Guida per l'utente di Amazon FSx File Gateway

AWS Storage Gateway

Versione API 2021-03-31

AWS Storage Gateway: Guida per l'utente di Amazon FSx File Gateway

Table of Contents

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.

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.

Cos'è Amazon FSx File Gateway

Amazon FSx File Gateway (FSx File Gateway) è un nuovo tipo di File Gateway che offre una bassa latenza e un accesso efficiente al cloud FSx per le condivisioni di file Windows File Server dalla tua struttura locale. Se gestisci lo storage di file in locale a causa dei requisiti di latenza o larghezza di banda, puoi invece utilizzare FSx File Gateway per accedere senza problemi a condivisioni di file Windows completamente gestite, altamente affidabili e praticamente illimitate fornite nel Cloud da for Windows File Server. AWS FSx

Vantaggi dell'utilizzo di Amazon FSx File Gateway

FSx File Gateway offre i seguenti vantaggi:

- Aiuta a eliminare i file server locali e consolida tutti i relativi dati AWS per sfruttare la scalabilità e l'economia dello storage nel cloud.
- Fornisce opzioni che puoi utilizzare per tutti i carichi di lavoro relativi ai file, compresi quelli che richiedono l'accesso locale ai dati cloud.
- Le applicazioni che devono rimanere on-premise possono ora usufruire della stessa bassa latenza e delle stesse prestazioni elevate che avevano in precedenza AWS, senza gravare sulle reti o influire sulle latenze riscontrate dalle applicazioni più esigenti.

Come funziona Amazon FSx File Gateway

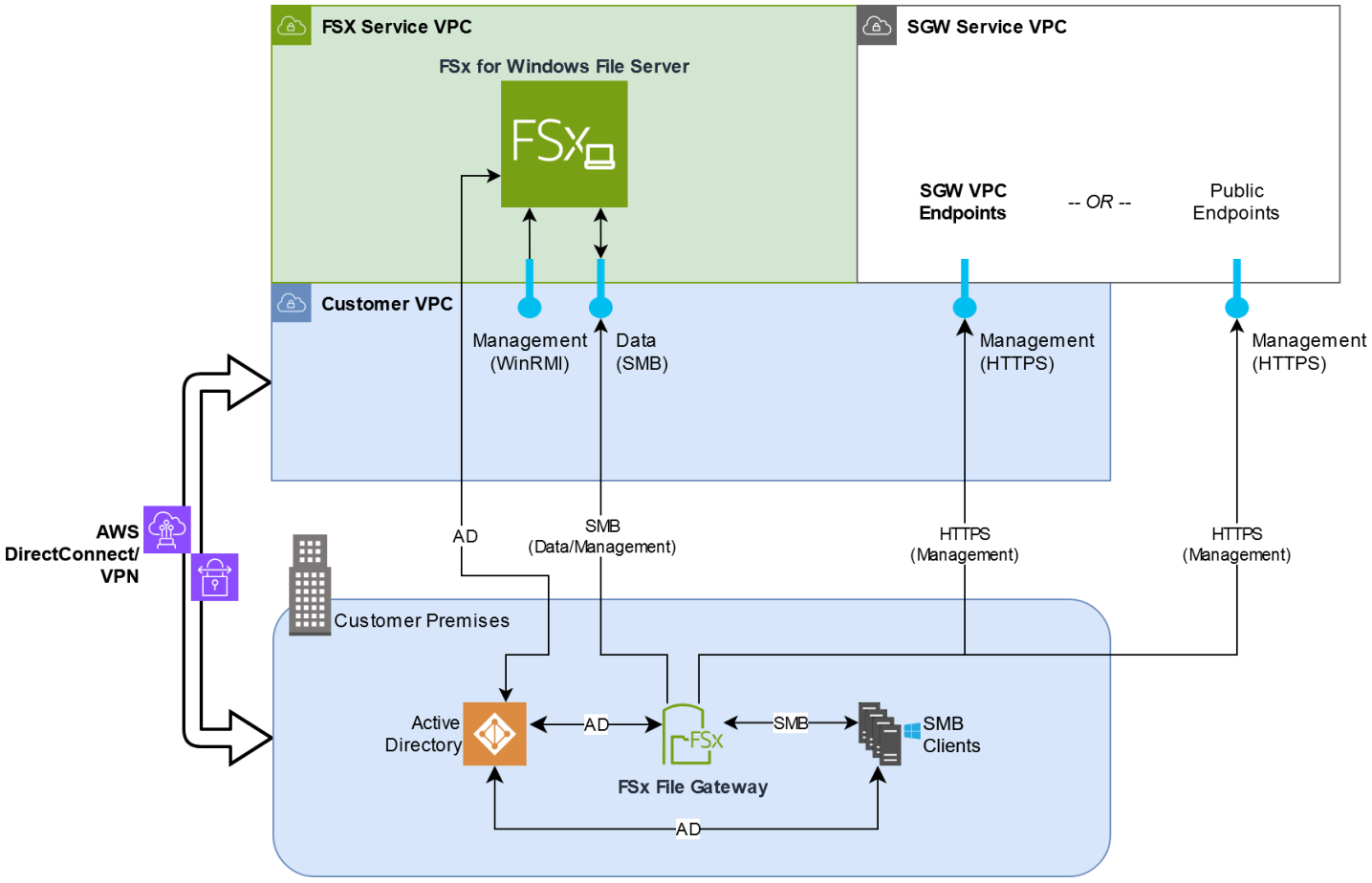
Per utilizzare Amazon FSx File Gateway (FSx File Gateway), devi disporre di almeno un file system Amazon FSx for Windows File Server. È inoltre necessario disporre dell'accesso locale FSx a Windows File Server, tramite una VPN o tramite una Direct Connect connessione. Per ulteriori informazioni sull'uso dei FSx file system Amazon, consulta What is Amazon FSx for Windows File Server?

