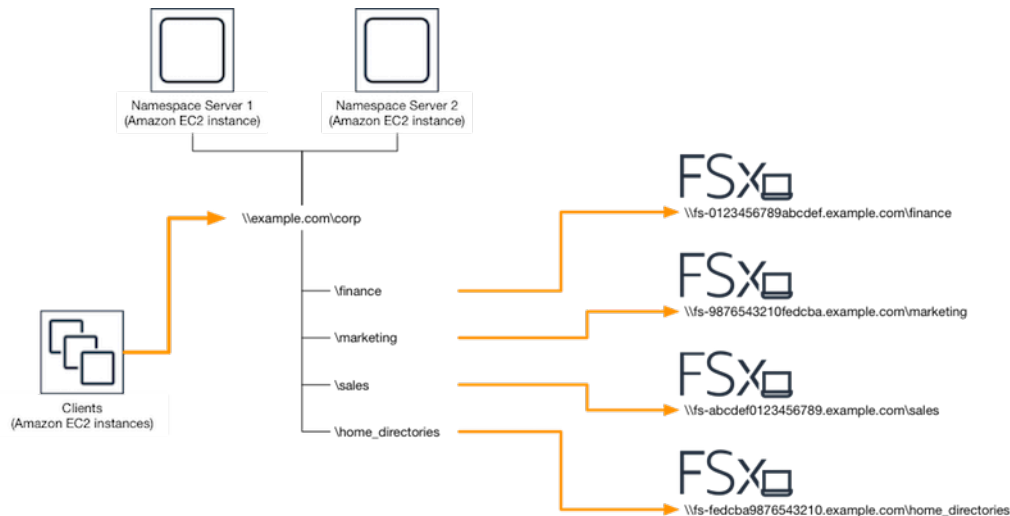
Utilizzo dei namespace DFS

DFS Namespaces è un servizio di ruolo di Windows Server utilizzato per raggruppare le cartelle condivise situate su server diversi in uno o più namespace strutturati in modo logico. In questo modo è possibile offrire agli utenti una visualizzazione virtuale delle cartelle condivise, in cui un unico percorso conduce ai file che si trovano su più file system, come illustrato nel diagramma seguente. Oltre a organizzare e unificare l'accesso alle condivisioni di file su più file system,

Raggruppa più file system FSx per Windows File Server con namespace DFS

È possibile utilizzare i namespace DFS (Distributed File System) di Microsoft per raggruppare le condivisioni di file su più file system FSx per Windows File Server in un'unica struttura di cartelle o spazio dei nomi comune. Utilizzando DFS Namespaces, è possibile scalare lo storage dei file oltre la capacità di archiviazione massima del singolo file system (64 TiB) per set di dati di file di grandi dimensioni, fino a centinaia di petabyte. Questa sezione mostra come configurare i namespace DFS su più file system per Windows File Server. FSx

DFS Namespaces è un servizio di ruolo di Windows Server utilizzato per raggruppare cartelle condivise situate su server diversi in uno o più namespace strutturati in modo logico. In questo modo è possibile offrire agli utenti una visualizzazione virtuale delle cartelle condivise, in cui un unico percorso conduce ai file che si trovano su più file system, come illustrato nel diagramma seguente. Oltre a organizzare e unificare l'accesso alle condivisioni di file su più file system,



Per una step-by-step procedura di raggruppamento FSx per i file system Windows utilizzando i namespace DFS, vedere. [Raggruppa più file system in un unico spazio dei nomi](#)

Miglioramento delle prestazioni con gli shard

Amazon FSx per Windows File Server supporta l'uso del Microsoft Distributed File System (DFS). Utilizzando i namespace DFS, 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 la soluzione fornita [Suddivisione dei dati utilizzando i namespace DFS per prestazioni di scalabilità orizzontale](#) per distribuire l'accesso in lettura/scrittura ai dati in modo uniforme tra più dati FSx per i file system Windows File Server.

Raggruppa più file system in un unico spazio dei nomi

In questa procedura, creerete un unico spazio dei nomi basato sul dominio (`example.com\corp`) su due server dello spazio dei nomi, al fine di consolidare le condivisioni di file archiviate su più file system FSx per Windows (finanza, marketing, vendite, `home_directories`). Verranno inoltre impostate quattro condivisioni di file nello spazio dei nomi, ognuna delle quali reindirizza in modo trasparente gli utenti alle condivisioni ospitate su file system Windows separati. FSx Ciò consente agli utenti di

accedere alle condivisioni di file utilizzando uno spazio dei nomi comune anziché dover specificare i nomi DNS 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.

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. CloudFormation](#) [Per ulteriori informazioni sulla creazione di uno stack, consulta la sezione Creazione di uno stack sulla console nella Guida per l'utente. 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 [Connecting to Your Windows Instance](#) nella Amazon EC2 User Guide.
3. Accedi alla console di gestione DFS aprendo. Apri il menu Start ed esegui dfsmgmt.msc. Verrà aperto 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. Scegli Next (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

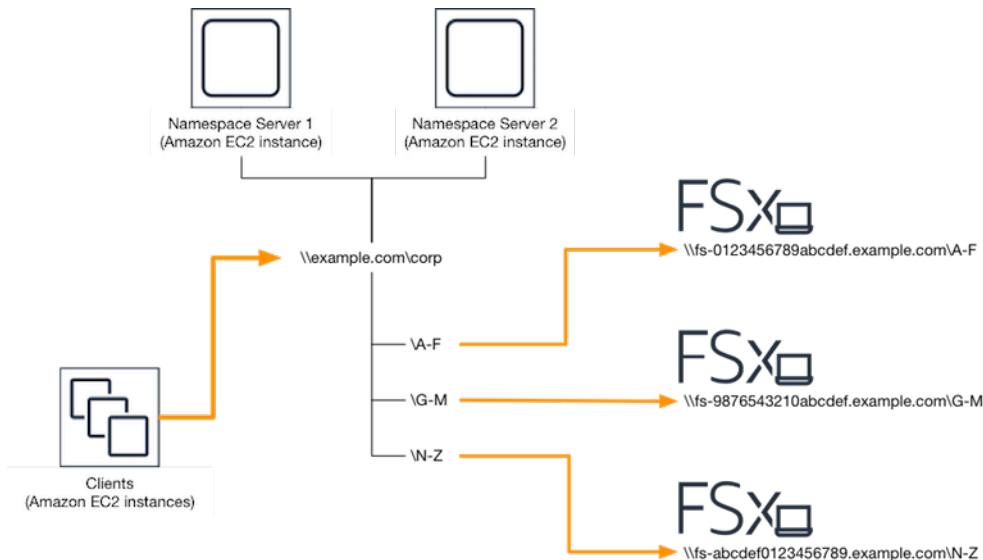
La modalità Windows Server 2008 è l'ultima opzione disponibile per i namespace.

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.

Suddivisione dei dati utilizzando i 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 *corp* namespace vengono suddivisi alfabeticamente. I file di dati 'A-F', 'G-M' e 'N-Z' sono tutti archiviati in 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.](#) CloudFormation [Per ulteriori informazioni sulla creazione di uno stack, consulta la sezione Creazione di uno stack sulla console nella Guida per l'utente. 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 [Connecting to Your Windows Instance](#) nella Amazon EC2 User Guide.
3. Accedi alla console di gestione DFS. Apri il menu Start ed esegui dfsmgmt.msc. Verrà aperto 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. Scegli Next (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.

Gestione della capacità di throughput

È possibile aumentare e diminuire la capacità di trasmissione del file system per gestirne le prestazioni in qualsiasi momento. La capacità di throughput è una delle dimensioni che determina la velocità alla quale il file server che ospita il file system FSx per Windows File Server può servire i dati. Livelli più elevati di capacità di throughput comportano anche livelli più elevati di I/O operazioni al

secondo (IOPS) e una maggiore quantità di memoria cache sul file server. Per ulteriori informazioni, consulta [FSx per le prestazioni di Windows File Server](#).

Argomenti

- [Come funziona la scalabilità del throughput](#)
- [Sapere quando modificare la capacità di throughput](#)
- [Modifica della capacità di throughput](#)
- [Monitoraggio degli aggiornamenti della capacità di throughput](#)

Come funziona la scalabilità del throughput

Quando modifichi la capacità di throughput del tuo file system, Amazon FSx passa dal file server del file system a uno con una velocità effettiva maggiore o minore dietro le quinte. Per i file system Multi-AZ, il passaggio a un nuovo file server attiva un failover e un failback automatici mentre FSx Amazon disattiva i file server preferiti e secondari. I file system Single-AZ non saranno disponibili per alcuni minuti mentre il file server viene cambiato durante la scalabilità della capacità di throughput. La nuova quantità di capacità di throughput viene fatturata non appena sarà disponibile per il file system.

Note

Durante un'operazione di manutenzione sul back-end, le modifiche al sistema (incluse le modifiche alla capacità di throughput) possono subire ritardi. Le operazioni di manutenzione possono causare la messa in coda delle modifiche al sistema per l'elaborazione.

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 avvengono durante la scalabilità della capacità di throughput, la manutenzione del file system e un'interruzione non pianificata del servizio, il traffico in corso verso il file system verrà servito dal file server rimanente. Quando il file server sostituito torna online, FSx per Windows eseguirà un processo di risincronizzazione per garantire la sincronizzazione dei dati 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 dati persi, ma anche dalla natura della perdita di dati sul file system. Se il carico di lavoro è intenso in termini di scrittura e IOPS, il processo di sincronizzazione dei dati potrebbe richiedere più tempo e richiedere 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 trasmissione durante i periodi di inattività quando il carico sul file system è minimo. Si consiglia inoltre di assicurarsi che il file system disponga di una capacità di trasmissione sufficiente per eseguire il processo di sincronizzazione in aggiunta al carico di lavoro, in modo da ridurre la durata della sincronizzazione dei dati. Infine, consigliamo di testare l'impatto dei failover quando il file system ha un carico più leggero.

Sapere quando modificare la capacità di throughput

Amazon FSx si integra con Amazon CloudWatch, consentendoti di monitorare i livelli di utilizzo del throughput continuo del tuo file system. Le prestazioni (throughput e IOPS) che puoi ottenere attraverso il tuo file system dipendono dalle caratteristiche specifiche del carico di lavoro, oltre alla capacità di throughput, alla capacità di archiviazione e al tipo di storage del file system. È possibile utilizzare le CloudWatch metriche per determinare quali di queste dimensioni modificare per migliorare le prestazioni. Per ulteriori informazioni, consulta [Monitoraggio con Amazon CloudWatch](#).

FSx per Windows File Server fornisce avvisi sulle prestazioni basati sui valori delle CloudWatch metriche per il file system nel dashboard di monitoraggio e prestazioni nella pagina dei dettagli del file system sulla console Amazon FSx . Ciò include la capacità di throughput e altri parametri del file system che possono trarre vantaggio dall'aumento della capacità di throughput. Per ulteriori informazioni, consulta [Avvertenze e raccomandazioni sulle prestazioni](#).

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 abilitate 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](#).

Modifica della capacità di throughput

Puoi aumentare o diminuire la capacità di throughput del tuo file system utilizzando la FSx console Amazon, AWS Command Line Interface (AWS CLI) o l' FSx API Amazon, come descritto nelle seguenti procedure.

Per modificare la capacità di throughput di un file system (console)

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Passa a File system e scegli il file system Windows per cui desideri aumentare la capacità di throughput.
3. Per Azioni, scegli Aggiorna velocità effettiva.

Oppure, nel pannello Riepilogo, scegliete Aggiorna accanto alla capacità di throughput del file system.

Viene visualizzata la finestra Aggiorna capacità di trasmissione.

4. Scegliete il nuovo valore per la capacità di trasmissione dall'elenco.
5. Scegliete Aggiorna per avviare l'aggiornamento della capacità di throughput.

Note

I file system Multi-AZ eseguono il failover e il failback durante l'aggiornamento della scalabilità del throughput e sono completamente disponibili. I file system Single-AZ subiscono un periodo di indisponibilità molto breve durante l'aggiornamento.

6. È possibile monitorare l'avanzamento dell'aggiornamento nella pagina dei dettagli dei file system, nella scheda Aggiornamenti.

Puoi monitorare lo stato di avanzamento dell'aggiornamento utilizzando la FSx console Amazon AWS CLI, e l'API. Per ulteriori informazioni, consulta [Monitoraggio degli aggiornamenti della capacità di throughput](#).

Per modificare la capacità di throughput (CLI) di un file system

Per aumentare o diminuire la capacità di throughput di un file system, utilizzate il comando. AWS CLI [update-file-system](#) Imposta i seguenti parametri:

- `--file-system-id` dall'ID del file system che state aggiornando.

- `ThroughputCapacity` valore desiderato; i valori validi sono 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4608, 6144, 9216, 12288. MBps

Puoi monitorare lo stato di avanzamento dell'aggiornamento utilizzando la FSx console Amazon AWS CLI, e l'API. Per ulteriori informazioni, consulta [Monitoraggio degli aggiornamenti della capacità di throughput](#).

Monitoraggio degli aggiornamenti della capacità di throughput

Puoi monitorare lo stato di avanzamento di una modifica della capacità di throughput utilizzando la FSx console Amazon, l'API e il AWS CLI.

Monitoraggio delle variazioni della capacità di throughput nella console

Nella scheda Aggiornamenti della finestra dei dettagli del file system, è possibile visualizzare le 10 azioni di aggiornamento più recenti per ogni tipo di azione di aggiornamento.

Updates (10) 🔄					
Filter updates < 1 > ⚙️					
Update type ▼	Target value ▼	Status ▼	Progress % ▼	Request time ▲	
Storage capacity	154	✅ Completed	-	2020-05-22T12:14:58-04:00	
Throughput capacity	64	✅ Completed	-	2020-05-22T12:14:50-04:00	
Throughput capacity	128	✅ Completed	-	2020-05-21T13:55:58-04:00	
Storage capacity	140	✅ Completed	-	2020-05-21T13:55:30-04:00	
Storage capacity	122	✅ Completed	-	2020-05-18T11:36:33-04:00	

Per le azioni di aggiornamento della capacità di throughput, è possibile visualizzare le seguenti informazioni.

Tipo di aggiornamento

Il valore possibile è la capacità di trasmissione.

Target value (Valore target)

Il valore desiderato su cui modificare la capacità di trasmissione del file system.

Stato

Lo stato attuale dell'aggiornamento. Per gli aggiornamenti della capacità di throughput, i valori possibili sono i seguenti:

- In sospeso: Amazon FSx ha ricevuto la richiesta di aggiornamento, ma non ha avviato l'elaborazione.
- In corso: Amazon FSx sta elaborando la richiesta di aggiornamento.
- Ottimizzazione aggiornata: Amazon FSx ha aggiornato le I/O, CPU, and memory resources. The new disk I/O performance level is available for write operations. Your read operations will see disk I/O prestazioni di rete del file system tra il livello precedente e il nuovo livello fino a quando il file system non si trova più in questo stato.
- Completato: l'aggiornamento della capacità di throughput è stato completato con successo.
- Non riuscito: l'aggiornamento della capacità di throughput non è riuscito. Scegli il punto interrogativo (?) per visualizzare i dettagli sul motivo per cui l'aggiornamento del throughput non è riuscito.

Orario della richiesta

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

Monitoraggio delle modifiche con l'API AWS CLI and

È possibile visualizzare e monitorare le richieste di modifica della capacità di throughput del file system utilizzando il comando [describe-file-systems](#) CLI e [DescribeFileSystems](#) l'azione API.

L'AdministrativeActionsarray elenca le 10 azioni di aggiornamento più recenti per ogni tipo di azione amministrativa. Quando si modifica la capacità di throughput di un file system, viene generata un'azione FILE_SYSTEM_UPDATE amministrativa.

L'esempio seguente mostra l'estratto della risposta di un comando CLI `describe-file-systems`. Il file system ha una capacità di throughput di 8 MBps e la capacità di throughput di destinazione di 256. MBps

```
.
.
.
  "ThroughputCapacity": 8,
  "AdministrativeActions": [
    {
      "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
```

```

    "RequestTime": 1581694764.757,
    "Status": "PENDING",
    "TargetFileSystemValues": {
      "WindowsConfiguration": {
        "ThroughputCapacity": 256
      }
    }
  }
]

```

Quando Amazon FSx completa correttamente l'elaborazione dell'azione, lo stato cambia in `COMPLETED`. La nuova capacità di throughput è quindi disponibile per il file system e viene visualizzata nella `ThroughputCapacity` proprietà. Ciò è illustrato nel seguente estratto di risposta di un comando `CLDescribe-file-systems`.

```

.
.
.
  "ThroughputCapacity": 256,
  "AdministrativeActions": [
    {
      "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
      "RequestTime": 1581694764.757,
      "Status": "COMPLETED",
      "TargetFileSystemValues": {
        "WindowsConfiguration": {
          "ThroughputCapacity": 256
        }
      }
    }
  ]
]

```

Se la modifica della capacità di throughput non riesce, lo stato cambia e la `FailureDetails` proprietà fornisce informazioni sull'errore. `FAILED` Per informazioni sulla risoluzione dei problemi relativi alle azioni non riuscite, vedere [Gli aggiornamenti della capacità di storage o di throughput non riescono](#).

Gestione del tipo di rete

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

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

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

Utilizzo della modalità dual-stack

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

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

Modifica del tipo di rete

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

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

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

Viene visualizzata la finestra **Aggiorna tipo di rete**.

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

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

5. Scegli **Aggiorna**.

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

- Per modificare il tipo di rete di un file system, utilizzate il comando [update-file-system](#) CLI (o l'operazione [UpdateFileSystem](#) API equivalente), come illustrato nell'esempio seguente.

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

Taggare le tue risorse Amazon FSx

Per aiutarti a gestire i tuoi file system e altre risorse FSx per Windows File Server, puoi assegnare i tuoi metadati a ciascuna risorsa sotto forma di tag. I tag consentono di classificare le AWS risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Questa caratteristica è molto utile quando hai tante risorse dello stesso tipo in quanto puoi rapidamente individuare una risorsa specifica in base ai tag assegnati. Questo argomento descrive i tag e mostra come crearli.

Argomenti

- [Nozioni di base sui tag](#)
- [Tagging delle risorse](#)
- [Limitazioni applicate ai tag](#)
- [Autorizzazioni necessarie per etichettare le risorse](#)

Nozioni di base sui tag

Un tag è un'etichetta che si assegna a una AWS risorsa. Ogni tag è composto da una chiave e da un valore opzionale, entrambi personalizzabili.

I tag consentono di classificare le AWS risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ad esempio, puoi definire un set di tag per i tuoi account per i file system di FSx Windows File Server che ti aiutino a tenere traccia del proprietario e del livello di stack di ogni istanza.

Ti consigliamo di creare un set di chiavi di tag in grado di soddisfare i requisiti di ciascun tipo di risorsa. Con un set di chiavi di tag coerente, la gestione delle risorse risulta semplificata. Puoi cercare e filtrare le risorse in base ai tag aggiunti. [Per ulteriori informazioni su come implementare una strategia efficace di etichettatura delle risorse, consulta il AWS white paper Tagging Best Practices.](#)

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 FSx per Windows File Server, la AWS CLI o un AWS SDK, puoi utilizzare l'azione TagResource API per applicare tag alle risorse esistenti. Inoltre, alcune operazioni per la creazione di risorse ti consentono di specificare tag per una risorsa durante la sua creazione. Se i tag non possono essere applicati durante la creazione della risorsa, eseguiamo il rollback del processo di creazione della risorsa. Ciò fa sì che le risorse vengano create con i tag oppure che non vengano create affatto, nonché che nessuna risorsa sia mai sprovvista di tag. Il tagging delle risorse in fase di creazione ti permette di evitare di eseguire script di tagging personalizzati dopo la creazione delle risorse. Per ulteriori informazioni sull'abilitazione agli utenti affinché possano aggiungere tag alle risorse durante la creazione, vedere [Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione.](#)

Tagging delle risorse

Puoi taggare FSx le risorse di Windows File Server presenti nel tuo account. Se utilizzi la FSx console Amazon, puoi applicare tag alle risorse utilizzando la scheda Tag nella schermata delle risorse pertinente. Quando crei risorse, puoi applicare la chiave Name con un valore e puoi applicare tag a tua scelta quando crei un nuovo file system. La console può organizzare le risorse in base al tag Name, ma questo tag non ha alcun significato semantico FSx per il servizio Windows File Server.

Puoi applicare autorizzazioni a livello di risorsa basate su tag nelle tue policy IAM alle azioni dell'API FSx per Windows File Server che supportano l'aggiunta di tag alla creazione per implementare il controllo granulare sugli utenti e i gruppi che possono taggare le risorse al momento della creazione. Le risorse vengono adeguatamente protette a partire dal momento della creazione, ovvero i tag vengono applicati subito alle risorse. Pertanto qualsiasi autorizzazione basata su tag a livello di risorsa che controlla l'uso delle risorse risulta immediatamente valida. Le risorse possono essere monitorate e segnalate con maggiore precisione. Puoi applicare l'uso del tagging alle nuove risorse e controllare quali chiavi e valori di tag sono impostati per le risorse.

Puoi anche applicare autorizzazioni a livello di risorsa alle e per le azioni dell'API Windows File Server nelle tue policy IAM `UntagResource` FSx per controllare quali chiavi `TagResource` e valori dei tag sono impostati sulle tue risorse esistenti.

Per ulteriori informazioni sul tagging delle risorse per la fatturazione, consulta [Utilizzo di tag per l'allocazione dei costi](#) nella Guida per l'utente di AWS Billing .

Limitazioni applicate ai tag

Si applicano le seguenti limitazioni di base ai tag:

- Numero massimo di tag per risorsa: 50
- Per ciascuna risorsa, ogni chiave del tag deve essere univoca e ogni chiave del tag può avere un solo valore.
- Lunghezza massima della chiave: 128 caratteri Unicode in formato UTF-8
- Lunghezza massima del valore: 256 caratteri Unicode in formato UTF-8
- I caratteri consentiti FSx per i tag di Windows File Server sono: lettere, numeri e spazi rappresentabili in UTF-8 e i seguenti caratteri: + - = . _ / @.
- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole.
- Il `aws :` prefisso è riservato all'uso. AWS Se il tag ha una chiave di tag con questo prefisso, non puoi modificare o eliminare la chiave o il valore de tag. I tag con il prefisso `aws :` non vengono conteggiati per il limite del numero di tag per risorsa.

Non è possibile eliminare una risorsa in base esclusivamente ai relativi tag; è necessario specificare l'identificatore della risorsa. Ad esempio, per eliminare un file system etichettato con una chiave di tag chiamata `DeleteMe`, è necessario utilizzare l'`DeleteFileSystem` azione con l'identificatore di risorsa del file system, ad esempio `fs-1234567890abcdef0`.

Quando taggate risorse pubbliche o condivise, i tag assegnati sono disponibili solo per le vostre risorse; nessun altro avrà accesso a tali tag. Account AWS Account AWS Per il controllo dell'accesso basato su tag alle risorse condivise, ognuno Account AWS deve assegnare il proprio set di tag per controllare l'accesso alla risorsa.

Autorizzazioni necessarie per etichettare le risorse

Per ulteriori informazioni sulle autorizzazioni necessarie per etichettare le FSx risorse Amazon al momento della creazione, consulta [Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione](#). Per ulteriori informazioni sull'utilizzo dei tag per limitare l'accesso alle FSx risorse Amazon nelle policy IAM, consulta [Utilizzo dei tag per controllare l'accesso alle FSx risorse Amazon](#).

Aggiornare un file system utilizzando AWS CLI

È possibile aggiornare tre elementi utilizzando le procedure illustrate in questa procedura dettagliata. Tutti gli altri elementi del file system che è possibile aggiornare possono essere aggiornati dalla console. Queste procedure presuppongono che l'utente abbia AWS CLI installato e configurato il file sul computer locale. Per ulteriori informazioni, vedere [Installazione e configurazione](#) nella Guida AWS Command Line Interface per l'utente.

- `AutomaticBackupRetentionDays`— il numero di giorni in cui desiderate conservare i backup automatici del file system.
- `DailyAutomaticBackupStartTime`— l'ora del giorno, espressa in UTC (Coordinated Universal Time), in cui si desidera che inizi la finestra di backup automatico giornaliero. La finestra dura 30 minuti a partire dall'ora specificata. Questa finestra non può sovrapporsi alla finestra di backup settimanale per la manutenzione.
- `WeeklyMaintenanceStartTime`— l'ora della settimana in cui si desidera che inizi la finestra di manutenzione. Il giorno 1 è lunedì, il 2 è martedì e così via. La finestra è di 30 minuti a partire dall'ora specificata. Questa finestra non può sovrapporsi alla finestra di backup automatico giornaliero.

Le seguenti procedure descrivono come aggiornare il file system con. AWS CLI

Per aggiornare il periodo di conservazione dei backup automatici per il file system

1. Apri un prompt dei comandi o un terminale sul tuo computer.

2. Esegui il comando seguente, sostituendo l'ID del file system con l'ID del file system e il numero di giorni per i quali desideri 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. Apri un prompt dei comandi o un terminale sul tuo computer.
2. Esegui il comando seguente, sostituendo l'ID del file system con l'ID del file system e l'ora in cui desideri 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. Apri un prompt dei comandi o un terminale sul tuo computer.
2. Esegui il comando seguente, sostituendo l'ID del file system con l'ID del file system e la data e l'ora in cui desideri iniziare la finestra.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-configuration WeeklyMaintenanceStartTime=1:01:30
```

Protezione dei dati con backup, copie shadow e repliche pianificate

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

- I FSx backup nativi di Amazon supportano le tue esigenze di conservazione e conformità dei backup all'interno di Amazon FSx.
- AWS Backup i backup dei tuoi FSx file system Amazon fanno parte di una soluzione di backup centralizzata e automatizzata tra AWS 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 tuo FSx file system Amazon su un secondo file system fornisce protezione e ripristino dei dati.

Argomenti

- [Protezione dei dati con backup](#)
- [Protezione dei dati con copie shadow](#)
- [Replica pianificata utilizzando AWS DataSync](#)

Protezione dei dati con backup

È possibile proteggere i dati del file system FSx per Windows File Server eseguendo backup regolari del file system. Amazon ti FSx offre diverse opzioni per il backup dei tuoi file system. Puoi utilizzare backup giornalieri automatici per eseguire un backup ogni giorno. È possibile eseguire un backup del file system avviato dall'utente in qualsiasi momento. Puoi anche utilizzarlo AWS Backup come parte di una soluzione di backup centralizzata per le tue risorse. AWS Queste soluzioni di backup possono aiutarti a soddisfare le tue 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.

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'istantanea point-in-time 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 FSx backup di Amazon 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 durante il processo di backup, lo storage I/O 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 come una breve pausa. I/O 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 integra la replica che Amazon FSx for Windows File Server esegue per il tuo file system. FSx I backup di Amazon aiutano a supportare le tue esigenze di conservazione e conformità dei backup. Lavorare con FSx i backup di Amazon 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](#)
- [Utilizzo dei backup avviati dall'utente](#)
- [Utilizzo AWS Backup con Amazon FSx](#)
- [Copia di backup](#)
- [Ripristino dei backup su un nuovo file system](#)
- [Creazione di backup avviati dall'utente](#)
- [Eliminazione di backup](#)

- [Dimensioni dei backup](#)
- [Copiare i backup all'interno dello stesso account](#)
- [Ripristino di un backup su un nuovo file system](#)

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 si sceglie la finestra di backup giornaliera, si consiglia di scegliere un momento della giornata conveniente che non rientri nei normali orari di funzionamento per le applicazioni che utilizzano il file system. Consigliamo inoltre di scegliere una finestra di backup al di fuori della finestra di manutenzione, poiché i backup automatici potrebbero non essere eseguiti in caso di manutenzione continua del 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 FSx console Amazon, il periodo di conservazione del backup giornaliero automatico predefinito è di 30 giorni. Il periodo di conservazione predefinito è diverso nell' FSx API e nella CLI di Amazon. 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.

È possibile utilizzare AWS CLI o uno di questi AWS SDKs per modificare la finestra di backup e il periodo di conservazione dei backup per i file system. Utilizza l'operazione [UpdateFileSystem](#) API o il comando [update-file-system](#) CLI. Per ulteriori informazioni, consulta [Aggiornare un file system utilizzando AWS CLI](#).

Important

La riduzione del periodo di conservazione per i backup giornalieri automatici comporterà l'eliminazione permanente dei backup al di fuori della nuova finestra di conservazione. Assicurati di non aver più bisogno di questi backup precedenti prima di procedere.

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 FSx console Amazon, l'API o AWS Command Line Interface (AWS CLI). I backup dei FSx file system Amazon avviati dall'utente non scadono mai e sono disponibili per tutto il tempo che desideri conservarli. I backup avviati dall'utente vengono conservati anche dopo l'eliminazione del file system di cui era stato eseguito il backup. Puoi eliminare i backup avviati dall'utente solo utilizzando la FSx console Amazon, 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.

Per informazioni su come eseguire backup avviati dall'utente dei file system, consulta [Creazione di backup avviati dall'utente](#)

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 eseguiti da AWS Backup sono incrementali rispetto a qualsiasi altro FSx backup di Amazon 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 nella FSx console Amazon, AWS Backup nella CLI e nell'API. Tuttavia, non puoi eliminare i backup eseguiti nella FSx console Amazon, AWS Backup nella CLI o nell'API. Per ulteriori informazioni su come eseguire il backup dei FSx file system Amazon, consulta [Working with Amazon FSx File Systems](#) nella AWS Backup Developer Guide. AWS Backup

Copia di backup

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

È inoltre possibile utilizzare AWS Backup per copiare i backup tra AWS regioni e tra account. 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 effettuare copie di backup all'interno dello stesso AWS account (interregionale o regionale) utilizzando la FSx console Amazon o l' AWS CLI API Amazon FSx . Puoi anche utilizzarlo [AWS Backup](#) per 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 per copiare i 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'CopyBackupazione 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.

JSON

```
{
  "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 incremental

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 incremental, 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 informazioni su come copiare i backup dei file system, consulta [Copiare i backup all'interno dello stesso account](#)

Ripristino dei backup su un nuovo file system

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

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 Active Directory del file system originale. Per ulteriori informazioni su Active Directory, vedere [Lavorare con Microsoft Active Directory](#).

Per informazioni su come ripristinare un backup su un nuovo file system FSx per Windows, consulta [Ripristino di un backup su un nuovo file system](#).

Note

È possibile ripristinare un backup del file system solo su un nuovo file system con lo stesso tipo di distribuzione e la stessa capacità di archiviazione dell'originale. È possibile aumentare la capacità di archiviazione del nuovo file system dopo che sarà disponibile. Per ulteriori informazioni, consulta [Gestione della capacità di storage](#).

È possibile modificare una delle seguenti impostazioni del file system quando si ripristina un backup su un nuovo file system:

- Storage Type (Tipo di storage)
- Capacità effettiva di trasmissione
- VPC
- Zona di disponibilità
- Sottorete
- Gruppi di sicurezza VPC
- Configurazione di Active Directory

- AWS KMS chiave di crittografia
- Ora di inizio del backup automatico giornaliero
- Finestra di manutenzione settimanale

Creazione di backup avviati dall'utente

Oltre ai backup giornalieri automatici del file system, puoi creare un backup del file system avviato dall'utente in qualsiasi momento, utilizzando la FSx console Amazon come descritto nella procedura seguente.

Per creare un backup del file system avviato dall'utente

1. Apri la FSx console Amazon 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 FSx console Amazon selezionando Backup nella barra di navigazione a sinistra. Il tuo nuovo backup avviato dall'utente ha questo tipo USER_INITIATED e il suo stato è CREATING fino a quando non diventa AVAILABLE. Per ulteriori informazioni, consulta [Utilizzo dei backup avviati dall'utente](#).

Eliminazione di backup

Puoi eliminare qualsiasi backup giornaliero avviato dall'utente e automatico del tuo file system utilizzando la console Amazon FSx, la CLI o l'API, descritte nelle seguenti procedure. Per eliminare i backup eseguiti da AWS Backup, che hanno un tipo di AWS backup, è necessario utilizzare la AWS Backup console, la CLI o l'API. L'eliminazione di un backup è un'azione permanente e irreversibile. Vengono eliminati anche tutti i dati contenuti in un backup eliminato. Non eliminare un backup a meno che non siate sicuri di non averne più bisogno in futuro.

Per eliminare un backup (console)

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

2. Dalla dashboard della console, scegli Backup dalla barra di navigazione a sinistra.
3. Scegli il backup che desideri eliminare dalla tabella Backup, quindi scegli Elimina backup.
4. Nella finestra di dialogo Elimina backup che si apre, verifica che l'ID del backup 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.

Per fornire backup durevoli e incrementali, Amazon FSx esegue il backup dei dati a livello di blocco. file-system-consistent I dati sui volumi di archiviazione 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.

Utilizza i tag per organizzare la AWS fattura in modo da rispecchiare la tua struttura dei costi. A tale scopo, registrati per ricevere la Account AWS fattura con i valori chiave dell'etichetta inclusi. Per visualizzare il costo delle risorse combinate, puoi organizzare le informazioni di fatturazione in base alle risorse con gli stessi valori di chiave di tag. Puoi ad esempio applicare tag a numerose risorse con un nome di applicazione specifico, quindi organizzare le informazioni di fatturazione per visualizzare il costo totale dell'applicazione in più servizi. Per ulteriori informazioni, consulta la pagina sull'[utilizzo dei tag per l'allocazione dei costi](#) nella Guida per l'utente di AWS Billing .

Note

Quando si [aumenta la capacità di storage](#), il processo di migrazione dei dati dal vecchio set di dischi di archiviazione al nuovo set più ampio di dischi di archiviazione può comportare

un aumento temporaneo dell'utilizzo del backup fino all'eliminazione dei backup associati al vecchio set di dischi di archiviazione. Se lo storage del file system è stato utilizzato solo parzialmente prima di aumentare la capacità di storage, la dimensione dei dati da migrare sui nuovi dischi potrebbe essere maggiore della dimensione dei dati esistenti sui dischi di storage originali. Ciò può causare un aumento dell'utilizzo del backup fino al nuovo livello di capacità di archiviazione. È necessario considerare l'impatto dell'aumento della capacità di storage sulla pianificazione del backup.

Copiare i backup all'interno dello stesso account

È possibile utilizzare Console di gestione AWS e AWS CLI per copiare manualmente i backup all'interno dello stesso AWS account su un altro Regione AWS (copie tra aree geografiche) o all'interno dello stesso Regione AWS (copie interne all'area) utilizzando le seguenti procedure.

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

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Nel pannello di navigazione, scegliere Backup.
3. Nella tabella Backup, scegli il backup che desideri copiare, quindi scegli Copia backup.
4. Nella sezione Rule settings (Impostazioni regole), procedi nel seguente modo:
 - Nell'elenco Regione di destinazione, scegli una AWS regione di destinazione in cui copiare il backup. La destinazione può trovarsi in un'altra AWS regione (copia interregionale) o all'interno della stessa AWS regione (copia interna all'area).
 - (Facoltativo) Seleziona Copia tag per copiare i tag dal backup di origine al backup di destinazione. Se si seleziona Copia tag e si aggiungono anche tag al passaggio 6, tutti i tag vengono uniti.
5. Per Crittografia, scegli la chiave di AWS KMS crittografia per crittografare il backup copiato.
6. Per Tag: facoltativo, inserisci una chiave e un valore per aggiungere tag per il backup copiato. Se aggiungi tag qui e hai selezionato anche Copia tag al passaggio 4, tutti i tag vengono uniti.
7. Scegli Copia backup.

Il backup viene copiato all'interno dello stesso 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 [CopyBackup](#) API per copiare un backup all'interno dello stesso AWS account, in una AWS regione o all'interno di una AWS regione.

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

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

La risposta mostra la descrizione del backup copiato.

Puoi visualizzare i tuoi backup sulla FSx console Amazon o in modo programmatico utilizzando il comando `describe-backups` CLI o l'operazione API. [DescribeBackups](#)

Ripristino di un backup su un nuovo file system

È possibile ripristinare un backup del file system per creare un nuovo file system utilizzando la Console di gestione AWS CLI e l'API, come descritto nella procedura seguente.

Per ripristinare un file system da un backup

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

Amazon FSx sta creando un nuovo file system e, una volta modificato lo stato AVAILABLE, puoi utilizzarlo normalmente.

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 FSx per 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](#)
- [Impostazione della quantità massima di spazio di archiviazione per copie shadow](#)
- [Visualizzazione dell'archiviazione delle copie shadow](#)
- [Creazione di una pianificazione personalizzata delle copie shadow](#)
- [Visualizzazione della pianificazione della copia ombra](#)
- [Creazione di una copia shadow](#)
- [Visualizzazione delle copie shadow esistenti](#)
- [Eliminazione di copie shadow](#)
- [Eliminazione di una pianificazione di copie shadow](#)
- [Eliminazione dell'archiviazione, della pianificazione e di tutte le copie shadow](#)
- [Risoluzione dei problemi relativi alle 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 sufficienti per le prestazioni: 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 I/O operazioni per ogni operazione di scrittura di file.
- Usa l'archiviazione SSD e aumenta la capacità di trasmissione: poiché Windows richiede un livello elevato di prestazioni di I/O per conservare le copie shadow, consigliamo di utilizzare lo storage 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 spazio di archiviazione (su scala TB) su un singolo file system, processi come il failover e il failback potrebbero richiedere un po' più di tempo. Ciò è dovuto alla necessità per Windows di eseguire controlli di coerenza sull'archiviazione delle copie FSx shadow. È inoltre possibile che

si verifichi una maggiore latenza delle I/O operazioni a causa della FSx necessità che 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 per 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 spazio di archiviazione 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

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

- Impostazione della quantità massima di spazio di archiviazione che le copie shadow possono consumare 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 mantenere meno di 64 copie shadow in qualsiasi momento per garantire disponibilità e prestazioni. Quando si raggiunge questo limite, la copia shadow successiva che si esegue 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 FSx le impostazioni predefinite di Amazon, 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 per cento 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 spazio di archiviazione illimitato, assicurati di scalare la capacità di archiviazione man mano che vengono raggiunti i limiti relativi alla copia shadow. Per informazioni sulla configurazione dello storage di copie shadow su una dimensione specifica o illimitata, 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 dell'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 livello elevato di I/O prestazioni per la

gestione delle copie shadow, è consigliabile 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 che si verifichi una maggiore latenza delle I/O operazioni 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 portare a un massimo di tre I/O operations for every file write operation. If Windows is unable to keep up with the incoming rate of I/O operations per second, it can cause all shadow copies to be deleted because it can no longer maintain the shadow copies via copy-on-write. Therefore, it is important that you provision sufficient I/O performance capacity for your workload needs on your file system (both the throughput capacity dimension that determines the file server I/O performance, and the storage type and capacity that determine the storage I/O prestazioni).
- In genere si consiglia di utilizzare file system configurati con l'archiviazione SSD anziché con l'archiviazione su disco rigido quando si abilitano le copie shadow, dato che Windows consuma I/O prestazioni superiori per la gestione delle copie shadow e dato che lo storage su HDD offre una capacità prestazionale 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 GBMaxSpace.

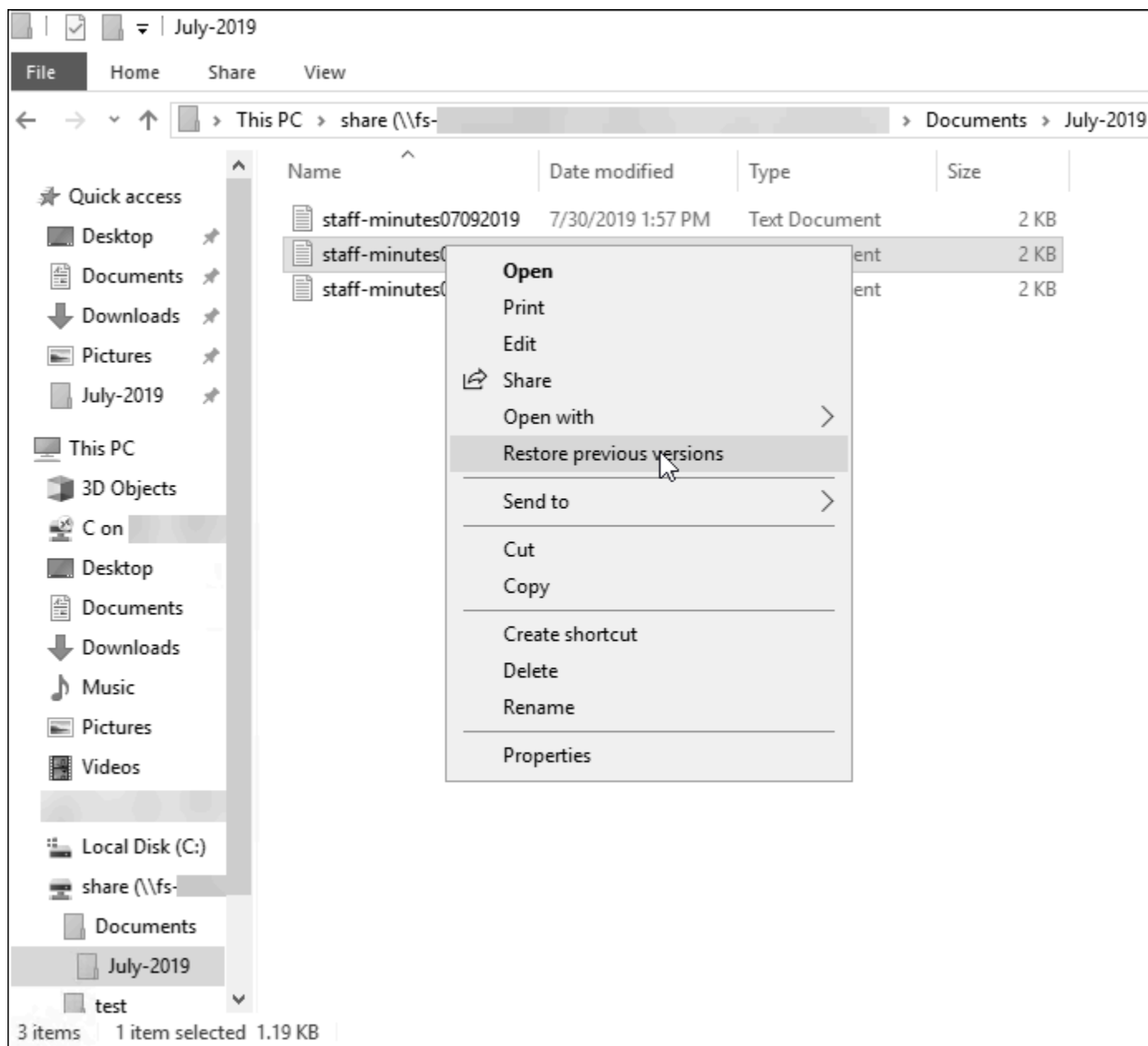
 Warning

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](#)

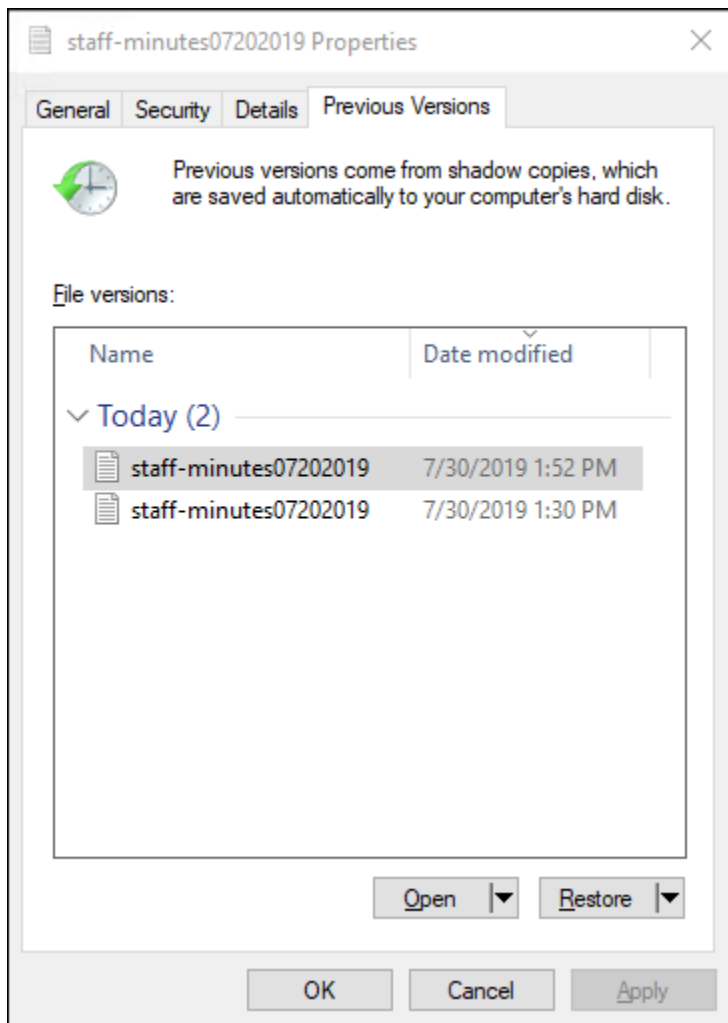
Ripristino di singoli file e cartelle

Dopo aver configurato le copie shadow sul tuo FSx file system Amazon, 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 di 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.



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

È possibile configurare rapidamente copie shadow sul file system utilizzando l'impostazione e la pianificazione predefinite per l'archiviazione delle copie shadow. 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. In AWS Managed Microsoft AD, quel gruppo è AWS FSx Delegated 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 FSx console Amazon, nella sezione Rete e sicurezza della schermata dei dettagli del file system o nella risposta dell'operazione DescribeFileSystem 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. In AWS Managed Microsoft AD, quel gruppo è AWS FSx Delegated 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, vedere [Creazione di una pianificazione personalizzata delle copie shadow](#).

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 consumare 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 archiviazione delle copie shadow su un file system FSx per 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. In AWS Managed Microsoft AD, quel gruppo è AWS FSxDelegated 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 FSx file system Amazon. Sostituiscilo *FSxFileSystem-Remote-PowerShell-Endpoint* con l' PowerShell endpoint remoto Windows del file system che desideri amministrare. Puoi trovare l' PowerShell endpoint Windows Remote nella FSx console Amazon, nella sezione Rete e sicurezza della schermata dei dettagli del file system o nella risposta dell'operazione DescribeFileSystem API.

```
PS C:\Users\delegateadmin> enter-psession -computename FSxFileSystem-Remote-PowerShell-Endpoint -configurationname fsxremoteadmin
```

4. Verifica che lo storage delle copie shadow non sia già configurato sul file system utilizzando il comando seguente.

```
[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'-Defaultopzione.

```
[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 dell'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, consulta [Utilizzo dell'Amazon FSx CLI 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).

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 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 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
```

- 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. 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 FSx console Amazon, nella sezione Rete e sicurezza della schermata dei dettagli del file system o nella risposta dell'operazione `DescribeFileSystem` API.

```
PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
```

- Inserisci la riga seguente al `>>` prompt per impostare la pianificazione della copia shadow utilizzando il `set-fsxshadowcopyschedule` comando.