Puoi implementare il gateway nel tuo ambiente locale come macchina virtuale (VM) in esecuzione su VMware ESXi Microsoft Hyper-V o macchina virtuale basata su Linux Kernel (KVM) o come appliance hardware ordinata dal tuo rivenditore preferito. Puoi anche implementare la macchina virtuale Storage Gateway nel VMware cloud o come AMI in Amazon. AWS EC2 Dopo aver distribuito l'appliance, è possibile attivare il FSx File Gateway dalla console Storage Gateway o tramite l'API Storage Gateway.

Dopo che Amazon FSx File Gateway è stato attivato e può accedere FSx per Windows File Server, usa la console Storage Gateway per aggiungerlo al tuo dominio Microsoft Active Directory. Dopo che il gateway ha aggiunto correttamente un dominio, si utilizza la console Storage Gateway per collegare il gateway a un file server esistente FSx per Windows. FSx per Windows File Server rende tutte le condivisioni sul server disponibili come condivisioni sul tuo Amazon FSx File Gateway. Puoi quindi utilizzare un client per sfogliare e connetterti alle condivisioni di file su FSx File Gateway che corrispondono al FSx File Gateway selezionato.

Quando le condivisioni di file sono connesse, è possibile leggere e scrivere i file localmente, sfruttando al contempo tutte le funzionalità disponibili su FSx Windows File Server. FSx File Gateway mappa le condivisioni di file locali e il relativo contenuto su condivisioni di file archiviate in remoto in FSx Windows File Server. Esiste una corrispondenza 1:1 tra i file remoti e visibili localmente e le relative condivisioni.

Il diagramma seguente fornisce una panoramica dell'implementazione dello storage di file per Storage Gateway.



Notate quanto segue nel diagramma:

- Direct Connect oppure è necessaria una VPN per consentire a FSx File Gateway di accedere alla condivisione di FSx file Amazon tramite SMB e FSx per consentire a Windows File Server di unirsi al dominio Active Directory locale.
- Amazon Virtual Private Cloud (Amazon VPC) è necessario per connettersi al servizio VPC FSx per Windows File Server e al servizio Storage Gateway VPC utilizzando endpoint privati. Il FSx File Gateway può anche connettersi agli endpoint pubblici.

Puoi utilizzare Amazon FSx File Gateway in tutte le AWS regioni in cui è disponibile FSx per Windows File Server.