```
>> 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 della copia ombra

Per visualizzare la pianificazione delle copie 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, consulta [Utilizzo dell'Amazon FSx CLI 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

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, consulta [Utilizzo dell'Amazon FSx CLI 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, consulta [Utilizzo dell'Amazon FSx CLI 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, consulta [Utilizzo dell'Amazon FSx CLI 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 copie IDs 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

Eliminazione di una pianificazione di copie shadow

Per eliminare la pianificazione delle copie 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, consulta [Utilizzo dell'Amazon FSx CLI 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>
```

Eliminazione dell'archiviazione, della pianificazione e di tutte le copie shadow

È possibile eliminare la configurazione della copia shadow, incluse tutte le copie shadow esistenti e la 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, consulta [Utilizzo dell'Amazon FSx CLI 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.

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 FSx backup Amazon 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 I/O prestazionale insufficiente del file system (ad esempio, perché si utilizza l'archiviazione 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 disponibile. I/O Prendi in considerazione i seguenti consigli per prevenire questo problema:

- Se utilizzi lo storage su HDD, utilizza la FSx console Amazon o l' FSx API Amazon per passare all'utilizzo dello storage SSD. Per ulteriori informazioni, consulta [Gestione del tipo di storage del file system](#).
- 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 FSx backup Amazon o accedere a copie shadow su un file system ripristinato o aggiornato di recente

Questo è il comportamento previsto. Amazon FSx ricostruisce lo stato shadow-copy su un file system ripristinato di recente e non consente l'accesso a copie shadow o backup mentre la ricostruzione è ancora in corso.

Replica pianificata utilizzando AWS DataSync

È possibile utilizzare AWS DataSync per pianificare la replica periodica del file FSx system Windows File Server su un secondo file system. Questa funzionalità è disponibile sia per le distribuzioni a livello locale che interregionale. Per ulteriori informazioni, consulta [Migrazione dei file esistenti su FSx Windows File Server utilizzando AWS DataSync](#) questa guida e [Trasferimento dati tra servizi di AWS storage](#) nella Guida per l'utente.AWS DataSync

Utilizzo FSx per Windows File Server con Microsoft SQL Server

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

Note

Al momento, 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 la maggior parte dei carichi di lavoro sensibili alla latenza, inclusi i database.

Per informazioni sull'utilizzo di Amazon FSx per ridurre la complessità e i costi delle distribuzioni ad alta disponibilità di SQL Server, consulta i seguenti post sullo AWS Storage Blog:

- [Semplifica le distribuzioni ad alta disponibilità di Microsoft SQL Server utilizzando Amazon FSx per Windows File Server](#)
- [Ottimizzazione dei costi per le distribuzioni di SQL Server ad alta disponibilità su AWS](#)
- [Semplifica le distribuzioni Always On di SQL Server con Launch AWS Wizard e Amazon FSx](#)

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

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 i database SQL Server supportando condivisioni di file a disponibilità continua (CA). Queste condivisioni di file sono progettate per applicazioni come SQL Server che richiedono un accesso ininterrotto ai dati di file condivisi. Sebbene sia possibile creare condivisioni CA su file system Single-AZ 2, è necessario utilizzare le condivisioni CA su file system Multi-AZ per tutte le distribuzioni di SQL Server, con o senza disponibilità elevata.

Crea una condivisione sempre disponibile

Puoi creare condivisioni CA utilizzando Amazon FSx CLI for Remote Management su PowerShell. Per specificare che la condivisione è una condivisione sempre disponibile, usa l'opzione `New-FSxSmbShare` con l'opzione `-ContinuouslyAvailable` impostata su `$True`. Per ulteriori informazioni, consulta [Per creare una condivisione a disponibilità continua \(CA\)](#).

Configurare le impostazioni di timeout SMB

Come descritto in [Processo di failover](#), 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 della condivisione di file per PMI

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

Migrazione dello storage di file esistente su Amazon FSx

Amazon FSx per 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 dello storage locale di Microsoft Windows File Server su Windows File Server prevede i seguenti quattro passaggi principali: FSx

1. Esegui la migrazione dei file su Windows File FSx Server. Per ulteriori informazioni, consulta [Migrazione dello storage di file esistente su Windows File Server FSx](#).
2. Esegui la migrazione della configurazione di condivisione dei file su FSx Windows File Server. Per ulteriori informazioni, consulta [Migrazione delle configurazioni di condivisione di file locali 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. Passato a Windows FSx File Server. Per ulteriori informazioni, consulta [Trasferimento delle operazioni su Amazon FSx for Windows File Server](#).

Puoi trovare i dettagli di ogni fase del processo nelle seguenti sezioni.

Argomenti

- [Migrazione dello storage di file esistente su Windows File Server FSx](#)
- [Migrazione delle configurazioni di condivisione di file locali su Amazon FSx](#)
- [Migrazione della configurazione DNS locale a Windows File Server FSx](#)
- [Trasferimento delle operazioni su Amazon FSx for Windows File Server](#)

Migrazione dello storage di file esistente su Windows File Server FSx

Per migrare i file esistenti verso FSx i file system Windows File Server, si consiglia di utilizzare AWS DataSync un servizio di trasferimento dati online progettato per semplificare, automatizzare e accelerare la copia di grandi quantità di dati da AWS e verso i servizi di archiviazione. DataSync copia i dati su Internet o. 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 dei file esistenti su FSx 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 verso Windows File Server, FSx consulta. [Migrazione di file esistenti su Windows File Server utilizzando Robocopy FSx](#)

Le migliori pratiche per la migrazione dello storage di file esistente su Windows File Server FSx

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

Per spostare i dati da un FSx file system Amazon utilizzando lo storage SSD allo storage HDD, puoi seguire i seguenti passaggi. (Tieni presente che i file system HDD hanno una capacità di archiviazione 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 su un nuovo file system](#).

Migrazione dei file esistenti su FSx Windows File Server utilizzando AWS DataSync

Si consiglia di AWS DataSync utilizzarlo FSx per trasferire dati tra file system 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 servizi di AWS archiviazione su Internet o. 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 NTFS (ACLs) e supporta anche la copia delle informazioni di controllo degli accessi ai file, note anche come liste di controllo degli

accessi di sistema NTFS (SACLs), utilizzate dagli amministratori per controllare la registrazione di controllo dei tentativi degli utenti di accedere ai file.

È possibile utilizzarli DataSync per trasferire file tra due file system FSx per Windows File Server e anche per spostare i dati in un file system con un account OR diverso. Regione AWS AWS È possibile utilizzare DataSync con FSx i file system Windows File Server per altre attività. Ad esempio, è possibile eseguire migrazioni di dati una tantum, inserire periodicamente dati per carichi di lavoro distribuiti e pianificare la replica per la protezione e il ripristino dei dati.

Nel AWS DataSync, una posizione FSx per Windows File Server è un endpoint per un file server per Windows. FSx È possibile trasferire file tra una posizione FSx per Windows File Server e una posizione per altri file system. Per informazioni, vedere [Lavorare con le posizioni](#) nella Guida AWS DataSync per l'utente.

DataSync accede al file server FSx per 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 DataSync requisiti. 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 Amazon FSx File System 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: [Le migliori pratiche per la migrazione dello storage di file esistente su Windows File Server FSx](#).

Se il set di dati è composto principalmente da file di piccole dimensioni, con un numero di file che si aggira intorno ai milioni, o se disponi di una larghezza di banda di rete superiore a quella che può consumare 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' I/O utilizzo del disco del file system utilizzando FSx metriche prestazionali.](#)

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 al tuo FSx per Windows File Server, consulta [Trasferimento di dati tra storage autogestito e AWS](#), [Creazione di una posizione per SMB](#) e [Creazione di una posizione per Amazon FSx for Windows File Server](#) nella Guida per l'AWS DataSync utente.

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

Migrazione tra due FSx file system Amazon

Puoi utilizzarlo DataSync per migrare i dati tra due FSx file system Amazon. 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: [Accesso ai dati tramite alias DNS](#)

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.
- Utilizzate un tipo di storage SSD per i file system di origine e di destinazione. Puoi passare dai tipi di storage HDD a SSD eseguendo il ripristino dal backup. Per ulteriori informazioni, vedere: [Migrazione dello storage di file esistente su Windows File Server FSx](#)
- 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 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 Windows File Server utilizzando Robocopy FSx

Basato su Microsoft Windows Server, Amazon FSx for Windows File Server ti consente di migrare completamente i set di dati esistenti nei tuoi FSx file system Amazon. 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 (ACLs), informazioni sui proprietari e informazioni di controllo. Con questo supporto totale per la migrazione, Amazon FSx consente di spostare i carichi di lavoro e le 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. Durante l'esecuzione di questa copia, conservi tutti i metadati dei file dai data center locali o dai file server autogestiti su Amazon EC2.

Prerequisiti per la migrazione dei file con Robocopy

Prima di iniziare, assicurati di effettuare queste operazioni:

- Stabilisci la connettività di rete (utilizzando Direct Connect o VPN) tra il tuo Active Directory locale e il VPC in cui desideri creare il file system FSx Amazon.
- 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 FSx file system Amazon, 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.
- Annota la posizione (ad esempio \\Target\Share) della condivisione di file sul tuo FSx file system Amazon a cui desideri trasferire i file esistenti.

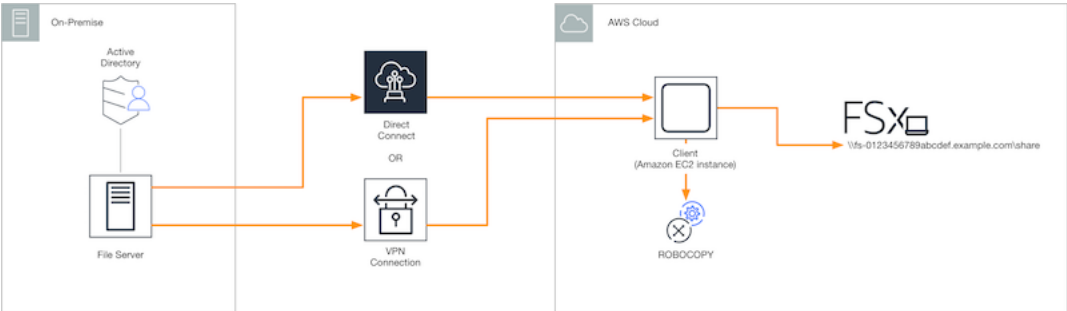
La tabella seguente riassume i requisiti di accessibilità del file system di origine e di destinazione per tre modelli di accesso utente di migrazione.

Modello di accesso utente per la migrazione	Requisiti di accessibilità del file system di origine	Requisiti di accessibilità del FSx file server di destinazione
Modello di read/write autorizzazioni dirette	L'utente deve disporre almeno delle autorizzazioni	L'utente deve disporre almeno delle autorizzazioni

Modello di accesso utente per la migrazione	Requisiti di accessibilità del file system di origine	Requisiti di accessibilità del FSx file server di destinazione
	di lettura (NTFS ACLs) per i file e le cartelle da migrare.	di scrittura (NTFS ACLs) per i file e le cartelle da migrare.
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 utilizzare il flag /b con. RoboCopy	L'utente deve essere membro del gruppo di amministratori del FSx file system Amazon* e utilizzare 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 FSx file system Amazon* e utilizzare il flag /b con RoboCopy

 **Note**

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



Migrazione dei file con Robocopy

È possibile migrare i file esistenti dai file system locali ai FSx file system Windows File Server utilizzando la procedura seguente.

Per migrare i file esistenti su Amazon FSx utilizzando Robocopy

1. Avvia un'istanza Amazon EC2 per Windows Server 2016 nello stesso Amazon VPC del tuo 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 FSx file system Amazon 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 FSx file system Amazon. 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 per la migrazione dei file con Robocopy](#)

```
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 FSx destinazione Amazon. La copia conserva il file NTFS di file e cartelle ACLs, 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 — NTFS ACLs
 - 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 il relativo NTFS ACLs nega le autorizzazioni all'utente corrente.
- /MT:8 — Specifica 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 `/zb` al posto dell'opzione `/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 locali 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 della condivisione di file. Per ulteriori informazioni, consulta [Migrazione dello storage di file esistente su Windows File Server FSx](#).

Per migrare le condivisioni di file esistenti su Windows File FSx 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 tuo 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 FSx file system Amazon risiedono su `D:\share`.

4. Importa la configurazione di condivisione di file esistente FSx in Windows File Server. Su un client che ha accesso al FSx file system Amazon 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-Clxml -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 Gestione dei segreti AWS risorsa, utilizzate il comando seguente.

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

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

```
$FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",
  "ConcurrentUserLimit", "CTimeout", "FolderEnumerationMode", "CachingMode",
  "FullAccess", "ChangeAccess", "ReadAccess", "NoAccess", "SecurityDescriptor",
  "Path", "Name", "EncryptData")
ForEach ($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
  amznfsxxxxxxxxxx.corp.com -ErrorVariable errormsg -ScriptBlock { New-FSxSmbShare -
  Credential $Using:credential @Using:param }
}
```

Migrazione della configurazione DNS locale a Windows File Server FSx

FSx per Windows File Server fornisce un nome DNS (Domain Name System) predefinito per ogni file system che è possibile utilizzare per accedere ai dati del 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 tuoi nomi DNS durante la migrazione ad Amazon. FSx Puoi associare gli alias DNS ai file system esistenti FSx per Windows File Server, quando crei nuovi file system e quando crei 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 memorizza i caratteri alfabetici come lettere minuscole (a-z), indipendentemente da come li specifichi: come lettere maiuscole, lettere minuscole o le lettere corrispondenti nei codici di escape.

Le seguenti procedure descrivono come associare gli alias DNS ai file system esistenti FSx per Windows File Server utilizzando la FSx console Amazon, la CLI e l'API. 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 FSx console Amazon 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.

Manage DNS aliases

Associate new DNS aliases

transactions.corp.example.com

Specify up to 50 aliases separated with commas, or put each on a new line.

Associate

Current DNS aliases (1)

filesystem.domain.name.com

< 1 >

☐	DNS name	Status
☐	financials.corp.example.com	Available

If you associate or disassociate DNS aliases, your file system will experience a temporary loss of availability.

Close

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 [AssociateFileSystemAliases](#) API 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 ([DescribeFileSystemAliases](#) è 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).

Trasferimento delle operazioni su Amazon FSx for Windows File Server

Dopo aver migrato l'archiviazione di file locale, la configurazione della condivisione di file e la configurazione DNS, il passaggio successivo consiste nel trasferire le operazioni ai file system Windows File Server. FSx Per eseguire il trasferimento al file system FSx per 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 dei servizi (SPNs) per il tuo FSx file system Amazon.
- Aggiorna i record DNS CNAME in modo che puntino al tuo FSx file system Amazon.

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

Argomenti

- [Preparazione per il passaggio ad Amazon FSx](#)
- [Configura SPNs per l'autenticazione Kerberos](#)
- [Aggiorna i record DNS CNAME per il file system Amazon FSx](#)

Preparazione per il passaggio ad Amazon FSx

Per prepararti al cutover del tuo FSx file system Amazon, 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 Windows File Server FSx](#).
- Esegui una sincronizzazione finale della configurazione della condivisione di file. Per ulteriori informazioni, consulta [Migrazione delle configurazioni di condivisione di file locali su Amazon FSx](#).

Configura SPNs 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 tuo file system. Per abilitare l'autenticazione Kerberos per i client che accedono ad Amazon FSx utilizzando un alias DNS, devi aggiungere i nomi principali del servizio (SPNs) che corrispondono all'alias DNS sull'oggetto computer Active Directory del tuo FSx file system Amazon.

Ce ne sono due necessari per l'autenticazione Kerberos. SPNs

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

Ad esempio, se l'alias è `finance.domain.com`, i due richiesti SPNs 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 oggetti SPNs per il nome DNS configurato per il computer Active Directory del tuo file system originale, devi eliminarli prima di crearli SPNs per il tuo FSx file system Amazon.

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

Per installare il modulo PowerShell Active Directory richiesto

1. Accedi a un'istanza Windows aggiunta all'Active Directory a cui è collegato il tuo FSx file system Amazon.
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 l'alias DNS esistente nell' SPNs oggetto computer Active Directory del file system originale

1. SPNs Trovate quelli esistenti utilizzando i seguenti comandi. Sostituiscilo `alias_fqdn` con l'alias DNS associato al file system in. [Migrazione della configurazione DNS locale a Windows File Server 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 l'HOST esistente SPNs restituito 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 locale a Windows File Server 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 locale a Windows File Server FSx](#)

Da impostare SPNs sull'oggetto informatico Active Directory del tuo FSx file system Amazon

1. Imposta SPNs un nuovo FSx file system Amazon eseguendo i seguenti comandi.
 - Sostituisci *file_system_DNS_name* con il nome DNS FSx assegnato da Amazon al file system.

Per trovare il nome DNS del tuo file system sulla FSx console Amazon, 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 [DescribeFileSystemsAPI](#).

- Sostituiscilo *alias_fqdn* con l'alias DNS completo in cui hai associato il file system. [Migrazione della configurazione DNS locale a Windows File Server 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 tuo FSx file system Amazon 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 elementi esistenti, consulta [SPNs Per trovare ed eliminare l'alias DNS esistente nell' SPNs oggetto computer Active Directory del file system originale](#)

2. Verificate che i nuovi alias SPNs siano configurati per l'alias DNS utilizzando lo script di esempio seguente. Assicurati che la risposta includa due HOST SPNs eHOST/*alias*. HOST/*alias_fqdn*

Sostituiscilo *file_system_dns_name* con il nome DNS FSx assegnato da Amazon al tuo file system. Per trovare il nome DNS del tuo file system sulla FSx console Amazon, 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 [DescribeFileSystemsAPI](#).

```
## 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 locale a Windows File Server 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 utilizzando Group Policy Objects \(\) GPOs](#) la procedura dettagliata 5: Utilizzo degli alias DNS per accedere al file system.

Aggiorna i record DNS CNAME per il file system Amazon FSx

Dopo aver SPNs configurato correttamente il 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

Per installare i cmdlet richiedi PowerShell

1. Accedi a un'istanza Windows aggiunta ad Active Directory a cui fa parte il tuo FSx file system Amazon come utente membro di un gruppo con autorizzazioni di amministrazione DNS (amministratori di sistema con nomi di dominio AWS delegati in AWS Microsoft Active Directory gestita e amministratori di dominio o un altro gruppo a cui hai delegato le autorizzazioni di amministrazione DNS nella tua Active Directory gestita autonomamente)

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 tuo FSx file system Amazon. 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 tuo file system Amazon. FSx

Per eseguire lo script:

- *alias_fqdn* Sostituiscilo con l'alias DNS associato al file system.
- Sostituisci *file_system_DNS_name* con il nome DNS predefinito FSx che Amazon 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 locale a Windows File Server FSx](#)

FSx Monitoraggio dei file system Windows File Server

Il monitoraggio è un elemento importante FSx per mantenere l'affidabilità, la disponibilità e le prestazioni di Windows File Server e delle tue AWS soluzioni. È consigliabile raccogliere i dati di monitoraggio da tutte le parti della AWS soluzione in modo da poter eseguire più facilmente il debug di un eventuale errore. Tuttavia, prima di iniziare il monitoraggio FSx per Windows File Server, 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 FSx per Windows File Server, vedere i seguenti argomenti.

Argomenti

- [Monitoraggio automatico e manuale](#)
- [Monitoraggio con Amazon CloudWatch](#)
- [Registrazione delle chiamate API Amazon FSx per Windows File Server utilizzando AWS CloudTrail](#)

Monitoraggio automatico e manuale

AWS fornisce diversi strumenti che è possibile utilizzare FSx per il monitoraggio di Windows File Server. È possibile configurare alcuni di questi strumenti in modo che eseguano il monitoraggio automaticamente, 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 FSx per controllare Windows File Server 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 politica di Amazon Auto EC2 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 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 FSx di Windows File Server prevede il monitoraggio manuale degli elementi che gli CloudWatch allarmi di Amazon non coprono. I dashboard FSx per Windows File Server e altre AWS console forniscono una at-a-glance panoramica dello stato dell'ambiente AWS . CloudWatch

Il dashboard FSx di monitoraggio e prestazioni di Amazon mostra:

- Avvisi e CloudWatch allarmi attuali
- Un riepilogo dell'attività del file system
- Capacità e utilizzo dello storage del file system
- Prestazioni dei file server e dei volumi di storage
- CloudWatch allarmi

Amazon CloudWatch Dashboard mostra:

- Stato e allarmi attuali
- Grafici degli allarmi e delle risorse

- Stato di integrità dei servizi

Inoltre, puoi 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 sulla dashboard di FSx monitoraggio e prestazioni di Amazon, consulta [Utilizzo delle metriche del file system](#).

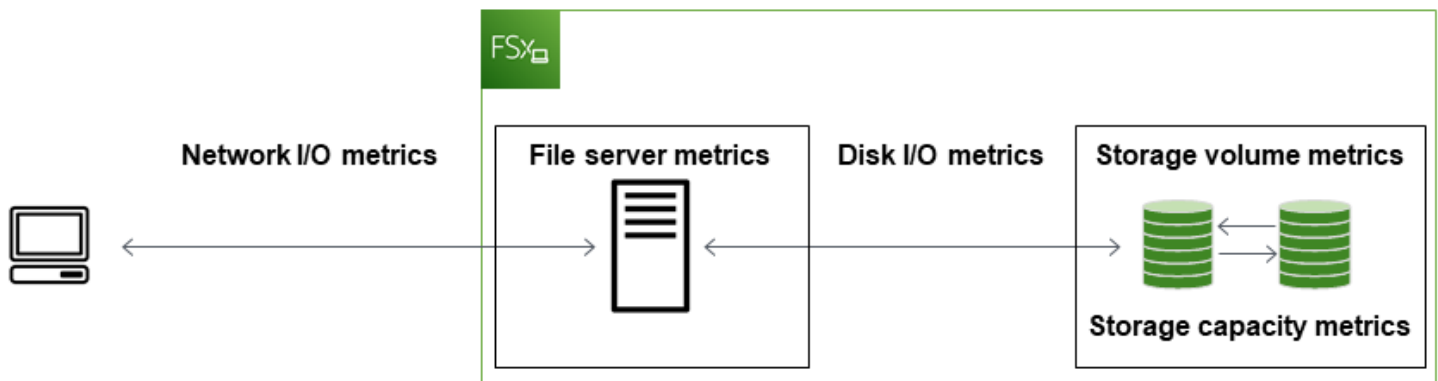
Monitoraggio con Amazon CloudWatch

Amazon CloudWatch raccoglie ed elabora i dati grezzi dal tuo file system FSx per Windows File Server in metriche leggibili quasi in tempo reale. Queste statistiche vengono conservate per un periodo di 15 mesi, consentendoti di accedere a informazioni storiche per aiutarti a ottenere prospettive sulle prestazioni del flusso di lavoro o del file system.

FSx per Windows File Server pubblica CloudWatch 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 del throughput 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 per 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 FSx CloudWatch metriche di Amazon sono riportate come byte non elaborati. I byte non sono arrotondati a un multiplo decimale o binario dell'unità.

Argomenti

- [CloudWatch metriche e dimensioni](#)
- [Utilizzo delle metriche del file system](#)
- [Avvertenze e raccomandazioni sulle prestazioni](#)
- [Accesso alle metriche del file system](#)
- [Creazione di CloudWatch allarmi](#)

CloudWatch metriche e dimensioni

FSx per Windows File Server pubblica le seguenti metriche nello spazio dei nomi AWS/FSx di CloudWatch Amazon per tutti i file system:

- DataReadBytes
- DataWriteBytes
- DataReadOperations
- DataWriteOperations
- MetadataOperations
- FreeStorageCapacity

FSx per Windows File Server pubblica le metriche descritte nelle seguenti sezioni nello spazio dei AWS/FSx nomi di CloudWatch Amazon per i file system configurati con una capacità di throughput di almeno 32. MBps

Metriche di I/O di rete

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 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.

Parametro	Descrizione
MetadataOperations	Unità: numero
	Statistiche valide: Sum
	Il numero di operazioni sui metadati per i client che accedono al file system.
	Unità: numero
ClientConnections	Statistiche valide: Sum
	Il numero di connessioni attive tra i client e il file server.
	Unità: numero

Metriche del file server

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. Unità: percentuale
MemoryUtilization	La percentuale di utilizzo delle risorse di memoria del file server. Unità: percentuale

Parametro	Descrizione
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 del disco

Lo spazio dei nomi AWS/FSx 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

Parametro	Descrizione
	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

FSx per le metriche del volume di archiviazione di 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. Unità: percentuale
DiskThroughputBalance	(Solo HDD) La percentuale di crediti burst disponibili per la velocità effettiva del disco e gli IOPS del disco per i volumi di archiviazione.

Parametro	Descrizione
	Unità: percentuale
DiskIopsUtilization	(Solo SSD) Gli IOPS del disco tra il server di file e i volumi di storage, come percentuale del limite IOPS assegnato determinato dai volumi di archiviazione. Unità: percentuale

Parametri della capacità di archiviazione

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 percentuale della capacità di archiviazione totale. Unità: percentuale
DeduplicationSavedStorage	La quantità di spazio di archiviazione risparmiata dalla deduplicazione dei dati, se abilitata. Unità: byte

Namespace e dimensioni per le metriche di Windows FSx File Server

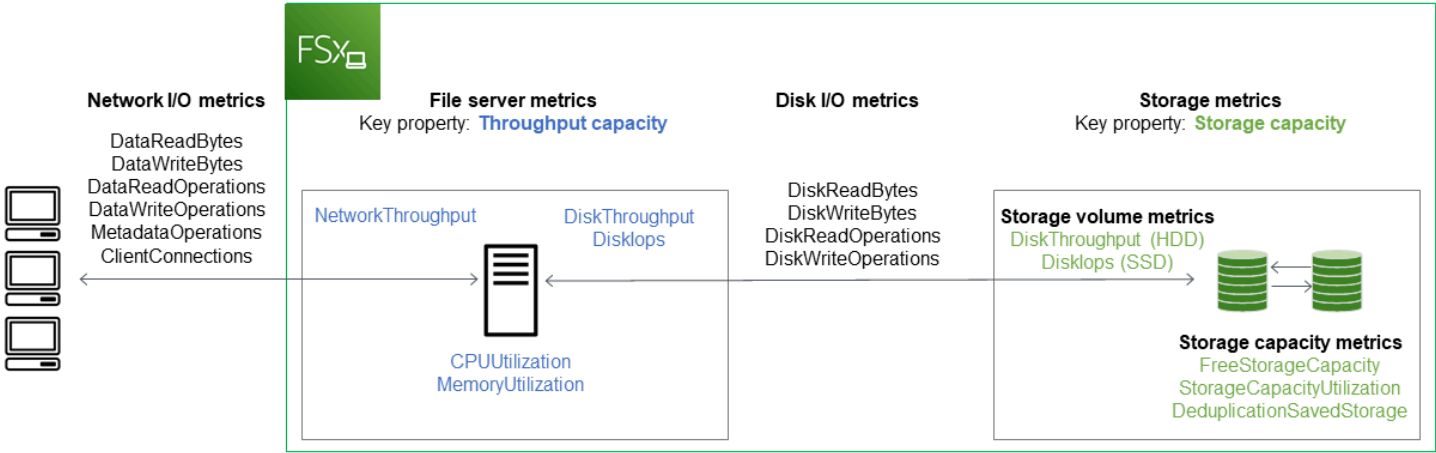
FSx per le metriche di Windows File Server utilizzano lo spazio dei FSx nomi e forniscono metriche per una singola dimensione,. FileSystemId È possibile trovare l'ID di un file system utilizzando il [describe-file-systems](#) AWS CLI comando o il comando API. [DescribeFileSystems](#) Un ID del file system assume la forma di *fs-0123456789abcdef0*.

Utilizzo delle metriche del file system

Esistono due componenti architettonici principali di ogni FSx file system Amazon:

- 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 per Windows File Server riporta metriche CloudWatch che tengono traccia delle prestazioni e dell'utilizzo delle risorse per il file server e i volumi di archiviazione del file system. Il diagramma seguente illustra un FSx file system Amazon con i suoi componenti architettonici e le CloudWatch metriche di prestazioni e risorse disponibili per il monitoraggio. La proprietà chiave mostrata per un set di metriche è la proprietà del file system che determina la capacità di tali metriche. La regolazione di tale proprietà modifica le prestazioni del file system per quel set di metriche.



Utilizza il pannello Monitoraggio e prestazioni nella FSx console Amazon per visualizzare i CloudWatch parametri FSx per Windows File Server descritti nella tabella seguente.

Pannello	Come posso...	Grafico	Parametri rilevanti
Monitoraggio e prestazioni	... determinare gli IOPS totali del mio file system?	IOPS totali	SUM (DataReadOperations + DataWriteOperations)

Pannello	Come posso...	Grafico	Parametri rilevanti
Monitoraggio e prestazioni			+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 dalla deduplicazione dei dati	DeduplicationSavedStorage

Pannello	Come posso...	Grafico	Parametri rilevanti
Monitoraggio e prestazioni	... 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 ¹
	... 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 ¹
	... 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
	... 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

Pannello	Come posso...	Grafico	Parametri rilevanti
Monitoraggio e prestazioni	... 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 throughput disponibile e i crediti burst IOPS per le operazioni che accedono ai volumi di storage degli HDD?	Disk Throughput Burst Balance (HDD)	DiskThroughputBalance ²
	... determinare gli IOPS per le operazioni che accedono ai volumi di storage, come percentuale del limite previsto determinato dalla capacità di storage dell'HDD?	Utilizzo degli IOPS del disco (HDD)	SUM (DiskReadOperations + DiskWriteOperations) / Period(in secondi) / (12 * capacità di storage HDD fornita in TiB)
	... determinare gli IOPS per le operazioni che accedono ai volumi di storage, come percentuale del limite assegnato determinato dalla capacità di storage SSD?	Utilizzo degli IOPS del disco (SSD)	DiskIopsUtilization

 Note

¹ Si consiglia di mantenere un utilizzo medio della capacità di throughput inferiore al 50% per garantire una capacità di throughput di riserva sufficiente in caso di picchi imprevisti del carico di lavoro e per eventuali operazioni di storage Windows in background (come sincronizzazione dello storage, deduplicazione o copie shadow).

² I volumi di storage HDD possono subire variazioni significative delle prestazioni a seconda del carico di lavoro. I picchi improvvisi degli IOPS o del throughput possono portare a un peggioramento delle prestazioni del disco. Per ulteriori informazioni, consulta [Prestazioni HDD burst](#).

Avvertenze e raccomandazioni sulle prestazioni

FSx per 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 si avvicina o supera 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 della dashboard di monitoraggio e prestazioni. Tutti gli avvisi FSx sulle prestazioni di Amazon attivi o recenti e tutti gli CloudWatch allarmi configurati per il file system che si trovano in uno stato ALARM vengono visualizzati nel pannello Monitoraggio e prestazioni nella sezione Riepilogo. L'avviso appare anche nella sezione del pannello di controllo in cui viene visualizzato il grafico metrico.

Puoi creare CloudWatch allarmi per qualsiasi FSx metrica di Amazon. Per ulteriori informazioni, consulta [Creazione di CloudWatch allarmi](#).

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	
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. [FSx per le prestazioni di Windows File Server](#)

Accesso alle metriche del file system

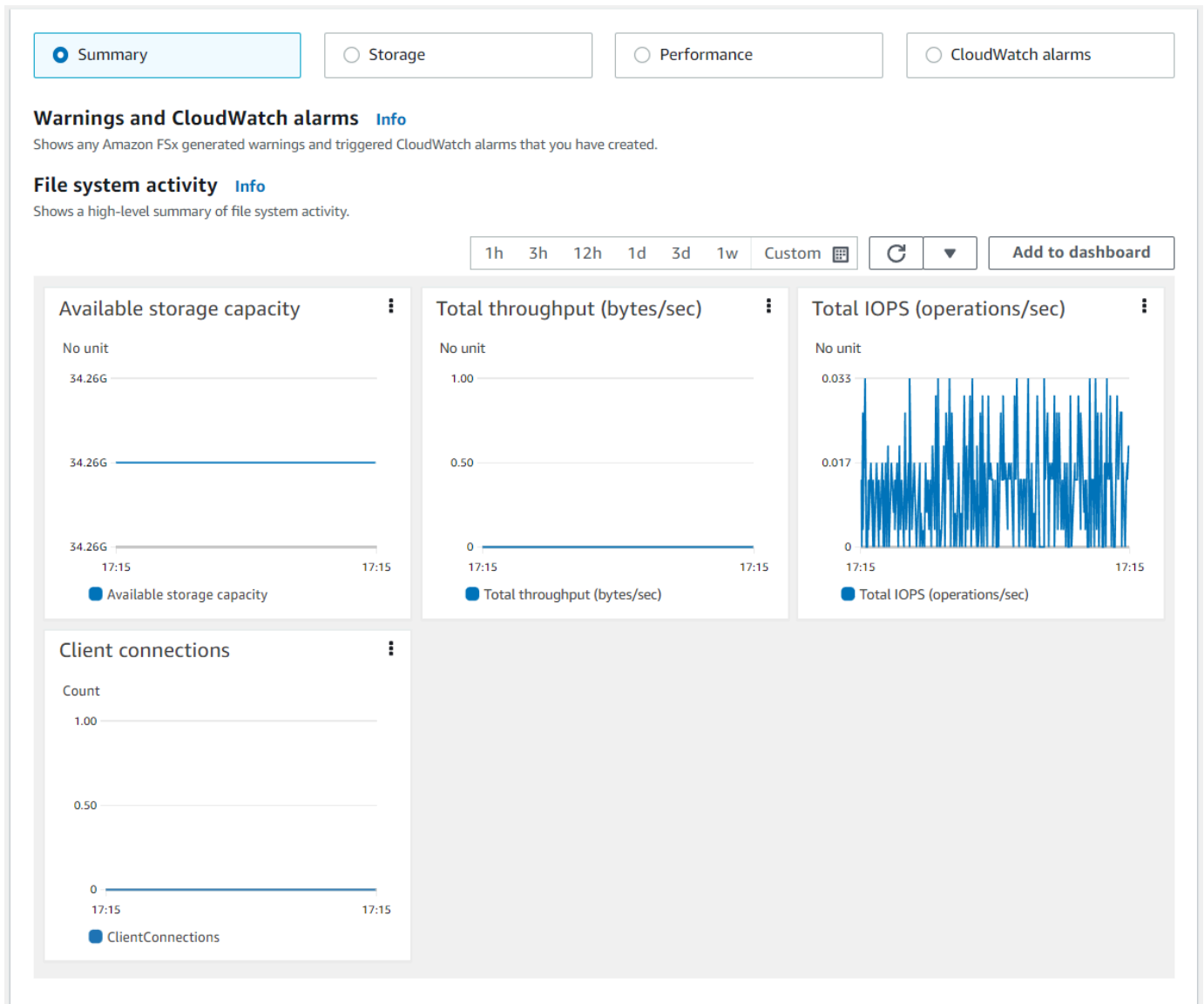
Puoi visualizzare i FSx parametri di Amazon CloudWatch nei seguenti modi.

- La FSx console Amazon
- La CloudWatch console
- La CloudWatch CLI
- 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 FSx console Amazon 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.

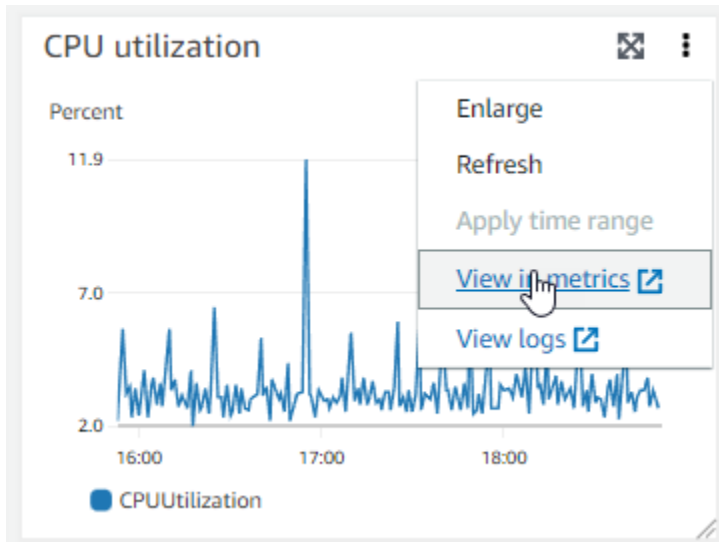


- Le metriche di riepilogo vengono visualizzate per impostazione predefinita e mostrano eventuali avvisi e CloudWatch allarmi attivi insieme alle metriche di attività del file system.
- Scegli Archiviazione per visualizzare la capacità di archiviazione e le metriche di utilizzo.
- Scegli Performance 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.

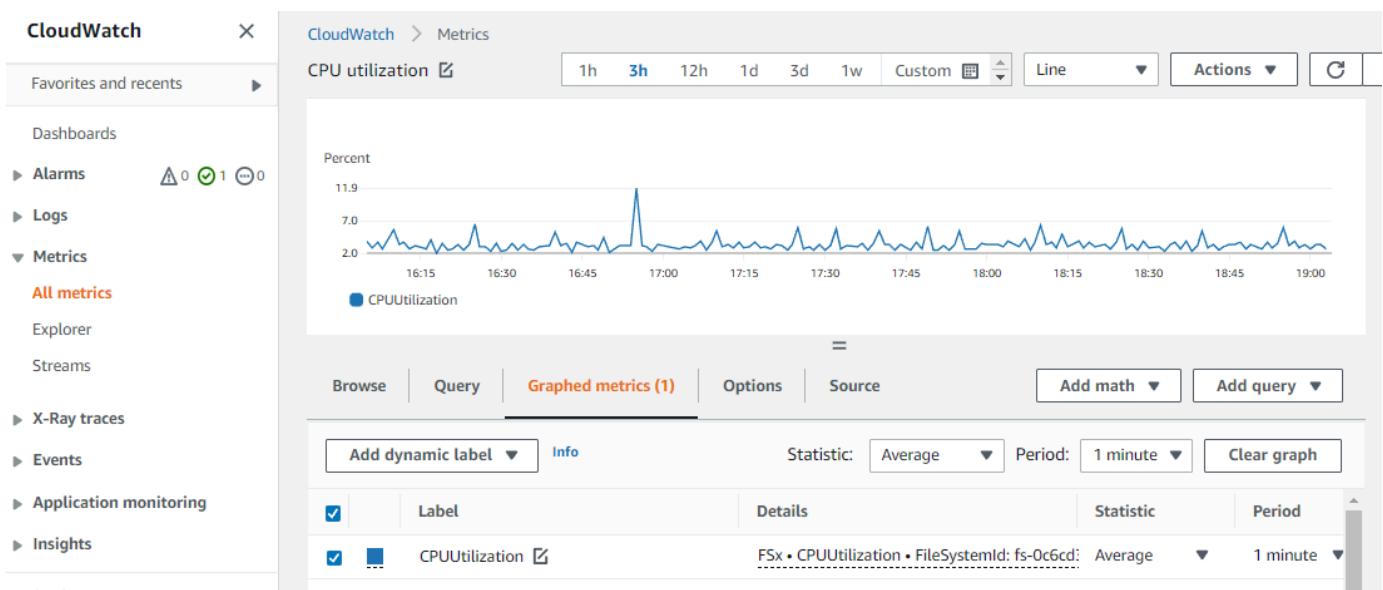
Per ulteriori informazioni, consulta [Utilizzo delle metriche del file system](#)

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 FSx parametri del file system Windows a una dashboard nella CloudWatch console, scegli il set di parametri (Riepilogo, Archiviazione o Prestazioni) nel pannello Monitoraggio e prestazioni della console Amazon FSx .
2. Scegli Aggiungi alla dashboard in alto a destra del pannello per aprire la CloudWatch console.
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](#).

```
$ aws cloudwatch list-metrics --namespace "AWS/FSx"
aws cloudwatch list-metrics --namespace "AWS/FSx"
{
  "Metrics": [
    {
      "Namespace": "AWS/FSx",
      "MetricName": "DataWriteOperationTime",
      "Dimensions": [
        {
          "Name": "FileSystemId",
          "Value": "fs-09a106ebc3a0bb087"
        }
      ]
    },
    {
      "Namespace": "AWS/FSx",
      "MetricName": "CapacityPoolWriteBytes",
      "Dimensions": [
        {
          "Name": "VolumeId",
          "Value": "fsvol-0cb2281509f5db3c2"
        },
        {
          "Name": "FileSystemId",
          "Value": "fs-09a106ebc3a0bb087"
        }
      ]
    }
  ]
}
```

```

    ]
  },
  {
    "Namespace": "AWS/FSx",
    "MetricName": "DiskReadBytes",
    "Dimensions": [
      {
        "Name": "FileSystemId",
        "Value": "fs-09a106ebc3a0bb087"
      }
    ]
  },
  {
    "Namespace": "AWS/FSx",
    "MetricName": "CompressionRatio",
    "Dimensions": [
      {
        "Name": "FileSystemId",
        "Value": "fs-0f84c9a176a4d7c92"
      }
    ]
  },
  .
  .
  .
}

```

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

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 FSx console Amazon o dalla CloudWatch console.

Le seguenti procedure descrivono come creare allarmi per Amazon FSx utilizzando la console e AWS CLI l'API.

Per impostare una CloudWatch sveglia (console)

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Dal pannello di navigazione, scegli File system, quindi scegli il file system per cui desideri creare l'allarme.
3. 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. Scegli Next (Successivo).

 Note

Se usi Crea argomento per creare un nuovo argomento Amazon SNS, gli indirizzi e-mail devono essere verificati prima di poter ricevere le notifiche. Le e-mail sono inviate solo quando 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 a Console di gestione AWS e apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Scegli Crea allarme per avviare la procedura guidata di creazione di allarme.
3. Scegli FSx Metriche e scorri le FSx metriche di Amazon per individuare la metrica su cui desideri inserire un allarme. Per visualizzare solo le FSx metriche di Amazon 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 un CloudWatch allarme (CLI)

- Chiamare [put-metric-alarm](#). Per ulteriori informazioni, consulta il [Riferimento ai comandi AWS CLI](#).

Per impostare un allarme (API)

- Chiama [PutMetricAlarm](#). Per ulteriori informazioni, consulta [Amazon CloudWatch API Reference](#).

Registrazione delle chiamate API Amazon FSx per Windows File Server utilizzando AWS CloudTrail

Amazon FSx for Windows File Server è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un AWS servizio in Amazon FSx. CloudTrail acquisisce tutte le chiamate API per Amazon FSx come eventi. Le chiamate acquisite includono chiamate dalla FSx console Amazon e chiamate in codice alle operazioni dell' FSx API Amazon. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon. FSx Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare la richiesta che è stata effettuata ad Amazon FSx, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per ulteriori informazioni CloudTrail, consulta la [Guida AWS CloudTrail per l'utente](#).

FSx Informazioni su Amazon in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in Amazon FSx, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi AWS di servizio nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti nel tuo Account AWS. Per ulteriori informazioni, consulta [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi del tuo sito Account AWS, compresi gli eventi per Amazon FSx, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il trail registra gli eventi di tutte le regioni della AWS partizione e consegna i file di log al bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei log. CloudTrail Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un percorso](#)
- [CloudTrail servizi e integrazioni supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)
- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Tutte le FSx azioni di Amazon vengono registrate CloudTrail e documentate nell'[Amazon FSx API Reference](#). Ad esempio, le chiamate CreateBackup e TagResource le azioni generano voci nei file di CloudTrail registro. CreateFileSystem

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Comprendere le voci dei file di FSx log di Amazon

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra il TagResource funzionamento quando viene creato un tag per un file system dalla console.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:sts::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-14T22:36:07Z"
      }
    }
  },
  "eventTime": "2018-11-14T22:36:07Z",
  "eventSource": "fsx.amazonaws.com",
  "eventName": "TagResource",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-ab12cd34ef56gh789"
  },
  "responseElements": null,
  "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
  "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
  "eventType": "AwsApiCall",
  "apiVersion": "2018-03-01",
```

```
"recipientAccountId": "111122223333"
}
```

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'UntagResourceazione che si verifica quando un tag per un file system viene eliminato dalla console.