Guida introduttiva con Gateway di archiviazione AWS

Questa sezione fornisce istruzioni per iniziare. AWSÈ necessario disporre di un AWS account prima di poter iniziare a utilizzare Gateway di archiviazione AWS. Puoi utilizzare un AWS account esistente o registrarne uno nuovo. È inoltre necessario che nel proprio AWS account sia presente un utente IAM che appartenga a un gruppo con le autorizzazioni amministrative necessarie per eseguire le attività di Storage Gateway. Gli utenti con i privilegi appropriati possono accedere alla console Storage Gateway e all'API Storage Gateway per eseguire attività di implementazione, configurazione e manutenzione del gateway. Se sei un utente alle prime armi, ti consigliamo di consultare le sezioni AWS Regioni supportate e Requisiti di configurazione del File Gateway prima di iniziare a utilizzare Storage Gateway.

Questa sezione contiene i seguenti argomenti, che forniscono informazioni aggiuntive su come iniziare a Gateway di archiviazione AWS:

Argomenti

- Registrazione ad Amazon Web Services- Scopri come registrarti AWS e creare un AWS account.
- Crea un utente IAM con privilegi di amministratore- Scopri come creare un utente IAM con privilegi amministrativi per il tuo AWS account.
- Accedere Gateway di archiviazione AWS- Scopri come accedere Gateway di archiviazione AWS tramite la console Storage Gateway o utilizzando programmaticamente il. AWS SDKs
- Regioni AWS che supportano Storage Gateway- Scopri quali AWS regioni puoi utilizzare per archiviare i tuoi dati quando attivi il gateway in Storage Gateway.

Registrazione ad Amazon Web Services

An Account AWS è un requisito fondamentale per accedere ai AWS servizi. Your Account AWS è il contenitore di base per tutte le AWS risorse che crei come AWS utente. Il tuo Account AWS è anche il limite di sicurezza di base per AWS le tue risorse. Tutte le risorse che crei nel tuo account sono disponibili per gli utenti che dispongono delle credenziali per l'account. Prima di poter iniziare a utilizzare Gateway di archiviazione AWS, devi registrarti per un Account AWS.

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

Per iscriverti a un Account AWS

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

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

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

Ti consigliamo inoltre di richiedere agli utenti di utilizzare credenziali temporanee per l'accesso AWS. Per fornire credenziali temporanee, puoi utilizzare la federazione e un provider di identità, come AWS IAM Identity Center. Se la tua azienda utilizza già un provider di identità, puoi utilizzarlo con la federazione per semplificare il modo in cui fornisci l'accesso alle risorse del tuo AWS account.

Crea un utente IAM con privilegi di amministratore

Dopo aver creato l' AWS account, segui i passaggi seguenti per creare un utente AWS Identity and Access Management (IAM) personale, quindi aggiungi quell'utente a un gruppo con autorizzazioni amministrative. Per ulteriori informazioni sull'utilizzo del AWS Identity and Access Management servizio per controllare l'accesso alle risorse di Storage Gateway, vedereGestione delle identità e degli accessi per AWS Storage Gateway.

Per creare un utente amministratore, scegli una delle seguenti opzioni.

Scelta di un modo per gestire il tuo amministratore	Per	Come	Puoi anche
In IAM Identity Center (Consigliato)	Usa credenziali a breve termine per accedere a AWS. Ciò è in linea con le best practice per la sicurezza. Per informazioni sulle best practice, consulta Best practice per la sicurezza in IAM nella Guida per l'utente di IAM.	Segui le istruzioni riportate in Nozioni di base nella Guida per l'utente di AWS IAM Identity Center .	Configurare l'accesso programmatico configurando l'uso AWS IAM Identity Center nella Guida AWS CLI per l'AWS Command Line Interface utente.
In IAM (Non consigliato)	Usa credenziali a lungo termine per accedere a AWS.	Segui le istruzioni in Creare un utente IAM per l'accesso di emergenza nella Guida per l'utente di IAM.	Configura l'accesso programmatico seguendo quanto riportato in Gestione delle chiavi di accesso per gli utenti IAM nella Guida per l'utente di IAM.

Warning

Gli utenti IAM dispongono di credenziali a lungo termine che presentano un rischio per la sicurezza. Per ridurre questo rischio, si consiglia di fornire a questi utenti solo le autorizzazioni necessarie per eseguire l'attività e di rimuoverli quando non sono più necessari.