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "Root",
    "principalId": "111122223333",
    "arn": "arn:aws:sts::111122223333:root",
    "accountId": "111122223333",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "sessionContext": {
      "attributes": {
        "mfaAuthenticated": "false",
        "creationDate": "2018-11-14T23:40:54Z"
      }
    }
  },
  "eventTime": "2018-11-14T23:40:54Z",
  "eventSource": "fsx.amazonaws.com",
  "eventName": "UntagResource",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "192.0.2.0",
  "userAgent": "console.amazonaws.com",
  "requestParameters": {
    "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-ab12cd34ef56gh789"
  },
  "responseElements": null,
  "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
  "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
  "eventType": "AwsApiCall",
  "apiVersion": "2018-03-01",
  "recipientAccountId": "111122223333"
}
```

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 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 conformità AWS](#). Per informazioni sui programmi di conformità applicabili ad Amazon FSx for Windows File Server, consulta [AWS Services in Scope by Compliance Program](#).
- **Sicurezza nel cloud:** la tua responsabilità è determinata dal AWS servizio che utilizzi. L'utente è anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della propria azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon FSx for Windows File Server. I seguenti argomenti mostrano come configurare Amazon FSx for Windows File Server 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

- [Protezione dei dati in Amazon FSx per Windows File Server](#)
- [Controllo degli accessi a livello di file e cartella tramite Windows ACLs](#)
- [Controllo degli accessi ai file system con Amazon VPC](#)
- [Registrazione dell'accesso dell'utente finale con il controllo dell'accesso ai file](#)
- [Gestione delle identità e degli accessi per Amazon FSx for Windows File Server](#)
- [Convalida della conformità per Amazon FSx for Windows File Server](#)
- [Amazon FSx per Windows File Server e endpoint VPC di interfaccia](#)

Protezione dei dati in Amazon FSx per Windows File Server

Il modello di [responsabilità AWS condivisa modello](#) si applica alla protezione dei dati in Amazon FSx per Windows File Server. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta [Lavorare con i CloudTrail percorsi](#) nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-3](#).

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò vale anche quando si lavora con FSx Windows File Server o altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Crittografia dei dati FSx per Windows File Server

Amazon FSx per Windows File Server supporta la crittografia dei dati inattivi e la crittografia dei dati in transito. La crittografia dei dati inattivi viene abilitata automaticamente durante la creazione di un FSx file system Amazon. 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. Amazon crittografa FSx automaticamente i dati in transito utilizzando la crittografia SMB quando accedi al tuo file system senza che tu debba modificare le tue 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.

Se la tua organizzazione è soggetta a politiche aziendali o normative che richiedono la crittografia dei dati e dei metadati inattivi, i tuoi dati vengono automaticamente crittografati quando sono inattivi. Si consiglia inoltre di abilitare la crittografia dei dati in transito installando il file system utilizzando la crittografia dei dati in transito.

Crittografia dei dati a riposo

Tutti i FSx file system Amazon 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 devi modificare le tue applicazioni.

Amazon FSx utilizza un algoritmo di crittografia AES-256 standard di settore per crittografare dati e metadati Amazon FSx inattivi. Per ulteriori informazioni, consulta [Elementi di base di crittografia](#) nella Guida per sviluppatori di AWS Key Management Service .

Note

L'infrastruttura di gestione delle AWS chiavi utilizza algoritmi crittografici approvati dal Federal Information Processing Standards (FIPS) 140-2. L'infrastruttura è compatibile con le raccomandazioni National Institute of Standards and Technology (NIST) 800-57.

Come FSx utilizza Amazon AWS KMS

Amazon FSx si integra con AWS KMS per la gestione delle chiavi. Amazon FSx utilizza un'AWS KMS key per crittografare il tuo 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

Politiche Amazon FSx Key per AWS KMS

Le policy chiave sono lo strumento principale per controllare l'accesso alle chiavi KMS. Per ulteriori informazioni sulle politiche chiave, consulta la sezione [Utilizzo delle politiche chiave AWS KMS](#) nella Guida per gli AWS Key Management Service sviluppatori. L'elenco seguente descrive tutte le autorizzazioni AWS KMS relative supportate da Amazon FSx per i file system crittografati a riposo:

- kms:Encrypt - (Facoltativa) Crittografa testo normale in testo criptato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms:Decrypt - (Obbligatoria) Decifra il testo criptato. Il testo cifrato è un testo normale che è stato precedentemente crittografato. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: ReEncrypt — (Facoltativo) Crittografa i dati sul lato server con una nuova chiave KMS, senza esporre il testo in chiaro dei dati sul lato client. I dati sono prima decifrati e quindi nuovamente crittografati. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: GenerateDataKeyWithoutPlaintext — (Obbligatorio) Restituisce una chiave di crittografia dei dati crittografata con una chiave KMS. Questa autorizzazione è inclusa nella politica delle chiavi predefinita in kms: *. GenerateDataKey

- kms: CreateGrant — (Obbligatorio) Aggiunge una concessione a una chiave per specificare chi può utilizzare la chiave e in quali condizioni. I grant sono meccanismi di autorizzazioni alternative alle policy sulle chiavi. Per ulteriori informazioni sulle sovvenzioni, consulta [Using grants](#) nella Developer Guide. AWS Key Management Service Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: DescribeKey — (Obbligatorio) Fornisce informazioni dettagliate sulla chiave KMS specificata. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.
- kms: ListAliases — (Facoltativo) Elenca tutti gli alias chiave dell'account. Quando usi la console per creare un file system crittografato, questa autorizzazione compila l'elenco delle chiavi KMS. Consigliamo di usare questa autorizzazione per garantire la migliore esperienza utente. Questa autorizzazione è inclusa nella policy sulla chiave predefinita.

Crittografia dei dati in transito

La crittografia dei dati in transito è supportata nelle condivisioni di file mappate su un'istanza di calcolo che supporta il protocollo SMB 3.0 o versione successiva. 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 garantisce 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.

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 per 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 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'Amazon FSx CLI 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). Nella risposta del sistema è possibile determinare la crittografia nelle impostazioni di transito per il file system in base ai valori delle proprietà <code>and. EncryptData</code> <code>RejectUnencryptedAccess</code>
Set-FSxSmbServerConfiguration	Questo comando ha due opzioni per configurare la crittografia in transito a livello globale sul file system: • <code>-EncryptData \$True \$False</code> — Imposta questo parametro su <code>True</code> per attivare la crittografia dei dati in transito. Imposta questo parametro su <code>False</code> per disattivare la crittografia dei dati in transito. • <code>-RejectUnencryptedAccess \$True \$False</code> — Impostate questo parametro per <code>True</code> impedire ai client che

Encryption in Transit Command	Descrizione
	non supportano la crittografia di accedere al file system. Impostare questo parametro per consentire <code>False</code> ai client che non supportano la crittografia di accedere al file system.
<code>Set-FSxSmbShare -name <i>name</i> -EncryptData \$True</code>	Imposta questo parametro su <code>True</code> per attivare la crittografia dei dati in transito per la condivisione. Imposta questo parametro su <code>False</code> per disattivare la crittografia dei dati in transito per la 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 `Get-FSxSmbServerConfiguration -?`.

Controllo degli accessi a livello di file e cartella tramite Windows ACLs

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 [Lavorare con Microsoft Active Directory](#).

Le tue istanze di calcolo aggiunte al dominio possono accedere alle condivisioni di file FSx Amazon utilizzando le credenziali di Active Directory. Utilizzi elenchi di controllo degli accessi standard di Windows (ACLs) per un controllo granulare degli accessi a livello di file e cartelle. I FSx file system Amazon verificano automaticamente le credenziali degli utenti che accedono ai dati del file system per applicare questi Windows ACLs.

Ogni FSx file system Amazon viene fornito con una condivisione di file Windows predefinita denominata `share`. Le finestre ACLs relative a questa cartella condivisa sono configurate per consentire l' `read/write` accesso agli utenti autenticati, inclusi gli utenti del dominio a cui fa parte il file system e gli utenti dei domini con una relazione di fiducia. Consentono inoltre il pieno controllo del gruppo di amministratori delegati di Active Directory, incaricato di eseguire azioni amministrative.

sui file system. Se stai integrando il tuo file system con AWS Managed Microsoft AD, questo gruppo è costituito da Amministratori AWS delegati FSx . 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 il ACLs, 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 per il controllo completo su tutte le cartelle all'interno del file system. Non modificare le autorizzazioni ACL NTFS 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.
- [Passaggio 1. Configurazione di un Active Directory.](#)

Controllo degli accessi ai file system con Amazon VPC

Puoi accedere al tuo FSx file system Amazon 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) associato al file system. Ti connetti al tuo FSx file system Amazon 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 Direct Connect o VPN o le risorse all'interno del sistema peer VPCs 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 per 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 [Working with Shared VPCs](#) nella Amazon VPC User Guide.

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.

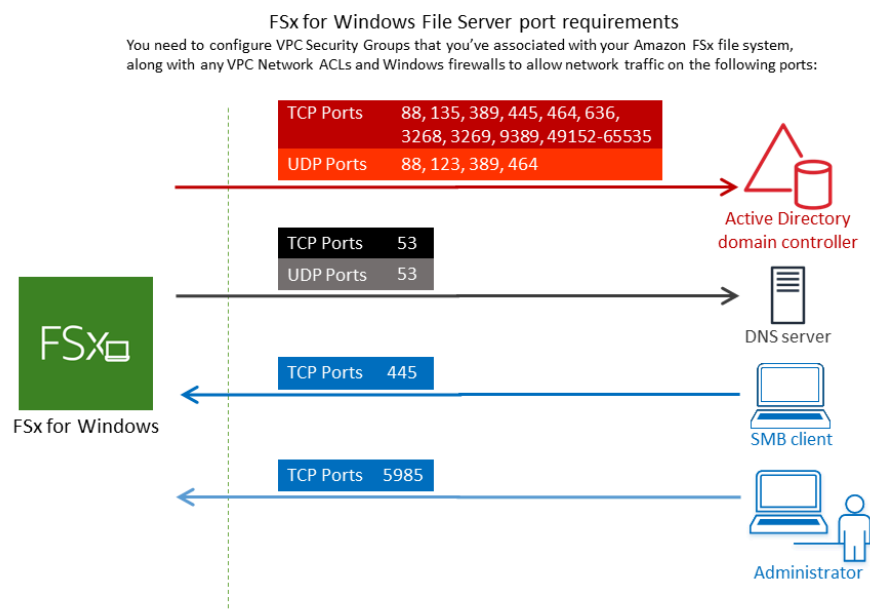
Per utilizzare un gruppo di sicurezza per controllare l'accesso al tuo FSx file system Amazon, aggiungi regole in entrata e in uscita. Le regole in entrata controllano il traffico in entrata e le regole in uscita controllano il traffico in uscita dal tuo file system. Assicurati di avere le regole del traffico di rete corrette nel tuo gruppo di sicurezza per mappare la condivisione di FSx file del tuo file system Amazon su una cartella sull'istanza di calcolo supportata.

Per ulteriori informazioni sulle regole dei gruppi di sicurezza, consulta le [regole del gruppo di sicurezza](#) nella Guida per l'utente di Amazon EC2.

Per creare un gruppo di sicurezza per Amazon FSx

1. [Apri la console Amazon EC2 in https://console.aws.amazon.com/ec2](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 la rete VPC ACLs per le sottoreti in cui stai creando il FSx file system 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)

Protocollo	Porte	Ruolo
TCP	445	Condivisione di file SMB di Servizi directory
TCP	636	Lightweight Directory Access Protocol over 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 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 e amministratori. FSx FSx

⚠ Important

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

ℹ Note

Se hai definito siti Active Directory, devi assicurarti che le sottoreti nel VPC associato al tuo file system FSx Amazon 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.

 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 FSx file system Amazon. Per ulteriori informazioni sulle regole in entrata richieste, consulta [AWS Managed Microsoft AD Prerequisiti nella Guida](#) all'AWS Directory Service amministrazione.

Ora che hai creato il tuo gruppo di sicurezza, puoi associarlo alle interfacce elastiche di rete del tuo FSx file system Amazon.

Per associare un gruppo di sicurezza al tuo FSx file system Amazon

1. Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
2. Nella dashboard, 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 inbound/outbound regole.

Rete Amazon VPC ACLs

Un'altra opzione per proteggere l'accesso al file system all'interno del VPC è la creazione di elenchi di controllo degli accessi alla rete (ACLsrete). Le reti sono separate dai gruppi di sicurezza, ma hanno funzionalità simili per aggiungere un ulteriore livello di sicurezza alle risorse del tuo VPC. Per ulteriori informazioni sulla rete ACLs, consulta [Rete ACLs](#) nella Amazon VPC User Guide.

Registrazione dell'accesso dell'utente finale con il 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.

Note

Il controllo dell'accesso ai file è supportato solo sui FSx file system Windows con una capacità di trasmissione pari o superiore a 32 MBps . È possibile modificare la capacità di trasmissione dei file system esistenti. Per ulteriori informazioni, consulta [Gestione della capacità di throughput](#).

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 (SACLs). Se hai già impostato i controlli di audit sui dati dei tuoi 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, Cambia le autorizzazioni e Diventa proprietario.
- 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.

Puoi configurare se desideri 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 dell'accesso 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](#)
- [Migrazione dei controlli di audit](#)
- [Visualizzazione dei registri degli eventi](#)
- [Impostazione dei controlli di controllo di file e cartelle](#)
- [Gestione del controllo degli accessi ai file](#)

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 tuo file system Amazon FSx for Windows File Server o in qualsiasi momento dopo 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 scegliere per i log degli eventi di controllo:

- 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 Amazon Data Firehose se desideri trasmettere continuamente gli eventi allo storage in Amazon S3, a un database in Amazon Redshift, ad OpenSearch Amazon Service o a soluzioni partner come Splunk o AWS Datadog 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 gruppo di `/aws/fsx/windows` log CloudWatch 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 Account AWS system Amazon FSx .

È possibile modificare la destinazione del registro degli eventi di controllo in qualsiasi momento (ad esempio, da CloudWatch Logs a Firehose). In tal caso, 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 hai già impostato audit controls (SACLs) sui tuoi dati di file esistenti, puoi creare un FSx file system Amazon e migrare i dati nel tuo nuovo file system. Ti consigliamo di AWS DataSync utilizzarlo per trasferire i dati e i dati associati SACLs al tuo FSx file system Amazon. 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. La posizione e il modo in cui vengono visualizzati i log dipendono 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](#).
- SubjectUserNames si riferisce all'utente che effettua l'accesso.
- ObjectNames si riferisce al file, alla cartella o alla condivisione di file di destinazione a cui è stato effettuato l'accesso.
- ShareName è 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.
- IpAddress si 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 è riuscito o meno. Per gli accessi riusciti, il valore è 0x8020000000000000. Per gli accessi non riusciti, il valore è 0x8010000000000000.
- TimeCreated SystemTime si riferisce all'ora in cui l'evento è stato generato nel sistema e visualizzato nel formato <YYYY-MM-MM:SS.S>z. DDThh
- Computer si riferisce al nome DNS del file system Windows Remote Endpoint e può essere utilizzato per identificare il file system. PowerShell
- 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
Elimina	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 write/append i dati di 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;0ICI;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'>\\AMZNFSXCYPDZ\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

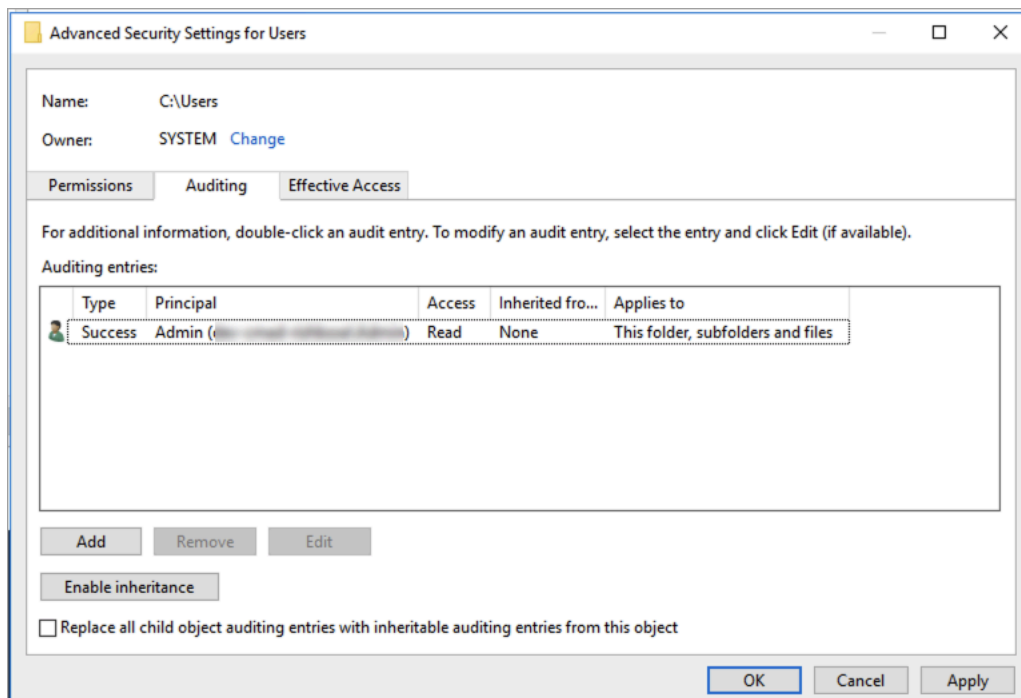
È necessario impostare i controlli di controllo sui file e sulle cartelle che si desidera controllare per i tentativi di accesso degli utenti. I controlli di controllo sono noti anche come elenchi di controllo degli accessi al sistema NTFS (SACLs).

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 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 FSx console Amazon.

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 FSx console Amazon o AWS CLI l'API.

Note

Il controllo dell'accesso ai file è supportato solo sui file system Amazon FSx per Windows File Server con una capacità di throughput pari MBps o superiore a 32. Non è possibile creare o aggiornare un file system con una capacità di throughput inferiore a 32 MBps se il controllo dell'accesso ai file è abilitato. È possibile modificare la capacità di trasmissione in qualsiasi momento dopo aver creato il 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 FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.

2. Segui la procedura per creare un nuovo file system descritta [Fase 5. 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.

▼ **Auditing - optional**

Log access to files and folders [Info](#)
Once you enable logging here, Windows generates audit logs for files and folders on which you have enabled audit controls (also known as System Access Control Lists or SACLs).

Log access to file shares [Info](#)

☐ Log successful attempts
☐ Log failed attempts

☐ Log successful attempts
☐ Log failed attempts

Log access to file shares [Info](#)
☐ Log successful attempts
☐ Log failed attempts

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 and/or falliti riusciti. 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 and/or falliti riusciti. 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 gruppo CloudWatch Logs /aws/fsx/windows 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.

▼ Auditing - optional

Log access to files and folders [Info](#)

Once you enable logging here, Windows generates audit logs for files and folders on which you have enabled audit controls (also known as System Access Control Lists or SACLs).

❗ If you don't already have audit controls configured for your individual files or folders, use the Windows GUI or PowerShell to do so. [See documentation.](#)

☒ Log successful attempts
 ☒ Log failed attempts

Log access to file shares [Info](#)

☒ Log successful attempts
 ☒ Log failed attempts

Choose an audit event log destination

☒ **CloudWatch Logs**
View and search audit logs in the AWS management console and run queries on logs using CloudWatch Logs Insights
 ☐ **Kinesis Data Firehose**
Continuously stream audit events to S3, an Amazon Redshift database, Amazon ElasticSearch, or to partner solutions such as Splunk and Datadog for further analysis

Choose a CloudWatch Logs destination

[Create new](#)

Pricing

Standard Amazon CloudWatch Logs pricing applies based on your usage. [Learn more](#)

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 [CreateFileSystem](#) API per abilitare il controllo dell'accesso ai file per il nuovo file system.

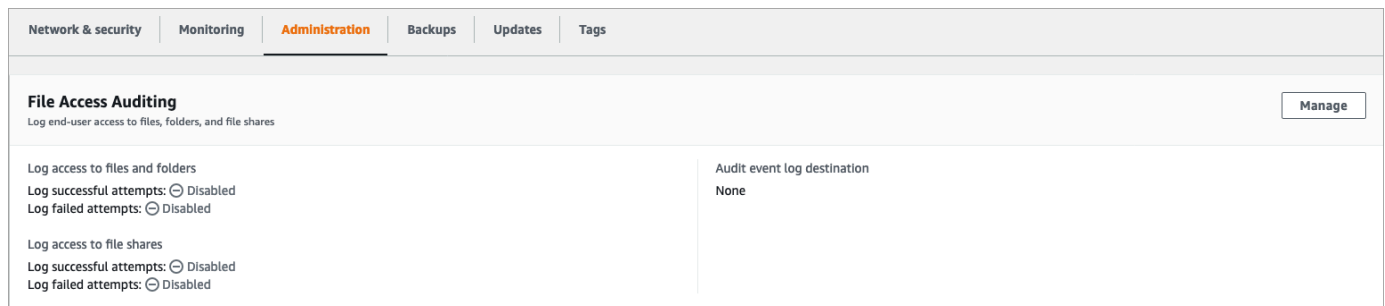
```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
  --windows-configuration
  AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
```

```
AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-customer-log-group"}'
```

- 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)

- Apri la FSx console Amazon all'indirizzo <https://console.aws.amazon.com/fsx/>.
- Passa a File system e scegli il file system Windows per cui desideri gestire il controllo degli accessi ai file.
- Scegli la scheda Amministrazione.
- Nel pannello File Access Auditing, scegli Gestisci.



- Nella finestra di dialogo Gestisci le impostazioni di controllo dell'accesso ai file, modifica le impostazioni desiderate.

Manage file access auditing settings

Log access to files and folders

Amazon FSx can log successful attempts to access files and folders, failed attempts to access files and folders, neither, or both. Once enabled here, audit logs are generated for files and folders on which audit controls (also known as System Access Control Lists or SACLs) have been configured.

☒ Log successful attempts
 ☒ Log failed attempts

Log access to file shares

Amazon FSx can log successful attempts to access file shares, failed attempts to access file shares, neither, or both.

☒ Log successful attempts
 ☒ Log failed attempts

Choose an audit event log destination

Amazon FSx supports access audit logging to one of the following audit destinations. If you change your audit destination, events will no longer be published to any previous audit destinations.

☒ CloudWatch Logs
 View and search audit logs in the AWS management console and run queries on logs using CloudWatch Logs Insights

☐ Kinesis Data Firehose
 Continuously stream audit events to S3, an Amazon Redshift database, Amazon Elasticsearch, or to partner solutions such as Splunk and DataDog for further analysis

Choose a CloudWatch Logs destination

Use a default CloudWatch Logs log stream created by Amazon FSx, an existing log stream, or create a new log stream.

Create new

Pricing

Standard Amazon CloudWatch Logs pricing applies based on your usage. [Learn more](#)

Cancel

Save

- Per Log access a file e cartelle, seleziona la registrazione dei tentativi falliti riusciti. and/or 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 and/or falliti riusciti. 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. Scegli Save (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 \
```

Gestione del controllo degli accessi ai file

412


```
--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"}'
```

Gestione delle identità e degli accessi per Amazon FSx for Windows File Server

AWS Identity and Access Management (IAM) è un software 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) da utilizzare FSx per le risorse di Windows File Server. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso tramite policy](#)
- [Come funziona Amazon FSx per Windows File Server con IAM](#)
- [Esempi di policy basate sull'identità per Amazon FSx for Windows File Server](#)
- [AWS politiche gestite per Amazon FSx for Windows File Server](#)
- [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon FSx for Windows File Server](#)
- [Usare i tag con Amazon FSx](#)
- [Utilizzo di ruoli collegati ai servizi FSx per Windows File Server](#)

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia in base al tuo ruolo:

- Utente del servizio: richiedi le autorizzazioni all'amministratore se non riesci ad accedere alle funzionalità (consulta [Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon FSx for Windows File Server](#))

- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta [Come funziona Amazon FSx per Windows File Server con IAM](#))
- Amministratore IAM: scrivi policy per gestire l'accesso (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 autenticarti come utente IAM o assumendo un ruolo IAM. Utente root dell'account AWS

Puoi accedere come identità federata utilizzando credenziali provenienti da una fonte di identità come AWS IAM Identity Center (IAM Identity Center), autenticazione Single Sign-On o credenziali. Google/Facebook Per ulteriori informazioni sull'accesso, consulta [Come accedere all' Account AWS](#) nella Guida per l'utente di Accedi ad AWS .

Per l'accesso programmatico, AWS fornisce un SDK e una CLI per firmare crittograficamente le richieste. Per ulteriori informazioni, consulta [AWS Signature Version 4 per le richieste API](#) nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un Account AWS, si inizia con un'identità di accesso denominata utente Account AWS root che ha accesso completo a tutte Servizi AWS le risorse. Consigliamo vivamente di non utilizzare l'utente root per le attività quotidiane. Per le attività che richiedono le credenziali dell'utente root, consulta [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente IAM.

Identità federata

Come procedura ottimale, richiedi agli utenti umani di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente della directory aziendale, del provider di identità Web o Directory Service che accede Servizi AWS utilizzando le credenziali di una fonte di identità. Le identità federate assumono ruoli che forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, si consiglia di utilizzare AWS IAM Identity Center. Per ulteriori informazioni, consulta [Che cos'è il Centro identità IAM?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è una identità che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ti consigliamo di utilizzare credenziali temporanee invece di utenti IAM con credenziali a lungo termine. Per ulteriori informazioni, consulta [Richiedere agli utenti umani di utilizzare la federazione con un provider di identità per accedere AWS utilizzando credenziali temporanee](#) nella Guida per l'utente IAM.

Un [gruppo IAM](#) specifica una raccolta di utenti IAM e semplifica la gestione delle autorizzazioni per gestire gruppi di utenti di grandi dimensioni. Per ulteriori informazioni, consulta [Casi d'uso per utenti IAM](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità con autorizzazioni specifiche che fornisce credenziali temporanee. Puoi assumere un ruolo [passando da un ruolo utente a un ruolo IAM \(console\)](#) o chiamando un'operazione AWS CLI o AWS API. Per ulteriori informazioni, consulta [Metodi per assumere un ruolo](#) nella Guida per l'utente di IAM.

I ruoli IAM sono utili per l'accesso degli utenti federati, le autorizzazioni utente IAM temporanee, l'accesso multi-account, l'accesso multi-servizio e le applicazioni in esecuzione su Amazon EC2. Per maggiori informazioni, consultare [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Gestione dell'accesso tramite policy

Puoi controllare l'accesso AWS creando policy e associandole a AWS identità o risorse. Una policy definisce le autorizzazioni quando è associata a un'identità o a una risorsa. AWS valuta queste politiche quando un preside effettua una richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per maggiori informazioni sui documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente IAM.

Utilizzando le policy, gli amministratori specificano chi ha accesso a cosa definendo quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Un amministratore IAM crea le policy IAM e le aggiunge ai ruoli, che gli utenti possono quindi assumere. Le policy IAM definiscono le autorizzazioni indipendentemente dal metodo utilizzato per eseguirle.

Policy basate sull'identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile collegare a un'identità (utente, gruppo o ruolo). Tali policy controllano le operazioni autorizzate per l'identità, nonché le risorse e le condizioni in cui possono essere eseguite. Per informazioni su come creare una policy basata su identità, consultare [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente IAM.

Le policy basate su identità possono essere policy in linea (con embedding direttamente in una singola identità) o policy gestite (policy autonome collegate a più identità). Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scegliere tra policy gestite e policy in linea](#) nella Guida per l'utente di IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi includono le policy di trust dei ruoli IAM e le policy dei bucket di Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#).

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi che possono impostare le autorizzazioni massime concesse dai tipi di policy più comuni:

- Limiti delle autorizzazioni: imposta il numero massimo di autorizzazioni che una policy basata su identità ha la possibilità di concedere a un'entità IAM. Per ulteriori informazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- Politiche di controllo del servizio (SCPs): specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa in AWS Organizations. Per ulteriori informazioni, consultare [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations.
- Politiche di controllo delle risorse (RCPs): imposta le autorizzazioni massime disponibili per le risorse nei tuoi account. Per ulteriori informazioni, consulta [Politiche di controllo delle risorse \(RCPs\)](#) nella Guida per l'AWS Organizations utente.

- Policy di sessione: policy avanzate passate come parametro quando si crea una sessione temporanea per un ruolo o un utente federato. Per maggiori informazioni, consultare [Policy di sessione](#) nella Guida per l'utente IAM.

Più tipi di policy

Quando a una richiesta si applicano più tipi di policy, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire o meno una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella IAM User Guide.

Come funziona Amazon FSx per Windows File Server con IAM

Prima di utilizzare IAM FSx per gestire l'accesso a Windows File Server, scopri quali funzionalità IAM sono disponibili per l'uso FSx per Windows File Server.

Funzionalità IAM che puoi utilizzare con Amazon FSx for Windows File Server

Funzionalità IAM	FSx supporto
Policy basate sull'identità	Sì
Policy basate su risorse	No
Operazioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
ACLs	No
ABAC (tag nelle policy)	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso	Sì
Ruoli di servizio	No

Funzionalità IAM	FSx supporto
Ruoli collegati al servizio	Sì

Per avere una panoramica di alto livello su come FSx e altri AWS servizi funzionano con la maggior parte delle funzionalità IAM, consulta [AWS i servizi che funzionano con IAM nella IAM](#) User Guide.

Politiche basate sull'identità per FSx

Supporta le policy basate sull'identità: sì

Le policy basate sull'identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente](#) nella Guida per l'utente di IAM.

Con le policy basate sull'identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente IAM.

Esempi di politiche basate sull'identità per FSx

Per visualizzare esempi di politiche basate FSx sull'identità di Windows File Server, vedere. [Esempi di policy basate sull'identità per Amazon FSx for Windows File Server](#)

Politiche basate sulle risorse all'interno FSx

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle risorse sono le policy di attendibilità dei ruoli IAM e le policy di bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni che un principale può eseguire su tale risorsa e a quali condizioni. In una policy basata sulle risorse è obbligatorio [specificare un'entità principale](#). I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, è possibile specificare un intero account o entità IAM in un altro account come entità principale in una policy basata sulle risorse. Per ulteriori informazioni, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente IAM.

Azioni politiche per FSx

Supporta le operazioni di policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco di FSx azioni, consulta [Actions defined by Amazon FSx for Windows File Server](#) nel Service Authorization Reference.

Le azioni politiche in FSx uso utilizzano il seguente prefisso prima dell'azione:

```
fsx
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [  
    "fsx:action1",  
    "fsx:action2"  
]
```

Per visualizzare esempi di politiche FSx basate sull'identità di Windows File Server, vedere. [Esempi di policy basate sull'identità per Amazon FSx for Windows File Server](#)

Risorse politiche per FSx

Supporta le risorse relative alle policy: sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'operazione. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Per le azioni che non supportano le autorizzazioni a livello di risorsa, si utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di FSx risorse e relativi ARNs, consulta [Resources defined by Amazon FSx for Windows File Server](#) nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta [Azioni definite da Amazon FSx for Windows File Server](#).

Per visualizzare esempi di politiche FSx basate sull'identità di Windows File Server, consulta. [Esempi di policy basate sull'identità per Amazon FSx for Windows File Server](#)

Chiavi relative alle condizioni delle politiche 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. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Condition` specifica quando le istruzioni vengono eseguite in base a criteri definiti. È possibile compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per visualizzare un elenco di chiavi di FSx condizione, consulta [Condition keys for Amazon FSx for Windows File Server](#) nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta [Azioni definite da Amazon FSx for Windows File Server](#).

Per visualizzare esempi di FSx politiche basate sull'identità di Windows File Server, consulta. [Esempi di policy basate sull'identità per Amazon FSx for Windows File Server](#)

ACLs in FSx

Supporti: No ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con FSx

Supporta ABAC (tag nelle policy): sì

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base ad attributi chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire operazioni quando il tag del principale corrisponde al tag sulla risorsa.

Per controllare l'accesso basato su tag, fornire informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Sì. Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per maggiori informazioni su ABAC, consulta [Definizione delle autorizzazioni con autorizzazione ABAC](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con FSx

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono l'accesso a breve termine alle AWS risorse e vengono create automaticamente quando si utilizza la federazione o si cambia ruolo. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza temporanee in IAM](#) e [Servizi AWS compatibili con IAM](#) nella Guida per l'utente IAM.

Sessioni di accesso diretto per FSx

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale chiamante an Servizio AWS, combinate con la richiesta di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta [Forward access sessions](#).

Ruoli di servizio per 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 [Create a role to delegate permissions to an Servizio AWS](#) nella Guida per l'utente IAM.

Warning

La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere FSx la funzionalità. Modifica i ruoli di servizio solo quando viene FSx fornita una guida 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'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati al servizio, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati FSx ai servizi di Windows File Server, vedere. [Utilizzo di ruoli collegati ai servizi FSx per Windows File Server](#)

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 FSx per creare o modificare le risorse di Windows File Server. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy IAM \(console\)](#) nella Guida per l'utente di IAM.

Per dettagli sulle azioni e sui tipi di risorse definiti da FSx, incluso il formato di ARNs per ogni 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 politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse FSx di Windows File Server nel tuo account. Queste azioni possono comportare costi aggiuntivi per l'Account AWS. Quando si creano o modificano policy basate sull'identità, seguire queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni. AWS Sono disponibili nel tuo Account AWS. Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per maggiori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente di IAM.
- Applicazione delle autorizzazioni con privilegio minimo - Quando si impostano le autorizzazioni con le policy IAM, concedere solo le autorizzazioni richieste per eseguire un'attività. È possibile farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegio minimo. Per maggiori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso - Per limitare l'accesso ad azioni e risorse è possibile aggiungere una condizione alle policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio CloudFormation. Per maggiori informazioni, consultare la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.

- Utilizzo dello strumento di analisi degli accessi IAM per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali - Lo strumento di analisi degli accessi IAM convalida le policy nuove ed esistenti in modo che aderiscano al linguaggio (JSON) della policy IAM e alle best practice di IAM. Lo strumento di analisi degli accessi IAM offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per maggiori informazioni, consultare [Convalida delle policy per il Sistema di analisi degli accessi IAM](#) nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungere le condizioni MFA alle policy. Per maggiori informazioni, consultare [Protezione dell'accesso API con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

Utilizzo della 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 dettagli sulle risorse FSx per Windows File Server presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console per gli utenti che effettuano chiamate solo verso AWS CLI o l' AWS API. Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano ancora utilizzare la FSx console, allega anche la policy FSx AmazonFSxConsoleReadOnlyAccess AWS gestita alle entità. Per maggiori informazioni, consulta [Aggiunta di autorizzazioni a un utente](#) nella Guida per l'utente di 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 collegate alla relativa identità utente. Questa politica include le autorizzazioni per completare questa azione sulla console o utilizzando l'API o a livello di codice. AWS CLI AWS

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "ViewOwnUserInfo",
    "Effect": "Allow",
    "Action": [
      "iam:GetUserPolicy",
      "iam:ListGroupsForUser",
      "iam:ListAttachedUserPolicies",
      "iam:ListUserPolicies",
      "iam:GetUser"
    ],
    "Resource": ["arn:aws:iam::*:user/${aws:username}"]
  },
  {
    "Sid": "NavigateInConsole",
    "Effect": "Allow",
    "Action": [
      "iam:GetGroupPolicy",
      "iam:GetPolicyVersion",
      "iam:GetPolicy",
      "iam:ListAttachedGroupPolicies",
      "iam:ListGroupPolicies",
      "iam:ListPolicyVersions",
      "iam:ListPolicies",
      "iam:ListUsers"
    ],
    "Resource": "*"
  }
]
}

```

AWS politiche gestite per Amazon FSx for Windows File Server

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. Le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Si consiglia

pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i propri casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

Amazon FSx ServiceRolePolicy

Consente FSx ad Amazon di gestire AWS le risorse per tuo conto. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi FSx per Windows File Server](#).

AWS politica gestita: Amazon FSx DeleteServiceLinkedRoleAccess

Non è possibile collegare AmazonFSxDeleteServiceLinkedRoleAccessalle 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 FSx per Windows File Server](#).

Questa politica concede autorizzazioni amministrative che consentono FSx ad Amazon di eliminare il suo Service Linked Role per l'accesso ad Amazon S3, utilizzato solo da Amazon FSx for Lustre.

Dettagli delle autorizzazioni

Questa policy include le autorizzazioni iam per consentire FSx ad Amazon di visualizzare, eliminare e visualizzare lo stato di eliminazione per i FSx Service Linked Roles for Amazon S3 access.

Per visualizzare le autorizzazioni per questa politica, consulta [Amazon FSx DeleteServiceLinkedRoleAccess](#) nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx FullAccess

Puoi collegare Amazon FSx FullAccess alle tue entità IAM. Amazon attribuisce questa politica FSx anche a un ruolo di servizio che consente FSx ad Amazon di eseguire azioni per tuo conto.

Fornisce accesso completo ad Amazon FSx e accesso ai AWS servizi correlati.

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **fsx**— Consente ai mandanti l'accesso completo per eseguire tutte le FSx azioni di Amazon, ad eccezione `BypassSnaplockEnterpriseRetention` di.
- **ds**— Consente ai dirigenti di visualizzare le informazioni sulle Directory Service directory.
- **ec2**
 - Consente ai mandanti di creare tag nelle condizioni specificate.
 - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
- **iam**— Consente ai principi di creare un ruolo collegato al FSx servizio Amazon per conto dell'utente. Ciò è necessario affinché Amazon FSx possa gestire AWS le risorse per conto dell'utente.
- **firehose**— Consente ai mandanti di scrivere record su Amazon Data Firehose. Ciò è necessario FSx per consentire agli utenti di monitorare l'accesso al file system di Windows File Server inviando registri di accesso di controllo a Firehose.
- **logs**— Consente ai responsabili di creare gruppi di log, flussi di log e scrivere eventi nei flussi di log. Ciò è necessario FSx per consentire agli utenti di monitorare l'accesso al file system di Windows File Server inviando i registri di accesso di controllo a Logs. CloudWatch

Per visualizzare le autorizzazioni per questa politica, consulta [Amazon FSx FullAccess](#) nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx ConsoleFullAccess

È possibile allegare la policy `AmazonFSxConsoleFullAccess` alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo ad Amazon FSx e l'accesso ai AWS servizi correlati tramite. Console di gestione AWS

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- **fsx**— Consente ai responsabili di eseguire tutte le azioni nella console di FSx gestione Amazon, ad eccezione `BypassSnaplockEnterpriseRetention` di.

- `cloudwatch`— Consente ai responsabili di visualizzare CloudWatch allarmi e metriche nella console di gestione Amazon FSx .
- `ds`— Consente ai responsabili di elencare le informazioni su una directory. Directory Service
- `ec2`
 - Consente ai mandanti di creare tag sulle tabelle di routing, elencare le interfacce di rete, le tabelle di routing, i gruppi di sicurezza, le sottoreti e il VPC associato a un file system Amazon FSx
 - Consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
 - Consente ai responsabili di visualizzare le interfacce di rete elastiche associate a un FSx file system Amazon.
- `kms`— Consente ai principali di elencare gli alias per le chiavi. AWS Key Management Service
- `s3`— Consente ai responsabili di elencare alcuni o tutti gli oggetti in un bucket Amazon S3 (fino a 1000).
- `secretsmanager`— Consente ai responsabili di elencare i segreti per la selezione delle credenziali degli Gestione dei segreti AWS account del servizio di accesso al dominio.
- `iam`— Concede l'autorizzazione a creare un ruolo collegato al servizio che consente FSx ad Amazon di eseguire azioni per conto dell'utente.

Per visualizzare le autorizzazioni per questa politica, consulta [Amazon FSx ConsoleFullAccess](#) nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx ConsoleReadOnlyAccess

È possibile allegare la policy `AmazonFSxConsoleReadOnlyAccess` alle identità IAM.

Questa politica concede autorizzazioni di sola lettura ad FSx Amazon e ai servizi AWS correlati in modo che gli utenti possano visualizzare le informazioni su questi servizi in. Console di gestione AWS

Dettagli delle autorizzazioni

Questa policy include le seguenti autorizzazioni:

- `fsx`— Consente ai responsabili di visualizzare le informazioni sui FSx file system Amazon, inclusi tutti i tag, nella Console di FSx gestione Amazon.

- **cloudwatch**— Consente ai responsabili di visualizzare CloudWatch allarmi e metriche nella Console di gestione Amazon FSx .
- **ds**— Consente ai responsabili di visualizzare le informazioni su una Directory Service directory nella Console di FSx gestione Amazon.
- **ec2**
 - Consente ai responsabili di visualizzare interfacce di rete, gruppi di sicurezza, sottoreti e il VPC associato a un FSx file system Amazon nella Console di gestione Amazon. FSx
 - Consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
 - Consente ai responsabili di visualizzare le interfacce di rete elastiche associate a un FSx file system Amazon.
- **kms**— Consente ai mandanti di visualizzare gli alias per le AWS Key Management Service chiavi nella Console di FSx gestione Amazon.
- **log**— Consente ai responsabili di descrivere i gruppi di log di Amazon CloudWatch Logs associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano visualizzare la configurazione esistente di controllo dell'accesso ai file per un file system FSx per Windows File Server.
- **secretsmanager**— Consente ai responsabili di elencare i segreti per la selezione delle credenziali degli Gestione dei segreti AWS account del servizio di accesso al dominio.
- **firehose**— Consente ai mandanti di descrivere i flussi di distribuzione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano visualizzare la configurazione esistente di controllo dell'accesso ai file per un file system FSx per Windows File Server.

Per visualizzare le autorizzazioni per questa politica, consulta [Amazon FSx ConsoleReadOnlyAccess](#) nella AWS Managed Policy Reference Guide.

AWS politica gestita: Amazon FSx ReadOnlyAccess

È possibile allegare la policy AmazonFSxReadOnlyAccess alle identità IAM.

- **fsx**— Consente ai responsabili di visualizzare le informazioni sui FSx file system Amazon, inclusi tutti i tag, nella Console di FSx gestione Amazon.
- **ec2**— Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.

Per visualizzare le autorizzazioni per questa politica, consulta [Amazon FSx ReadOnlyAccess](#) nella AWS Managed Policy Reference Guide.

FSx Aggiornamenti Amazon alle politiche AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon FSx da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS sulla pagina Amazon FSx [Cronologia dei documenti](#).

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>secretsmanager:ListSecrets</code> che consente ai responsabili di elencare i segreti Gestione dei segreti AWS per la selezione delle credenziali dell'account del servizio di accesso al dominio.	5 novembre 2025
Amazon FSx ConsoleReadOnlyAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>secretsmanager:ListSecrets</code> che consente ai responsabili di elencare i segreti Gestione dei segreti AWS per la selezione delle credenziali dell'account del servizio di accesso al dominio.	3 novembre 2025
Amazon FSx ServiceRolePolicy : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>ec2:AssignIpv6Addresses</code> che consente ai mandanti di assegnare IPv6 indirizzi alle interfacce di rete dei clienti dotate di un tag.	22 luglio 2025

Modifica	Descrizione	Data
	AmazonFSx.FileSystemId	
Amazon FSx ServiceRolePolicy : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>ec2:UnassignIpv6Addresses</code> che consente ai mandanti di annullare l'assegnazione IPv6 degli indirizzi dalle interfacce di rete dei clienti che dispongono di un tag. AmazonFSx.FileSystemId	22 luglio 2025
Amazon FSx ConsoleFullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>fsx:CreateAndAttachS3AccessPoint</code> che consente ai responsabili di creare un punto di accesso S3 e collegarlo a un FSx volume.	25 giugno 2025
Amazon FSx ConsoleFullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>fsx:DescribeS3AccessPointAttachments</code> che consente ai responsabili di elencare tutti i punti di accesso S3 Account AWS in un colpo solo. Regione AWS	25 giugno 2025

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>fsx:DetachAndDeleteS3AccessPoint</code> che consente ai responsabili di eliminare un punto di accesso S3.	25 giugno 2025
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>fsx>CreateAndAttachS3AccessPoint</code> che consente ai responsabili di creare un punto di accesso S3 e collegarlo a un FSx volume.	25 giugno 2025
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>fsx:DescribeS3AccessPointAttachments</code> che consente ai responsabili di elencare tutti i punti di accesso S3 Account AWS in un colpo solo. Regione AWS	25 giugno 2025
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>fsx:DetachAndDeleteS3AccessPoint</code> che consente ai responsabili di eliminare un punto di accesso S3.	25 giugno 2025

Modifica	Descrizione	Data
Amazon FSx ConsoleReadOnlyAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>ec2:DescribeNetworkInterfaces</code> che consente ai responsabili di visualizzare le interfacce di rete elastiche associate al proprio file system.	25 febbraio 2025
Amazon FSx ConsoleFullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>ec2:DescribeNetworkInterfaces</code> che consente ai responsabili di visualizzare le interfacce di rete elastiche associate al proprio file system.	07 febbraio 2025
Amazon FSx ServiceRolePolicy : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>ec2:GetSecurityGroupsForVpc</code> che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024

Modifica	Descrizione	Data
Amazon FSx ReadOnlyAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>ec2:GetSecurityGroupsForVpc</code> che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx ConsoleReadOnlyAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>ec2:GetSecurityGroupsForVpc</code> che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>ec2:GetSecurityGroupsForVpc</code> che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione, <code>ec2:GetSecurityGroupsForVpc</code> che consente ai responsabili di fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.	9 gennaio 2024
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica dei dati tra regioni e account FSx per i file system OpenZFS.	20 dicembre 2023
Amazon FSx ConsoleFullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica dei dati tra regioni e account FSx per i file system OpenZFS.	20 dicembre 2023
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica su richiesta dei volumi FSx per i file system OpenZFS.	26 novembre 2023

Modifica	Descrizione	Data
Amazon FSx ConsoleFu llAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di eseguire la replica su richiesta dei volumi FSx per i file system OpenZFS.	26 novembre 2023
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare, abilitare e disabilitare il supporto VPC condiviso FSx per i file system ONTAP Multi-AZ.	14 novembre 2023
Amazon FSx ConsoleFu llAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare, abilitare e disabilitare il supporto VPC condiviso FSx per i file system ONTAP Multi-AZ.	14 novembre 2023
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx gestire le configurazioni di rete FSx per i file system OpenZFS Multi-AZ.	9 agosto 2023

Modifica	Descrizione	Data
AWS politica gestita: Amazon FSx ServiceRolePolicy — Aggiornamento a una politica esistente	Amazon ha FSx modificato l'cloudwatch:PutMetricData autorizzazione esistente in modo che Amazon FSx pubblichi le CloudWatch metriche nel namespace. AWS/FSx	24 luglio 2023
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiornato la politica per rimuovere l'fsx:*autorizzazione e aggiungere fsx azioni specifiche.	13 luglio 2023
Amazon FSx ConsoleFullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiornato la politica per rimuovere l'fsx:*autorizzazione e aggiungere fsx azioni specifiche.	13 luglio 2023
Amazon FSx ConsoleReadOnlyAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare metriche di prestazioni migliorate e azioni consigliate FSx per i file system Windows File Server nella console Amazon FSx .	21 settembre 2022

Modifica	Descrizione	Data
Amazon FSx ConsoleFullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire agli utenti di visualizzare metriche di prestazioni migliorate e azioni consigliate FSx per i file system Windows File Server nella console Amazon FSx .	21 settembre 2022
Amazon FSx ReadOnlyAccess — Avviata la politica di tracciamento	Questa politica garantisce l'accesso in sola lettura a tutte le FSx risorse Amazon e a tutti i tag ad esse associati.	4 febbraio 2022
Amazon FSx DeleteServiceLinkedRoleAccess — Avviata la politica di tracciamento	Questa politica concede autorizzazioni amministrative che consentono FSx ad Amazon di eliminare il suo Service Linked Role per l'accesso ad Amazon S3.	7 gennaio 2022
Amazon FSx ServiceRolePolicy : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx gestire le configurazioni di rete per i file system Amazon FSx for NetApp ONTAP.	2 settembre 2021
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare tag sulle tabelle di routing EC2 per chiamate con ambito limitato.	2 settembre 2021

Modifica	Descrizione	Data
Amazon FSx ConsoleFu IlAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx creare file system Amazon FSx for NetApp ONTAP Multi-AZ.	2 settembre 2021
Amazon FSx ConsoleFu IlAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon FSx di creare tag sulle tabelle di routing EC2 per chiamate con ambito limitato.	2 settembre 2021
Amazon FSx ServiceRo lePolicy : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx descrivere e scrivere su CloudWatch Logs i flussi di log. Ciò è necessario per consentir e agli utenti di visualizzare i registri di controllo degli accessi ai file FSx per i file system Windows File Server utilizzando Logs. CloudWatch	08 giugno 2021

Modifica	Descrizione	Data
Amazon FSx ServiceRolePolicy : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ad Amazon di FSx descrivere e scrivere nei flussi di distribuzione di Amazon Data Firehose. Ciò è necessario per consentire agli utenti di visualizzare i log di controllo degli accessi ai file FSx per un file system Windows File Server utilizzando Amazon Data Firehose.	08 giugno 2021
Amazon FSx FullAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere e creare gruppi di log di CloudWatch Logs, log stream e scrivere eventi nei flussi di log. Ciò è necessario affinché i responsabili possano visualizzare i log di controllo degli accessi ai file FSx per i file system di Windows File Server utilizzando Logs. CloudWatch	08 giugno 2021

Modifica	Descrizione	Data
Amazon FSx FullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere e scrivere record su Amazon Data Firehose. Ciò è necessario per consentire agli utenti di visualizzare i log di controllo degli accessi ai file FSx per un file system Windows File Server utilizzando Amazon Data Firehose.	08 giugno 2021
Amazon FSx ConsoleFullAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere i gruppi di log di Amazon CloudWatch Logs associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano scegliere un gruppo di log CloudWatch Logs esistente durante la configurazione del controllo dell'accesso ai file per un FSx file system per Windows File Server.	08 giugno 2021

Modifica	Descrizione	Data
Amazon FSx ConsoleFu llAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere i flussi di distribuzione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario affinché i responsabili possano scegliere un flusso di distribuzione Firehose esistente durante la configurazione del controllo dell'accesso ai file per FSx un file system Windows File Server.	08 giugno 2021
Amazon FSx ConsoleRe adOnlyAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai responsabili di descrivere i gruppi di log di Amazon CloudWatch Logs associati all'account che effettua la richiesta. Ciò è necessario per consentire ai responsabili di visualizzare la configurazione esistente di controllo dell'accesso ai file per un file system FSx per Windows File Server.	08 giugno 2021

Modifica	Descrizione	Data
Amazon FSx Console ReadOnlyAccess : aggiornamento a una politica esistente	Amazon FSx ha aggiunto nuove autorizzazioni per consentire ai mandanti di descrivere i flussi di distribuzione di Amazon Data Firehose associati all'account che effettua la richiesta. Ciò è necessario per consentire ai responsabili di visualizzare la configurazione esistente di controllo dell'accesso ai file per un FSx file system per Windows File Server.	08 giugno 2021
Amazon FSx ha iniziato a tracciare le modifiche	Amazon FSx ha iniziato a tracciare le modifiche alle sue politiche AWS gestite.	08 giugno 2021

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 FSx Windows File Server e IAM.

Argomenti

- [Non sono autorizzato a eseguire un'azione in FSx](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie FSx risorse](#)

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'azione `iam:PassRole`, i tuoi criteri devono essere aggiornati per consentirti di passare un ruolo a FSx for Windows File Server.

Alcuni Servizi AWS consentono di passare 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.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console FSx per eseguire un'azione in Windows File Server. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per trasmettere il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie FSx risorse

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per concedere alle persone l'accesso alle tue risorse.

Per maggiori informazioni, consulta gli argomenti seguenti:

- Per sapere se FSx per Windows File Server supporta queste funzionalità, consulta [Come funziona Amazon FSx per Windows File Server con IAM](#)
- Per scoprire come fornire l'accesso alle risorse di tua proprietà, consulta [Fornire l'accesso a un utente IAM di un altro Account AWS utente di tua proprietà](#) nella IAM User Guide. Account AWS
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta [Fornire l'accesso a soggetti Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(federazione delle identità\)](#) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Accesso a risorse multi-account in IAM](#) nella Guida per l'utente di IAM.

Usare i tag con Amazon FSx

Puoi utilizzare i tag per controllare l'accesso alle FSx risorse Amazon e implementare il controllo degli accessi basato sugli attributi (ABAC). Gli utenti devono avere l'autorizzazione per applicare tag alle FSx risorse Amazon durante la creazione.

Concessione dell'autorizzazione all'applicazione di tag per le risorse durante la creazione

Alcune azioni di creazione di risorse FSx per l'API Windows File Server consentono di specificare i tag quando si crea la risorsa. È possibile 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 di autorizzazioni esplicite a utilizzare l'azione `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 necessita 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 FSx delle risorse Amazon, consulta [Taggare le tue risorse Amazon FSx](#). Per ulteriori informazioni sull'uso dei tag per controllare l'accesso alle FSx risorse, consulta [Utilizzo dei tag per controllare l'accesso alle FSx risorse Amazon](#).

Utilizzo dei tag per controllare l'accesso alle FSx risorse Amazon

Per controllare l'accesso alle FSx risorse e alle azioni di Amazon, puoi utilizzare policy AWS Identity and Access Management (IAM) basate su tag. È possibile fornire il controllo in due modi:

1. Controlla l'accesso alle FSx risorse Amazon 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 FSx delle risorse Amazon 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 [Taggare le tue 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 FSx risorsa Amazon, puoi utilizzare i tag sulla risorsa. Ad esempio, è possibile consentire o negare operazioni API specifiche su una risorsa di gateway di file in base alla coppia chiave-valore del tag sulla risorsa.

Example 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 FSx file system Amazon 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. Department=Finance

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:TagResource",
        "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
      "Condition": {
        "StringEquals": {

```

```

        "aws:RequestTag/Department": "Finance"
      }
    }
  ]
}

```

Example 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

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystemFromBackup",
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystemFromBackup",
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
      "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`.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:DeleteFileSystem"
      ],
      "Resource": "arn:aws:fsx:us-east-1:111122223333:file-system/*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:us-east-1:111122223333:backup/*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Department": "Finance"
        }
      }
    }
  ]
}

```

Utilizzo di ruoli collegati ai servizi FSx per Windows File Server

Amazon FSx for Windows File Server utilizza ruoli [collegati ai servizi AWS Identity and Access Management](#) (IAM). Un ruolo collegato ai servizi è un tipo unico di ruolo IAM collegato direttamente a Windows File FSx Server. I ruoli collegati ai servizi sono predefiniti da FSx for Windows File Server e includono tutte le autorizzazioni richieste dal servizio per chiamare altri servizi per conto dell'utente. AWS

Un ruolo collegato ai servizi semplifica la configurazione FSx di Windows File Server perché non è necessario aggiungere manualmente le autorizzazioni necessarie. FSx per Windows File Server definisce le autorizzazioni dei ruoli collegati ai servizi e, se non diversamente definito, solo FSx per Windows File Server può assumerne i ruoli. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere allegata a nessun'altra entità IAM.

È possibile eliminare un ruolo collegato al servizio solo dopo avere eliminato le risorse correlate. In questo modo si proteggono le risorse FSx per Windows File Server, in quanto non è possibile 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 Windows File Server FSx

FSx per Windows File Server 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 FSx a Windows File Server di completare le seguenti azioni su tutte le risorse applicabili: AWS

Non puoi collegare Amazon FSx ServiceRolePolicy alle tue entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente di gestire AWS le risorse FSx per tuo conto. Per ulteriori informazioni, consulta [Utilizzo di ruoli collegati ai servizi FSx per Windows File Server](#).

Per gli aggiornamenti a questa policy, consulta [Amazon FSx ServiceRolePolicy](#).

Questa politica concede autorizzazioni amministrative che consentono di gestire AWS le risorse FSx per conto dell'utente.

Dettagli delle autorizzazioni

Le autorizzazioni dei FSx ServiceRolePolicy ruoli Amazon sono definite dalla policy FSx ServiceRolePolicy AWS gestita di Amazon. Amazon FSx ServiceRolePolicy dispone delle seguenti autorizzazioni:

Note

Amazon FSx ServiceRolePolicy è utilizzato da tutti i tipi di FSx file system Amazon; alcune delle autorizzazioni elencate potrebbero non essere applicabili FSx a Windows.

- **ds**— Consente di FSx visualizzare, autorizzare e non autorizzare le applicazioni presenti nella directory. Directory Service
- **ec2**— Consente di FSx effettuare le seguenti operazioni:
 - Visualizza, crea e dissocia le interfacce di rete associate a un FSx file system Amazon.
 - Visualizza uno o più indirizzi IP elastici associati a un FSx file system Amazon.
 - Visualizza Amazon VPCs, i gruppi di sicurezza e le sottoreti associati a un FSx file system Amazon.
 - Assegna IPv6 indirizzi alle interfacce di rete dei clienti che dispongono di un tag. `AmazonFSx.FileSystemId`
 - Annulla l'assegnazione IPv6 degli indirizzi dalle interfacce di rete dei clienti che dispongono di un tag. `AmazonFSx.FileSystemId`
 - Fornire una convalida avanzata dei gruppi di sicurezza di tutti i gruppi di sicurezza che possono essere utilizzati con un VPC.
 - Crea un'autorizzazione per un utente AWS autorizzato a eseguire determinate operazioni su un'interfaccia di rete.
- **cloudwatch**— Consente di FSx pubblicare punti dati metrici nello spazio dei CloudWatch nomi AWS FSx /.
- **route53**— Consente FSx di associare un Amazon VPC a una zona ospitata privata.
- **logs**— Consente di FSx descrivere e scrivere nei log i flussi di CloudWatch log. In questo modo gli utenti possono inviare i registri di controllo degli accessi ai file per un file system FSx per Windows File Server a un CloudWatch flusso di log.

- **firehose**— Consente di FSx descrivere e scrivere sui flussi di distribuzione di Amazon Data Firehose. In questo modo gli utenti possono pubblicare i log di controllo degli accessi ai file per un file system FSx per Windows File Server su un flusso di distribuzione di Amazon Data Firehose.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateFileSystem",
      "Effect": "Allow",
      "Action": [
        "ds:AuthorizeApplication",
        "ds:GetAuthorizedApplicationDetails",
        "ds:UnauthorizeApplication",
        "ec2:CreateNetworkInterface",
        "ec2:CreateNetworkInterfacePermission",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeAddresses",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVPCs",
        "ec2:DisassociateAddress",
        "ec2:GetSecurityGroupsForVpc",
        "route53:AssociateVPCWithHostedZone"
      ],
      "Resource": "*"
    },
    {
      "Sid": "PutMetrics",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
```

```

        "StringEquals": {
            "cloudwatch:namespace": "AWS/FSx"
        }
    },
    {
        "Sid": "TagResourceNetworkInterface",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:network-interface/*"
        ],
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction": "CreateNetworkInterface"
            },
            "ForAllValues:StringEquals": {
                "aws:TagKeys": "AmazonFSx.FileSystemId"
            }
        }
    },
    {
        "Sid": "ManageNetworkInterface",
        "Effect": "Allow",
        "Action": [
            "ec2:AssignPrivateIpAddresses",
            "ec2:ModifyNetworkInterfaceAttribute",
            "ec2:UnassignPrivateIpAddresses"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:network-interface/*"
        ],
        "Condition": {
            "Null": {
                "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
            }
        }
    },
    {
        "Sid": "ManageRouteTable",
        "Effect": "Allow",

```

```

        "Action": [
            "ec2:CreateRoute",
            "ec2:ReplaceRoute",
            "ec2>DeleteRoute"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:route-table/*"
        ],
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
            }
        }
    },
    {
        "Sid": "PutCloudWatchLogs",
        "Effect": "Allow",
        "Action": [
            "logs:DescribeLogGroups",
            "logs:DescribeLogStreams",
            "logs:PutLogEvents"
        ],
        "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
    },
    {
        "Sid": "ManageAuditLogs",
        "Effect": "Allow",
        "Action": [
            "firehose:DescribeDeliveryStream",
            "firehose:PutRecord",
            "firehose:PutRecordBatch"
        ],
        "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
    }
]
}

```

Eventuali aggiornamenti a questa politica sono descritti in: [FSx Aggiornamenti Amazon alle politiche AWS gestite](#)

Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio è necessario 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 al servizio FSx per Windows File Server

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando crei un file system nella CLI Console di gestione AWS IAM o nell'API IAM, FSx per Windows File Server 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 al servizio, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando crei un file system, FSx per Windows File Server crea nuovamente il ruolo collegato al servizio per te.