Accedere Gateway di archiviazione AWS

È possibile utilizzare la Gateway di archiviazione AWS console per eseguire diverse attività di configurazione e manutenzione del gateway, tra cui l'attivazione o la rimozione dei dispositivi hardware Storage Gateway dalla distribuzione, la creazione, la gestione e l'eliminazione dei diversi tipi di gateway, la , la gestione e l' di file system separati da e il monitoraggio dello stato di vari elementi del servizio Storage Gateway. Per semplicità e facilità d'uso, questa guida si concentra sull'esecuzione di attività utilizzando l'interfaccia Web della console Storage Gateway. È possibile accedere alla console Storage Gateway tramite il browser Web all'indirizzo:https://console.aws.amazon.com/storagegateway/home/.

Se si preferisce un approccio programmatico, è possibile utilizzare l'API (Gateway di archiviazione AWS Application Programming Interface) o l'interfaccia a riga di comando (CLI) per configurare e gestire le risorse nell'implementazione di Storage Gateway. Per ulteriori informazioni sulle azioni, i tipi di dati e la sintassi richiesta per l'API Storage Gateway, consulta lo Storage Gateway API Reference. Per ulteriori informazioni sulla CLI di Storage Gateway, vedere il CLI Command Reference AWS .

È inoltre possibile utilizzarlo AWS SDKs per sviluppare applicazioni che interagiscono con Storage Gateway. AWS SDKs Per Java, .NET e PHP racchiudono l'API Storage Gateway sottostante per semplificare le attività di programmazione. Per informazioni sul download delle librerie SDK, consulta il AWS Developer Center.

Per informazioni sui prezzi, consultare Prezzi di Gateway di archiviazione AWS.

Regioni AWS che supportano Storage Gateway

An Regione AWS è una posizione fisica nel mondo in cui sono AWS presenti più zone di disponibilità. Le zone di disponibilità sono costituite da uno o più data AWS center discreti, ciascuno con alimentazione, rete e connettività ridondanti, ospitati in strutture separate. Ciò significa che ciascuna Regione AWS è fisicamente isolata e indipendente dalle altre regioni. Le regioni forniscono la tolleranza ai guasti, la stabilità e la resilienza e possono anche ridurre la latenza. Le risorse create in una regione non esistono in nessun'altra regione a meno che non si utilizzi esplicitamente una funzionalità di replica offerta da un AWS servizio. Ad esempio, Amazon S3 e Amazon EC2 supportano la replica tra regioni. Alcuni servizi, ad esempio AWS Identity and Access Management, non dispongono di risorse regionali. Puoi lanciare AWS risorse in sedi che soddisfano i tuoi requisiti aziendali. Ad esempio, potresti voler lanciare istanze Amazon EC2 per ospitare i tuoi Gateway di archiviazione AWS dispositivi Regione AWS in Europa, per essere più vicino agli utenti europei o per

soddisfare i requisiti legali. Sei tu a Account AWS determinare quali delle regioni supportate da un servizio specifico sono disponibili per l'uso.

Amazon FSx File Gateway archivia i dati dei file AWS nella regione in cui si trova FSx il file system Amazon. Prima di iniziare a implementare il gateway, scegli una regione nell'angolo superiore destro della console Storage Gateway.

- Amazon FSx File Gateway: per AWS le regioni supportate e un elenco di endpoint di AWS servizio che puoi utilizzare con Amazon FSx File Gateway, consulta gli endpoint e le quote di Amazon FSx File Gateway nel. Riferimenti generali di AWS
- Storage Gateway: per AWS le regioni supportate e un elenco degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere Gateway di archiviazione AWS endpoint e quote nel. Riferimenti generali di AWS
- Storage Gateway Hardware Appliance: per le regioni supportate che è possibile utilizzare con l'appliance hardware, vedere Gateway di archiviazione AWS Hardware Appliance Regions nel. Riferimenti generali di AWS

Requisiti di configurazione di File Gate

Salvo diversa indicazione, i seguenti requisiti sono comuni a tutti i tipi di File Gateway in Gateway di archiviazione AWS. La configurazione deve soddisfare i requisiti indicati in questa sezione. Esamina i requisiti applicabili alla configurazione del gateway prima di implementarlo.