Modifica di un ruolo collegato al servizio per Windows File Server FSx

FSx per Windows File Server non consente di modificare il ruolo collegato al servizio. Dopo avere creato un ruolo collegato al servizio, non sarà possibile modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta la sezione [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Windows File Server 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 FSx per Windows File Server utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Usa la console IAM, la CLI IAM oppure l'API IAM per eliminare il ruolo collegato al servizio . Per ulteriori informazioni, consulta [Eliminazione del ruolo collegato al servizio](#) nella Guida per l'utente di IAM.

Aree supportate FSx per i ruoli collegati al servizio Windows File Server

FSx per Windows File Server supporta l'utilizzo di ruoli collegati al servizio in tutte le aree geografiche 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 Ambito per programma di conformità](#) [Servizi AWS](#) di conformità e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di [AWS conformità Programmi](#) di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta [Scaricamento dei report in AWS Artifact](#) .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. Per ulteriori informazioni sulla responsabilità di conformità durante l'utilizzo Servizi AWS, consulta [AWS la documentazione sulla sicurezza](#).

Amazon FSx per Windows File Server e endpoint VPC di interfaccia

Puoi migliorare il livello di sicurezza del tuo VPC configurando FSx Amazon per utilizzare un endpoint VPC di interfaccia. Gli endpoint VPC di interfaccia sono basati su una tecnologia che consente di [AWS PrivateLink](#) accedere ad FSx APIs Amazon in modo privato senza un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione Direct Connect. Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare con Amazon FSx APIs. Il traffico tra il tuo VPC e Amazon FSx non esce dalla AWS rete.

Ogni endpoint VPC di interfaccia è rappresentato da una o più interfacce di rete elastiche nelle sottoreti. Un'interfaccia di rete fornisce un indirizzo IP privato che funge da punto di ingresso per il traffico verso l' FSx API Amazon. Amazon FSx supporta endpoint VPC configurati con tipi di indirizzi IP IPv4 -only e dual-stack (e). IPv4 IPv6 Per ulteriori informazioni, consulta [Creazione di un endpoint VPC di interfaccia](#) nella Amazon VPC User Guide.

Considerazioni sugli endpoint VPC con FSx interfaccia Amazon

Prima di configurare un endpoint VPC di interfaccia per Amazon FSx, assicurati di esaminare le proprietà [e le limitazioni dell'endpoint VPC dell'interfaccia nella Amazon VPC User Guide](#).

Puoi chiamare qualsiasi operazione dell' FSx API Amazon dal tuo VPC. Ad esempio, puoi creare un file system FSx per Windows File Server chiamando l' CreateFileSystem API dall'interno del tuo VPC. Per l'elenco completo di Amazon FSx APIs, consulta [Actions](#) in the Amazon FSx API Reference.

Considerazioni sul peering VPC

Puoi connetterne altri VPCs al VPC con endpoint VPC di interfaccia utilizzando il peering VPC. Il peering VPC è una connessione di rete tra due VPCs. Puoi stabilire una connessione peering VPC tra i tuoi due VPCs o con un VPC in un altro Account AWS. I VPCs possono essere disponibili anche in due versioni diverse. Regioni AWS

Il traffico tra utenti VPCs peer rimane sulla AWS rete e non attraversa la rete Internet pubblica. Una volta eseguito il peering, risorse come le istanze Amazon Elastic Compute Cloud EC2 (Amazon) in entrambe VPCs possono accedere all' FSx API Amazon tramite endpoint VPC di interfaccia creati in uno dei VPCs.

Creazione di un endpoint VPC di interfaccia per Amazon API FSx

Puoi creare un endpoint VPC per l' FSx API Amazon utilizzando la console Amazon VPC o il (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta [Creazione di un endpoint VPC di interfaccia](#) nella Amazon VPC User Guide.

Per creare un endpoint VPC di interfaccia per Amazon FSx, usa uno dei seguenti:

- **com.amazonaws.*region*.fsx**— Crea un endpoint per le operazioni delle FSx API Amazon.
- **com.amazonaws.*region*.fsx-fips**— Crea un endpoint per l' FSx API Amazon conforme al [Federal Information Processing Standard \(FIPS\)](#) 140-2.

Per utilizzare l'opzione DNS privato, devi impostare `enableDnsSupport` gli attributi `enableDnsHostnames` e del tuo VPC. Per ulteriori informazioni, consulta [Visualizzazione e aggiornamento del supporto DNS per il tuo VPC](#) nella Amazon VPC User Guide.

Ad eccezione Regioni AWS della Cina, se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API ad Amazon FSx con l'endpoint VPC utilizzando il suo nome DNS predefinito per, ad esempio. Regione `AWSfsx.us-east-1.amazonaws.com` Per la Cina (Pechino) e la Cina (Ningxia) Regioni AWS, puoi effettuare richieste API con l'endpoint VPC utilizzando e, rispettivamente. `fsx-api.cn-north-1.amazonaws.com.cn` `fsx-api.cn-northwest-1.amazonaws.com.cn`

Per ulteriori informazioni, consulta [Accesso a un servizio tramite un endpoint VPC di interfaccia](#) nella Amazon VPC User Guide.

Creazione di una policy sugli endpoint VPC per Amazon FSx

Per controllare ulteriormente l'accesso all' FSx API Amazon, puoi opzionalmente allegare una policy AWS Identity and Access Management (IAM) al tuo endpoint VPC. La policy specifica quanto segue:

- Il principale che può eseguire azioni.
- Le azioni che possono essere eseguite.
- Le risorse su cui è possibile eseguire le azioni.

Per ulteriori informazioni, consulta [Controllo degli accessi ai servizi con endpoint VPC](#) nella Guida per l'utente di Amazon VPC.

Utilizzo di altri servizi

Oltre ad Amazon CloudWatch, AWS Identity and Access Management, and AWS CloudTrail AWS DataSync, FSx per Windows File Server si integra anche con quanto segue: Servizi AWS

- Amazon WorkSpaces Applications — WorkSpaces Applications è un servizio di streaming di applicazioni completamente gestito che fornisce agli utenti l'accesso immediato alle loro applicazioni desktop da qualsiasi luogo. WorkSpaces Applications gestisce le AWS risorse necessarie per ospitare ed eseguire le applicazioni, si ridimensiona automaticamente e fornisce l'accesso agli utenti su richiesta. Scopri come creare uno storage persistente per singoli utenti e condividere lo storage tra più utenti sui tuoi file system FSx per Windows File Server utilizzando WorkSpaces Applications. Per ulteriori informazioni, consulta [Utilizzo di Amazon FSx con WorkSpaces le applicazioni Amazon](#).
- Amazon Kendra — Amazon Kendra è un servizio di ricerca intelligente che utilizza l'elaborazione del linguaggio naturale e algoritmi avanzati di apprendimento automatico per restituire risposte specifiche alle domande di ricerca dai tuoi dati. Con Amazon Kendra, puoi creare un'esperienza di ricerca unificata collegando più repository di dati a un indice e inserendo e scansionando documenti. Per ulteriori informazioni sull'utilizzo di Amazon Kendra FSx con per Windows File Server, consulta. [Utilizzo FSx per Windows File Server con Amazon Kendra](#)

Argomenti

- [Utilizzo di Amazon FSx con WorkSpaces le applicazioni Amazon](#)
- [Utilizzo FSx per Windows File Server con Amazon Kendra](#)

Utilizzo di Amazon FSx con WorkSpaces le applicazioni Amazon

Supportando il protocollo Server Message Block (SMB), Amazon FSx for Windows File Server supporta l'accesso al file system da istanze Amazon EC2, VMware Cloud on AWS WorkSpaces, Amazon e Amazon Applications. WorkSpaces Applications è un servizio di streaming di applicazioni completamente gestito. Gestisci centralmente le tue applicazioni desktop su WorkSpaces Applicazioni e le distribuisce in modo sicuro a un browser su qualsiasi computer. Per ulteriori informazioni sulle WorkSpaces applicazioni, consulta la [Amazon WorkSpaces Applications Administration Guide](#). Per istruzioni su come semplificare la gestione delle immagini e delle flotte delle WorkSpaces applicazioni Amazon, consulta il post del AWS blog [Crea automaticamente immagini Windows AppStream 2.0 personalizzate](#).

Le seguenti procedure mostrano come utilizzare Amazon FSx with WorkSpaces Applications per fornire storage persistente personale a ciascun utente e fornire una cartella condivisa in modo che più utenti possano accedere a file comuni.

Fornire spazio di archiviazione personale persistente a ciascun utente

Puoi usare Amazon FSx per fornire a ogni utente della tua organizzazione un'unità di archiviazione unica all'interno WorkSpaces delle sessioni di streaming delle applicazioni. 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 automaticamente conservati tra le sessioni di streaming.

È necessario eseguire tre procedure per completare questa operazione.

Per creare cartelle home per utenti di dominio che utilizzano Amazon FSx

1. Crea un FSx file system Amazon. Per ulteriori informazioni, consulta [Guida introduttiva ad Amazon FSx per Windows File Server](#).
2. Una volta che il file system è disponibile, crea una cartella per ogni utente WorkSpaces Applications del dominio all'interno del tuo FSx file system Amazon. L'esempio seguente utilizza il nome utente di dominio dell'utente come nome della cartella corrispondente. In questo modo è possibile creare il nome UNC della condivisione di file da mappare facilmente utilizzando la variabile %username% di ambiente Windows.
3. Condividi ognuna di queste cartelle come cartella condivisa. Per ulteriori informazioni, consulta [Creazione, aggiornamento e rimozione di condivisioni di file](#).

Per avviare un generatore di immagini Applications aggiunto a un dominio WorkSpaces

1. [Accedi alla console delle applicazioni: /appstream2 WorkSpaces https://console.aws.amazon.com](https://console.aws.amazon.com/appstream2/WorkSpaces)
2. Scegliete Directory Configs dal menu di navigazione e create un oggetto Directory Config. Per ulteriori informazioni, consulta [Using Active Directory with WorkSpaces Applications](#) nella Amazon WorkSpaces Applications Administration Guide.
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 image builder per aggiungere il generatore di immagini al tuo dominio Active Directory.

5. Avvia il generatore di immagini nello stesso VPC del tuo file system FSx Amazon. Assicurati di associare il generatore di immagini alla stessa AWS Managed Microsoft AD directory a cui è unito il tuo FSx file system Amazon. I gruppi di sicurezza VPC che associ al generatore di immagini devono consentire l'accesso al tuo 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 FSx file Amazon alle WorkSpaces applicazioni

1. Nel generatore di immagini, crea uno script batch con il seguente comando e memorizzalo 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 tuo FSx file system Amazon. In questo script utilizzi il nome DNS del tuo FSx file system Amazon o un alias DNS associato al file system, che puoi ottenere dalla visualizzazione dei dettagli del file system nella console Amazon. FSx

Se utilizzi il nome DNS del file system:

```
@echo off
net use S: /delete
net use S: \\file-system-DNS-name\users\%username%
```

Se utilizzi 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 esegui. `gpedit.msc`
3. Da Configurazione utente scegli Impostazioni di Windows e poi Accedi.
4. Passate allo script batch creato nel primo passaggio di questa procedura e selezionatelo.
5. In Configurazione computer, scegliete Modelli amministrativi di Windows, Sistema e quindi Criteri di gruppo.
6. Scegli la politica Configure Logon Script delay. Abilita la policy e riduci il ritardo a 0. 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 un parco di WorkSpaces applicazioni. Assicurati di far parte del parco WorkSpaces Applicazioni anche dello stesso dominio Active Directory utilizzato per Image Builder. Avvia la flotta nello stesso VPC utilizzato dal tuo FSx file system Amazon. I gruppi di sicurezza VPC che associ alla flotta devono fornire l'accesso al tuo FSx file system Amazon.
8. Avvia una sessione di streaming utilizzando SAML SSO. Per connetterti a una flotta unita ad Active Directory, configura la federazione Single Sign-On utilizzando un provider SAML. Per ulteriori informazioni, consulta [Single Sign-on Access to AppStream 2.0 Using SAML 2.0](#) nella Amazon WorkSpaces Applications Administration Guide.
9. La tua condivisione di FSx file Amazon è mappata sulla lettera dell'unità S: all'interno della sessione di streaming.

Fornire una cartella condivisa tra gli utenti

Puoi usare Amazon FSx per fornire una cartella condivisa agli utenti della tua organizzazione. Una cartella condivisa può essere utilizzata per mantenere i file comuni (ad esempio file demo, esempi di codice, manuali di istruzioni, ecc.) necessari a tutti gli utenti.

È necessario eseguire tre procedure per completare questa operazione.

Per creare una cartella condivisa utilizzando Amazon FSx

1. Crea un FSx file system Amazon. Per ulteriori informazioni, consulta [Guida introduttiva ad Amazon FSx per Windows File Server](#).
2. Per impostazione predefinita, ogni FSx file system Amazon include una cartella condivisa a cui puoi accedere utilizzando l'indirizzo `file-system-DNS-name\\share` o `\\fqdn-DNS-alias\share` se utilizzi alias DNS. Puoi utilizzare la condivisione predefinita o creare una cartella condivisa diversa. Per ulteriori informazioni, consulta [Creazione, aggiornamento e rimozione di condivisioni di file](#).

Per avviare un generatore di immagini per WorkSpaces Applicazioni

1. Dalla console WorkSpaces Applicazioni, 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 FSx Amazon. I gruppi di sicurezza VPC che associ al generatore di immagini devono consentire l'accesso al tuo 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 con WorkSpaces Applicazioni

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 visualizzazione dei dettagli del file system nella FSx console Amazon) e le credenziali per accedere alla cartella condivisa.

Se utilizzi il nome DNS del file system:

```
@echo off
net use S: /delete
net use S: \\file-system-DNS-name\share /user:username password
```

Se utilizzi 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 politica di gruppo per eseguire questo script batch a ogni accesso utente. È possibile 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.

Utilizzo FSx per Windows File Server con Amazon Kendra

Amazon Kendra è un servizio di ricerca estremamente preciso e intelligente. FSx i file system per Windows File Server possono essere utilizzati come fonti di dati per Amazon Kendra, consentendoti di indicizzare e cercare in modo intelligente le informazioni contenute nei documenti archiviati nel tuo file system.

- Per ulteriori informazioni su Amazon Kendra, [consulta What is Amazon Kendra nella Amazon Kendra Developer's Guide](#).
- Per ulteriori informazioni su come aggiungere il tuo file system come origine dati Amazon Kendra, [consulta Getting started with an Amazon Data Source \(console\) nella FSx Amazon Kendra Developer's Guide](#).
- Per informazioni generali su Amazon Kendra, consulta il sito Web Amazon [Kendra](#).
- Per una guida dettagliata su come effettuare ricerche nel tuo file system con Amazon Kendra, [consulta Ricerca sicura di dati non strutturati su file system Windows con il connettore Amazon Kendra per Amazon for Windows File Server sul Machine Learning Blog](#). FSx AWS

Prestazioni del file system

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

Assicurati che il tuo file system sia configurato con risorse sufficienti in modo da non influire sulle prestazioni del carico di lavoro. In particolare, se hai intenzione di indicizzare un numero elevato di file, ti consigliamo di utilizzare un file system con tipo di storage SSD, che offre livelli di throughput massimo e IOPS più elevati per le richieste che devono accedere ai volumi di archiviazione. Per ulteriori informazioni sul modello di FSx prestazioni di Amazon, consulta [FSx per le prestazioni di Windows File Server](#).

Quote

Di seguito, puoi scoprire le quote quando lavori con Amazon FSx for Windows File Server.

Argomenti

- [Quote che è possibile incrementare](#)
- [Quote di risorse per ogni file system](#)
- [Ulteriori considerazioni](#)
- [Quote specifiche per Microsoft Windows](#)

Quote che è possibile incrementare

Di seguito sono riportate le quote per Amazon FSx for Windows File Server per ognuna Account AWS di esse che puoi aumentare. Regione AWS

Risorsa	Di default	Description
File system Windows	100	Il numero massimo di file system Amazon FSx for Windows Server che puoi creare in questo account.
Capacità di velocità effettiva di Windows	10240	La quantità totale di capacità di throughput (in MBps) consentita per tutti i file system Amazon FSx for Windows in questo account.
Capacità di archiviazione HDD di Windows	524288	La quantità massima di capacità di archiviazione su disco rigido (in GiB) consentita per tutti i file system FSx Amazon for Windows File Server in questo account.

Risorsa	Di default	Description
Capacità di archiviazione SSD di Windows	524288	La quantità massima di capacità di archiviazione SSD (in GiB) consentita per tutti i file system FSx Amazon 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 for 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. Seleziona 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 delle quote nella](#) Guida per l'utente di 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 di throughput massima	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 FSx file system Amazon.
- 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 con Amazon FSx

Utilizza le seguenti sezioni per aiutarti a risolvere i problemi che hai con Amazon FSx.

Se riscontri problemi non elencati di seguito durante l'utilizzo di Amazon FSx, prova a porre una domanda nel [FSx forum Amazon](#).

Argomenti

- [Non riesci ad accedere al tuo file system](#)
- [La creazione di un nuovo FSx file system Amazon non riesce](#)
- [Il file system è in uno stato configurato in modo errato](#)
- [Non è possibile configurare DFS-R su un file system Multi-AZ o Single-AZ 2](#)
- [Gli aggiornamenti della capacità di storage o di throughput non riescono](#)

Non riesci ad 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

- [L'interfaccia elastic network interface del file system è stata modificata o eliminata](#)
- [L'indirizzo IP elastico collegato all'interfaccia di rete elastica del file system è stato eliminato](#)
- [Il gruppo di sicurezza del file system non dispone delle regole in entrata o in uscita richieste.](#)
- [Il gruppo di sicurezza dell'istanza di calcolo non dispone delle regole in uscita richieste](#)
- [Istanza di calcolo non unita a un Active Directory](#)
- [La condivisione di file non esiste](#)
- [L'utente di Active Directory non dispone delle autorizzazioni necessarie](#)
- [Consenti la rimozione delle autorizzazioni ACL NTFS \(controllo completo\)](#)
- [Impossibile accedere a un file system utilizzando un client locale](#)
- [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 FSx elastica di Amazon. 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 scollega FSx automaticamente qualsiasi indirizzo IP elastico, che è un indirizzo IP pubblico raggiungibile da Internet, che viene collegato all'interfaccia di rete elastica di un file system. Per ulteriori informazioni, consulta [Accesso ai tuoi dati](#).

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 [Usare 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, consulta [Creazione, aggiornamento e rimozione di condivisioni di file](#).

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 degli accessi di Windows (ACLs) 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 [Creazione, aggiornamento e rimozione di condivisioni di file](#). 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 utilizzando il tuo FSx file system Amazon da locale tramite Direct Connect VPN e stai utilizzando un intervallo di indirizzi IP non privato per il client locale.

Amazon supporta FSx solo l'accesso da client locali con indirizzi IP non privati su file system creati dopo il 17 dicembre 2020.

Se devi accedere al tuo file system FSx per Windows File Server creato prima del 17 dicembre 2020 utilizzando un intervallo di indirizzi IP non privato, puoi creare un nuovo file system ripristinando un backup del file system. Per ulteriori informazioni, consulta [Protezione dei dati con backup](#).

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. Devi configurare manualmente le voci DNS A per i tuoi FSx file system Amazon. 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. Nella <https://console.aws.amazon.com/fsx/>, scegli il file system di cui desideri 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 privato primario. IPv4
 - 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 privato secondario. IPv4
 - 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 privato secondario. IPv4

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 FSx console Amazon: 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 [DescribeFileSystemAliases](#) API 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 creati (SPNs) corrispondenti all'alias DNS sull'oggetto computer Active Directory del tuo FSx file system Amazon.

Per ulteriori informazioni, consulta [Configura i nomi principali dei servizi \(SPNs\) 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 [Aggiorna o crea un record DNS CNAME](#).

4. Se hai creato un record DNS CNAME valido SPNs , 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
```

- Se il record DNS CNAME si risolve nel DNS predefinito del FSx file system Amazon e il client non è ancora in grado di accedere al file system, consulta ulteriori [Non riesci ad accedere al tuo file system](#) passaggi per la risoluzione dei problemi.

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 [FSx console Amazon](#) scegliendo Windows File Server, rete e sicurezza. In alternativa, puoi trovarli nella risposta dell'operazione [CreateFileSystem](#) o [DescribeFileSystems](#) dell'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 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 FSx file system Amazon 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

- [Gruppo di sicurezza e rete VPC non configurati correttamente ACLs](#)
- [Nomi di gruppi di amministratori del file system duplicati](#)
- [Server DNS o controller di dominio non raggiungibili](#)
- [Credenziali dell'account di servizio non valide](#)
- [Amazon non FSx può accedere alle credenziali del tuo account del servizio Active Directory in Gestione dei segreti AWS](#)

- [Autorizzazioni insufficienti per l'account di servizio](#)
- [Capacità dell'account di servizio superata](#)
- [Amazon non FSx può accedere all'unità organizzativa \(OU\)](#)
- [L'account di servizio non può accedere al gruppo degli amministratori](#)
- [Amazon FSx ha perso la connettività nel dominio](#)
- [L'account di servizio non dispone delle autorizzazioni corrette](#)
- [Caratteri Unicode utilizzati nei parametri di creazione](#)
- [La commutazione del tipo di archiviazione su HDD durante il ripristino di un backup non riesce](#)

Gruppo di sicurezza e rete VPC non configurati correttamente ACLs

Assicurati che i gruppi di sicurezza e la rete VPC ACLs siano configurati utilizzando la configurazione dei gruppi di sicurezza consigliata. Per ulteriori informazioni, consulta [Creazione di gruppi di sicurezza](#).

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 per Windows File Server unito a un Active Directory autogestito.
3. Crea un nuovo file system usando o. Console di gestione AWS AWS CLI Per ulteriori informazioni, consulta [Unire un FSx file system Amazon 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 FSx file system Amazon e il tuo Active Directory autogestito. Per ulteriori informazioni, consulta [Prerequisiti](#).

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 FSx file system Amazon 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 FSx file system Amazon, insieme a qualsiasi rete VPC ACLs, 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 FSx file system Amazon. 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.

Caso 1: se si utilizza un Gestione dei segreti AWS segreto per archiviare le credenziali di Active Directory

1. Verificare [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#).
2. all'ARN segreto è corretto e segue il formato corretto:
`arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`
3. Verifica che il segreto contenga entrambi i campi obbligatori con valori non vuoti:
 - CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME— Il nome utente dell'account del servizio AD.
 - CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD— La password dell'account del servizio AD.
4. Verifica che il segreto e la chiave abbiano una politica basata sulle risorse che conceda al servizio FSx Amazon l'autorizzazione `fsx.amazonaws.com` principale per recuperare il valore segreto.

Caso 2: se utilizzi credenziali in testo non crittografato per accedere a Active Directory

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 [Account FSx di servizio Amazon](#)

Amazon non FSx può accedere alle credenziali del tuo account del servizio Active Directory in Gestione dei segreti AWS

Le seguenti sezioni descrivono i problemi più comuni e come risolverli.

L'aggiunta di un file system all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
You can't provide both username/password and a domain join service account secret to connect to your Active Directory. Provide only one set of credentials.
```

Per risolvere questo problema

1. Scegliete se desiderate fornire le credenziali archiviate in un segreto di Secrets Manager o in testo semplice.
2. Quando entri in Active Directory, fornisci solo uno di questi parametri e non entrambi.

L'aggiunta di un file system all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
The domain join service account secret ARN format you entered isn't valid. Use the format: arn:partition:secretsmanager:region:account-id:secret:secret-name-6chars
```

Per risolvere questo problema

1. Verificare [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#).

2. Verifica che il formato ARN che stai inserendo sia corretto. Un esempio di formato corretto è `arn:aws:secretsmanager:us-east-1:123456789012:secret:MyDatabaseSecret-Ab3d5f`.

L'aggiunta di un file system all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
Amazon FSx can't access the domain join service account secret [ARN]. Add a resource permission to the secret that grants the FSx service principal (fsx.amazonaws.com) permission to access it.
```

Per risolvere questo problema

1. Verificare [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#).
2. Verifica che il segreto di Secrets Manager che stai fornendo abbia le politiche corrette che consentano FSx ad Amazon di utilizzare il segreto.

L'aggiunta di un file system all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
You don't have permission to access the domain join service account secret [ARN]. A resource permission needs to be added to the secret to grant you access.
```

Per risolvere questo problema

- Il proprietario o l'amministratore del segreto di Secrets Manager deve consentire l'accesso all'account per utilizzare questo segreto. Per ulteriori informazioni, consulta [Politiche basate sull'identità](#).

L'aggiunta di un file system all'Active Directory autogestita non riesce e viene visualizzato il seguente messaggio di errore:

```
The domain join service account secret format or content isn't valid. Make sure the secret includes both CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME and CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD fields with non-empty values.
```

Per risolvere questo problema

1. Verificare [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#).
2. Verifica che il segreto di Secrets Manager che stai fornendo contenga entrambi i campi obbligatori.

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.
```

Utilizzare la procedura seguente per risolvere il problema.

- Assicurati di aver delegato le autorizzazioni richieste all'account di servizio che hai fornito. L'account di servizio deve essere in grado di creare ed eliminare oggetti informatici nell'unità organizzativa del dominio a cui si sta entrando a far parte del file system. L'account di servizio deve inoltre disporre almeno delle autorizzazioni per eseguire le seguenti operazioni:
 - Reimpostare le password
 - Impedisci agli account di leggere e scrivere dati
 - Capacità convalidata di scrittura sull'hostname DNS
 - Capacità convalidata di scrivere sul nome principale del servizio

Per ulteriori informazioni sulla creazione di un account di servizio con le autorizzazioni corrette, consulta. [Account FSx di servizio Amazon](#)

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 [Account FSx di servizio Amazon](#).

Amazon non FSx 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 [Account FSx di servizio Amazon](#)

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=FSx Admins, OU=example, DC=corp, DC=com`.

2. Assicurati che il gruppo di amministratori fornito esista nello stesso dominio Active Directory a cui desideri far parte del 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 riuscita a raggiungere i server DNS e i controller di dominio del tuo dominio Active Directory e aggiungere 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 tuo FSx file system Amazon 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, ACLs 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 autogestito 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 a cui 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 [Account FSx di servizio Amazon](#)

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.

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.

Per risolvere il problema, utilizzare la procedura seguente.

1. Attendi il completamento della richiesta di aumento della capacità di archiviazione e il file system dispone di 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 su un nuovo file system](#).

Il file system è in uno stato configurato in modo errato

Un file system FSx per 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 FSx console Amazon, 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.

Important

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

(Per l'elenco completo dei requisiti di Active Directory, consulta [Prerequisiti](#). 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 FSx console Amazon, dell'API o AWS CLI 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 FSx console Amazon oppure utilizza il `StartMisconfiguredStateRecovery` comando nella FSx console Amazon, nell'API o AWS CLI.

Argomenti

- [File system configurato in modo errato: Amazon non FSx riesce a raggiungere né i server DNS né i controller di dominio del tuo dominio.](#)
- [File system configurato in modo errato: le credenziali dell'account di servizio non sono valide](#)
- [File system configurato in modo errato: la chiave Gestione dei segreti AWS segreta o KMS non è configurata correttamente](#)
- [File system configurato in modo errato: l'account di servizio fornito non dispone dell'autorizzazione per aggiungere il file system al dominio](#)
- [File system configurato in modo errato: l'account del servizio non può aggiungere altri computer al dominio](#)
- [File system configurato in modo errato: l'account del servizio non ha accesso all'unità organizzativa](#)

File system configurato in modo errato: Amazon non FSx riesce a raggiungere né i server DNS né i controller di dominio del tuo dominio.

Un file system entrerà in uno Misconfigured stato in cui Amazon non sarà in FSx 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 un Microsoft Active Directory autogestito](#).
3. Esamina la configurazione di Active Directory autogestita del file system nella FSx console Amazon.
4. Per aggiornare la configurazione di Active Directory autogestita del file system, puoi utilizzare la FSx console Amazon.
 - 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 non è in FSx 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 un 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 FSx console Amazon.
 - 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' FSx API `Amazonupdate-file-system`. Per ulteriori informazioni, [UpdateFileSystem](#) consulta Amazon FSx API Reference.

File system configurato in modo errato: la chiave Gestione dei segreti AWS segreta o KMS non è configurata correttamente

Amazon non è in FSx grado di stabilire una connessione con il controller o i controller di dominio Microsoft Active Directory. Ciò è dovuto al fatto che il tuo Gestione dei segreti AWS account segreto o non AWS KMS key è configurato correttamente. Per ulteriori informazioni, consulta [Memorizzazione delle credenziali di Active Directory utilizzando Gestione dei segreti AWS](#).

Per risolvere l'errore di configurazione, procedi come segue:

1. Verifica che l'ARN segreto sia corretto e segua il formato corretto:
`arn:aws:secretsmanager:region:account-id:secret:secret-name-6chars`
2. Verifica che il segreto contenga entrambi i campi obbligatori con valori non vuoti:
 - `CUSTOMER_MANAGED_ACTIVE_DIRECTORY_USERNAME`— Il nome utente dell'account del servizio AD.

- CUSTOMER_MANAGED_ACTIVE_DIRECTORY_PASSWORD— La password dell'account del servizio AD.
- Verifica che il segreto e la chiave abbiano una politica basata sulle risorse che conceda al servizio FSx Amazon l'autorizzazione `fsx.amazonaws.com` principale per recuperare il valore segreto.

File system configurato in modo errato: l'account di servizio fornito non dispone dell'autorizzazione per aggiungere il file system al dominio

Amazon non è in FSx 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 di FSx servizio Amazon o crea un nuovo account di servizio con le autorizzazioni richieste. Per ulteriori informazioni su questa operazione, consulta [Account FSx di servizio Amazon](#)
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 FSx console Amazon.
 - 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' FSx API `Amazonupdate-file-system`. Per ulteriori informazioni, [UpdateFileSystem](#) consulta Amazon FSx API Reference.

File system configurato in modo errato: l'account del servizio non può aggiungere altri computer al dominio

Amazon non è in FSx 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' FSx API `Amazonupdate-file-system`. Per ulteriori informazioni, [UpdateFileSystem](#) consulta Amazon FSx API Reference.

File system configurato in modo errato: l'account del servizio non ha accesso all'unità organizzativa

Amazon non FSx può 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' FSx API `Amazonupdate-file-system`. Per ulteriori informazioni, [UpdateFileSystem](#) consulta Amazon FSx API Reference.

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 non riescono

Esistono diverse cause potenziali per cui le richieste di aggiornamento della capacità di storage e throughput del file system non riescono, ognuna con una propria risoluzione.

L'aumento della capacità di storage non riesce perché Amazon non FSx può accedere al file system AWS KMS key

Una richiesta di aumento della capacità di storage non è riuscita perché Amazon non FSx è stato in grado di accedere alla chiave KMS utilizzata per crittografare il file system.

Devi assicurarti che Amazon FSx abbia accesso alla chiave KMS utilizzata per crittografare il file system per eseguire l'azione amministrativa. Utilizza le seguenti informazioni per risolvere il problema di accesso alle chiavi.

- Se la chiave KMS è stata eliminata, il file system e tutti i relativi backup che utilizzano la chiave KMS eliminata non sono recuperabili. Per ulteriori informazioni, consulta la sezione [Eliminazione di s nella Guida per gli sviluppatori AWS KMS key](#). AWS Key Management Service
- Se la chiave KMS è disabilitata e si tratta di una chiave gestita dal cliente, sarà necessario riattivarla e quindi ripetere 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 perché è in sospeso l'eliminazione, è necessario [annullare l'eliminazione della chiave](#) mentre è ancora in uno stato. PendingDeletion Puoi riprovare la richiesta una volta ottenuta la chiave KMS. Enabled

- 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. MBps

Aumenta la capacità di trasmissione del file system a un minimo di 16 MBps, quindi riprova la richiesta. Per ulteriori informazioni, consulta [Gestione della capacità di throughput](#).

L'aggiornamento della capacità di throughput a 8 non riesce MBps

Una richiesta di modifica della capacità di throughput di un file system portandola a 8 MBps 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 storage richiede un throughput minimo di 16. MBps Attendi il completamento della richiesta di aumento della capacità di archiviazione, quindi riprova la richiesta di modifica della capacità di throughput.

Cronologia dei documenti

- Versione API: 2018-03-01
- Ultimo aggiornamento della documentazione: 30 settembre 2025

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 Gestione dei segreti AWS l'integrazione	Amazon FSx ora si integra con Gestione dei segreti AWS per una gestione avanzata delle credenziali di Active Directory . Per ulteriori informazioni, consulta Memorizzazione delle credenziali di Active Directory utilizzando . Gestione dei segreti AWS	5 novembre 2025
Amazon FSx ConsoleFu llAccess: aggiornamento a una politica esistente	Amazon FSx ha aggiunto una nuova autorizzazione che consente ai responsabili di elencare i segreti Gestione dei segreti AWS per la selezione delle credenziali dell'account del servizio di accesso al dominio. secretsmanager:ListSecrets Per ulteriori informazioni, consulta la policy AWS gestita: Amazon FSx FullAccess .	5 novembre 2025
Support aggiunto per Internet Protocol versione 6 (IPv6)	FSx per i file system Windows File Server ora supportano due opzioni di tipo di rete:	30 settembre 2025

IPv4 -only e dual-stack (per entrambe e). IPv4 IPv6 È necessario specificare una di queste opzioni durante la creazione del file system. È possibile modificare il tipo di rete di un file system esistente FSx per Windows File Server in qualsiasi momento. Per ulteriori informazioni, vedere [Gestione del tipo di rete](#).

[Amazon FSx ha aggiornato la politica FSx ServiceRolePolicy AWS gestita da Amazon](#)

Amazon FSx ha aggiunto le `ec2:UnassignIpv6Addresses` autorizzazioni `ec2:AssignIpv6Addresses` e ad Amazon FSxServiceRolePolicy. Per ulteriori informazioni, consulta [Amazon FSx ServiceRolePolicy](#).

22 luglio 2025

[Amazon FSx ha aggiornato la politica FSx FullAccess AWS gestita da Amazon](#)

La policy FSx FullAccess gestita da [Amazon](#) è stata aggiornata per aggiungere le `fsx:DetachAndDeleteS3AccessPoint` autorizzazioni `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments` , e.

25 giugno 2025

[Amazon FSx ha aggiornato la politica FSx ConsoleFullAccess AWS gestita da Amazon](#)

La policy FSx ConsoleFullAccess gestita da [Amazon](#) è stata aggiornata per aggiungere le `fsx:DetachAndDeleteS3AccessPoint` autorizzazioni `fsx:CreateAndAttachS3AccessPoint` `fsx:DescribeS3AccessPointAttachments`, e.

25 giugno 2025

[Amazon FSx ha aggiornato la politica FSx ConsoleReadOnlyAccess AWS gestita da Amazon](#)

Amazon FSx ha aggiornato la FSx ConsoleReadOnlyAccess politica di Amazon per aggiungere l'`ec2:DescribeNetworkInterfaces` autorizzazione. Per ulteriori informazioni, consulta la FSx ConsoleReadOnlyAccess politica di [Amazon](#).

25 febbraio 2025

[Support aggiunto per gli endpoint di interfaccia VPC dual-stack per Amazon FSx](#)

Ora puoi creare endpoint di interfaccia VPC dual-stack per FSx Amazon con indirizzi IP IPv4 IPv6 e nomi DNS. Per ulteriori informazioni, consulta [FSx Windows File Server e gli endpoint VPC di interfaccia](#).

7 febbraio 2025

[Support aggiunto per endpoint API dual-stack](#)

L'API del FSx servizio Amazon per la creazione e la gestione dei file system dispone di nuovi endpoint dual-stack. Per ulteriori informazioni, consulta gli [endpoint delle API](#) nell'Amazon FSx API Reference.

7 febbraio 2025

[Amazon FSx ha aggiornato la politica FSx ConsoleFullAccess AWS gestita da Amazon](#)

Amazon FSx ha aggiornato la FSx ConsoleFullAccess politica di Amazon per aggiungere l'ec2:DescribeNetworkInterfaces autorizzazione. Per ulteriori informazioni, consulta la FSx ConsoleFullAccess policy di [Amazon](#).

7 febbraio 2025

[Versione aggiornata dello strumento di convalida di Active Directory FSx per Windows File Server](#)

È disponibile una versione aggiornata dello strumento di convalida di Active Directory FSx per Windows File Server. Per ulteriori informazioni, vedere [Convalida della configurazione di Active Directory](#)

6 novembre 2024

[Support aggiunto per livelli più elevati di IOPS su file system con capacità di throughput pari o superiori a 4 GBps](#)

FSx per Windows File Server sta aumentando gli IOPS massimi da 130.000 a 150.000 per file system con 4 o più GBps di capacità di throughput, da 175.000 a 200K per file system con 6 GBps di capacità di throughput o superiore, da 260K a 300K per file system con 9 o più GBps di capacità di throughput e da 350K a 400K per file system con 12 GBps di capacità di throughput o superiore. Per [ulteriori](#) informazioni, vedere per le prestazioni di Windows File Server. FSx

17 gennaio 2024

[Amazon FSx ha aggiornato le politiche FSx ServiceRolePolicy AWS gestite di Amazon FSx FullAccess FSx ConsoleFullAccess FSx ReadOnlyAccess FSxConsoleReadOnlyAccess, Amazon, Amazon e Amazon](#)

Amazon FSx ha aggiornato le FSx ServiceRolePolicy politiche di Amazon FSx FullAccess FSx ConsoleFullAccess FSxReadOnlyAccess, Amazon FSxConsoleReadOnlyAccess, Amazon e Amazon per aggiungere l'ec2:GetSecurityGroupsForVpc autorizzazione. Per ulteriori informazioni, consulta [Amazon FSx updates to AWS managed policy](#).

9 gennaio 2024

[Amazon FSx ha aggiornato Amazon FSx FullAccess e le politiche FSx ConsoleFullAccess AWS gestite da Amazon](#)

Amazon FSx ha aggiornato le FSx ConsoleFullAccess politiche di Amazon FSx FullAccess e Amazon per aggiungere l'ManageCrossAccountDataReplication azione. Per ulteriori informazioni, consulta [Amazon FSx updates to AWS managed policy](#).

20 dicembre 2023

[Amazon FSx ha aggiornato Amazon FSx FullAccess e le politiche FSx ConsoleFullAccess AWS gestite da Amazon](#)

Amazon FSx ha aggiornato le FSx ConsoleFullAccess politiche di Amazon FSx FullAccess e Amazon per aggiungere l'fsx:CopySnapshotAndUpdateVolume autorizzazione. Per ulteriori informazioni, consulta [Amazon FSx updates to AWS managed policy](#).

26 novembre 2023

[Amazon FSx ha aggiornato Amazon FSx FullAccess e le politiche FSx ConsoleFullAccess AWS gestite da Amazon](#)

Amazon FSx ha aggiornato le FSx ConsoleFullAccess politiche di Amazon FSx FullAccess e Amazon per aggiungere le fsx:UpdateSharedVPCConfiguration autorizzazioni fsx:DescribeSharedVPCConfiguration e. Per ulteriori informazioni, consulta [Amazon FSx updates to AWS managed policy](#).

14 novembre 2023

[Support aggiunto per l'aggiornamento del tipo di storage del file system](#)

FSx per i file system Windows File Server ora supportano l'aggiornamento dal tipo di archiviazione HDD al tipo di archiviazione SSD. Per ulteriori informazioni, vedere [Gestione del tipo di archiviazione](#).

9 agosto 2023

[Support aggiunto per una maggiore capacità di throughput massima](#)

FSx per i file system Windows File Server ora supportano fino a 12 GBps velocità di trasmissione. Per ulteriori informazioni, vedere [FSx per le prestazioni di Windows File Server](#).

9 agosto 2023

[Support aggiunto per il provisioning di IOPS SSD](#)

FSx per i file system 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 politica FSx ServiceRolePolicy AWS gestita da Amazon](#)

Amazon FSx ha aggiornato l'cloudwatch:PutMetricData autorizzazione in Amazon FSxServiceRolePolicy. Per ulteriori informazioni, consulta [Amazon FSx ServiceRolePolicy.](#)

24 luglio 2023

[Amazon FSx ha aggiornato la politica FSx FullAccess AWS gestita da Amazon](#)

Amazon FSx ha aggiornato la FSx FullAccess politica di Amazon per rimuovere l'fsx:*autorizzazione e aggiungere fsx azioni specifiche. Per ulteriori informazioni, consulta la FSx FullAccess policy di [Amazon.](#)

13 luglio 2023

[Amazon FSx ha aggiornato la politica FSx ConsoleFullAccess AWS gestita da Amazon](#)

Amazon FSx ha aggiornato la FSx ConsoleFullAccess politica di Amazon per rimuovere l'fsx:*autorizzazione e aggiungere fsx azioni specifiche. Per ulteriori informazioni, consulta la FSx ConsoleFullAccess policy di [Amazon.](#)

13 luglio 2023

[Support aggiunto per nuove CloudWatch metriche per Amazon FSx for Windows File Server](#)

FSx per Windows File Server ora fornisce CloudWatch metriche aggiuntive che monitorano 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 parametri si avvicina o supera soglie predeterminate per tali CloudWatch metriche. 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 FSx console Amazon FSx per i file system 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' FSx API Amazon dal tuo VPC senza inviare traffico su Internet. Per ulteriori informazioni, consulta [Amazon FSx e interfaccia gli endpoint VPC.](#)

5 aprile 2022

[Supporto aggiunto per Amazon Kendra](#)

Ora puoi utilizzare il tuo file system FSx per Windows File Server come fonte di dati per Amazon Kendra, consentendo di indicizzare e cercare informazioni contenute nei documenti archiviati nel tuo file system. Per ulteriori informazioni, consulta [Utilizzo FSx per 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 condivisioni 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](#).

08 giugno 2021

[Support aggiunto per la copia dei backup](#)

Ora puoi usare Amazon FSx per copiare i backup all'interno dello stesso AWS account su un'altra Regione AWS (copie interregionali) o all'interno della stessa Regione AWS (copie all'interno della stessa regione). [Per ulteriori informazioni, consulta Copiare i backup](#).

12 Aprile 2021

[Aumenta automaticamente la capacità di archiviazione di un file system](#)

Utilizza un CloudFormation modello personalizzabile AWS sviluppato per aumentare automaticamente la capacità di archiviazione del file system quando la capacità raggiunge una soglia specifica. Per ulteriori informazioni, 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 FSx ai file system di Windows File Server con client locali utilizzando indirizzi IP non privati. Per ulteriori informazioni, vedere Ambienti [supportati](#). È possibile aggiungere il FSx file system 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 [Usare 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 FSx file system 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 utilizzarlo FSx per 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 FSx file system oltre a utilizzare i FSx backup nativi di Amazon. Per ulteriori informazioni, consulta [Utilizzo AWS Backup con Amazon FSx](#).

9 novembre 2020

[Support aggiunto per la scalabilità della capacità di throughput](#)

È ora possibile modificar e la capacità di throughput esistente FSx per i file system Windows File Server 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 dei file system esistenti FSx per Windows File Server man mano che i requisiti di storage evolvono. Per ulteriori informazioni, vedere [Gestione della capacità di archiviazione](#).

1 giugno 2020

[Support aggiunto per l'archiviazione su disco rigido \(HDD\)](#)

Lo storage su disco rigido offre flessibilità in termini di prezzi e prestazioni quando viene utilizzato FSx per Windows File Server. Per ulteriori informazioni, consulta [Optimizing Costs with Amazon FSx](#).

26 marzo 2020

[Support aggiunto per il trasferimento di file tramite AWS DataSync](#)

È ora possibile AWS DataSync 4 febbraio 2020
utilizzarlo per trasferire file da e verso il file server FSx per Windows. Per ulteriori informazioni, consulta [Migrare i file su Amazon FSx for Windows File Server Using AWS DataSync.](#)

[FSx for Windows File Server rilascia il supporto per ulteriori attività di amministrazione del file system di 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'Amazon FSx CLI per la gestione remota su PowerShell. [Per ulteriori informazioni, consulta Amministrazione dei file system.](#) 20 novembre 2019

[FSx per Windows File Server rilascia il supporto Multi-AZ nativo](#)

È possibile utilizzare l'implementazione Multi-AZ FSx for Windows File Server per creare più facilmente file system ad alta disponibilità che si estendono su più zone di disponibilità (AZs). Per ulteriori informazioni, consulta l'argomento relativo a [disponibilità e durabilità: file system Single-AZ e Multi-AZ.](#) 20 novembre 2019

[FSx per 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 Windows File Server. FSx 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](#)

Ora puoi configurare le copie shadow di Windows sui tuoi file system FSx per 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 FSx i file system di Windows File Server a AWS Managed Microsoft AD directory che si trovano in un VPC diverso o in un file system Account AWS diverso dal file system. Per ulteriori informazioni, consulta [Active Directory Support](#).

25 giugno 2019

[Amazon FSx rilascia il supporto avanzato per Microsoft Active Directory](#)

Ora puoi aggiungere FSx i file system di 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 stata valutata come conforme alla certificazione SOC. Per ulteriori informazioni, consulta [Sicurezza e protezione dei dati](#).

16 maggio 2019

[Aggiunta una nota chiarificatrice riguardante Direct Connect il supporto per connessioni peering VPN e VPC interregionali](#)

I FSx file system Amazon creati dopo il 22 febbraio 2019 sono accessibili tramite Direct Connect VPN e peering VPC interregionale. [Per ulteriori informazioni, consulta Metodi di accesso supportati](#).

25 febbraio 2019

[Direct Connect, Aggiunto il supporto per connessioni peering VPN e VPC interregionali](#)

Ora puoi accedere ai file system Amazon FSx for Windows File Server da risorse locali e da risorse in un altro Amazon Account AWS VPC o. 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 e trasferire e facilmente le applicazioni aziendali AWS.

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.