Argomenti

Prerequisiti

Prima di configurare Amazon FSx File Gateway (FSx File Gateway) , devi soddisfare i seguenti prerequisiti:

- Crea e configura un file system FSx per Windows File Server. Per istruzioni, consulta la Fase 1: Crea il tuo file system nella Guida FSx per l'utente di Amazon for Windows File Server.
- Configurare Microsoft Active Directory (AD) e creare un account del servizio Active Directory con le autorizzazioni necessarie. Per ulteriori informazioni, vedere Requisiti di account del servizio Active Directory.
- Verificare che vi sia una larghezza di banda di rete sufficiente tra il gateway e AWS. È necessario un minimo di 100 Mbps per scaricare, attivare e aggiornare correttamente il gateway.
- Configura la connessione che desideri utilizzare per il traffico di rete tra AWS e l'ambiente locale in cui stai implementando il gateway. Puoi connetterti utilizzando la rete Internet pubblica, una rete privata, una VPN o. Direct Connect Se desideri che il tuo gateway comunichi AWS tramite una connessione privata a un Amazon Virtual Private Cloud, configura Amazon VPC prima di configurare il gateway.
- Assicurati che il gateway sia in grado di risolvere il nome del tuo controller di dominio Active Directory. È possibile utilizzare DHCP nel dominio Active Directory per gestire la risoluzione o

specificare manualmente un server DNS dal menu delle impostazioni di configurazione di rete nella console locale del gateway.

Requisiti storage e hardware

Le seguenti sezioni forniscono informazioni sulle configurazioni hardware e di storage minime richieste per il gateway e sulla quantità minima di spazio su disco da allocare per lo storage richiesto.

Requisiti hardware per ambienti locali VMs

Quando distribuisci il gateway in locale, assicurati che l'hardware sottostante su cui distribuisci la macchina virtuale (VM) gateway possa dedicare le seguenti risorse minime:

- Quattro processori virtuali assegnati alla macchina virtuale
- 16 GiB di RAM riservata per i gateway di file
- 80 GiB di spazio su disco per l'installazione di immagini VM e dati di sistema

Requisiti per i tipi di istanze Amazon EC2

Quando distribuisci il gateway su Amazon Elastic Compute Cloud (Amazon EC2), la dimensione dell'istanza deve essere **`xlarge`**almeno per il funzionamento del gateway. Tuttavia, per la famiglia di istanze ottimizzate per il calcolo, la dimensione deve essere almeno. **`2xlarge`**

> **Note**
>
> L'AMI Storage Gateway è compatibile solo con le istanze basate su x86 che utilizzano processori Intel o AMD. Le istanze basate su ARM che utilizzano processori Graviton non sono supportate.

Utilizza uno dei seguenti tipi di istanza consigliati per il tuo tipo di gateway.

Consigliato per i tipi di File Gateway

- Famiglia di istanze per uso generico: tipo di istanza m5, m6 o m7. Scegli la dimensione dell'istanza xlarge o superiore per soddisfare i requisiti del processore e della RAM dello Storage Gateway.

- Famiglia di istanze ottimizzate per l'elaborazione: tipi di istanze c5, c6 o c7. Scegli la dimensione dell'istanza 2xlarge o superiore per soddisfare i requisiti del processore Storage Gateway e della RAM.
- Famiglia di istanze ottimizzate per la memoria: tipi di istanze r5, r6 o r7. Scegli la dimensione dell'istanza xlarge o superiore per soddisfare i requisiti del processore e della RAM dello Storage Gateway.
- Famiglia di istanze ottimizzate per lo storage: tipi di istanze i3, i4 o i7. Scegli la dimensione dell'istanza xlarge o superiore per soddisfare i requisiti del processore e della RAM dello Storage Gateway.

> **Note**
>
> Quando avvii il gateway in Amazon EC2 e il tipo di istanza scelto supporta lo storage temporaneo, i dischi vengono elencati automaticamente. Per ulteriori informazioni sullo storage di istanze Amazon EC2, consulta Instance Storage nella Amazon EC2 User Guide.

Requisiti di storage

Oltre a 80 GiB di spazio su disco per la macchina virtuale, sono necessari anche dischi aggiuntivi per il gateway.

Tipo di gateway	Cache (minimo)	Cache (massima)			
Gateway file	150 GiB	64 TiB			

> **Note**
>
> È possibile configurare una o più unità locali per la cache, fino alla capacità massima. Quando si aggiunge la cache a un gateway esistente, è importante creare nuovi dischi nell'host (hypervisor o istanza Amazon EC2). Non modificare le dimensioni dei dischi esistenti se i dischi sono stati precedentemente allocati come cache.

Requisiti di rete e firewall

Il gateway richiede accesso a internet, reti locali, server DNS (Domain Name Service), firewall, router ecc.

I requisiti di larghezza di banda della rete variano in base alla quantità di dati caricati e scaricati dal gateway. È necessario un minimo di 100 Mbps per scaricare, attivare e aggiornare correttamente il gateway. I modelli di trasferimento dei dati determineranno la larghezza di banda necessaria per supportare il carico di lavoro.

Di seguito, puoi trovare ulteriori informazioni sulle porte e sulle modalità per consentire l'accesso tramite firewall e router.

> **Note**
>
> In alcuni casi, potresti implementare il gateway su Amazon EC2 o utilizzare altri tipi di distribuzione (inclusa quella locale) con politiche di sicurezza di rete che AWS limitano gli intervalli di indirizzi IP. In questi casi, il gateway potrebbe riscontrare problemi di connettività del servizio quando i valori dell'intervallo AWS IP cambiano. I valori dell'intervallo di indirizzi AWS IP che devi utilizzare si trovano nel sottoinsieme di servizi Amazon per la AWS regione in cui attivi il gateway. Per i valori correnti dell'intervallo IP, consulta Intervalli di indirizzi IP AWS nella Riferimenti generali di AWS.

Argomenti

Requisiti porta

FSx File Gateway richiede l'autorizzazione di porte specifiche attraverso la sicurezza di rete per una distribuzione e un funzionamento corretti. Alcune porte sono necessarie per tutti i gateway, mentre altre sono necessarie solo per configurazioni specifiche, ad esempio per la connessione agli endpoint VPC.

Per FSx File Gateway, è necessario utilizzare Microsoft Active Directory per consentire agli utenti del dominio di accedere a una condivisione di file Server Message Block (SMB). Puoi aggiungere il tuo File Gateway a qualsiasi dominio Microsoft Windows valido (risolvibile tramite DNS).

Puoi anche Directory Service utilizzarlo per crearne uno AWS Managed Microsoft ADin Amazon Web Services Cloud. Per la maggior parte delle AWS Managed Microsoft AD implementazioni, è necessario configurare il servizio DHCP (Dynamic Host Configuration Protocol) per il VPC. Per informazioni sulla creazione di un set di opzioni DHCP, vedere Create a DHCP options set nella Administration Guide.AWS Directory Service

La tabella seguente elenca le porte necessarie e descrive i requisiti condizionali nella colonna Note.

Requisiti di porta per FSx File Gateway

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Browser	Browser	Macchina virtuale Storage Gateway	TCP/ HTTP	80	✓	✓	✓	Utilizzato dai sistemi locali per ottenere la chiave di attivazione dello Storage Gateway. La porta 80 viene usata solo durante l'attivaz

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
								ione di un'appliance Storage Gateway. Per una macchina virtuale Storage Gateway la porta 80 non deve essere accessibile pubblicamente. Il livello di accesso richiesto alla porta 80 dipende dalla configurazione di rete. Se si attiva il gateway dalla Storage Gateway

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
								Management Console, l'host da cui ci si connette alla console deve avere accesso alla porta 80 del gateway.
Browser	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	443	✓	✓	✓	AWS Console di gestione (tutte le altre operazioni)

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
DNS	Macchina virtuale Storage Gateway	Server DNS (Domain Name Service)	DNS TCP E UDP	53	✓	✓	✓	Utilizzato per la comunicazione tra una macchina virtuale Storage Gateway e il server DNS per la risoluzione dei nomi IP.

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
NTP	Macchina virtuale Storage Gateway	Server NTP (Network Time Protocol)	TCP E UDP NTP	123	✓	✓	✓	Utilizzato dai sistemi locali per sincronizzare l'ora della macchina virtuale con l'ora dell'host. Una macchina virtuale Storage Gateway è configurata in modo che possa utilizzare i seguenti server NTP: • 0.amazon.pool.ntp.org

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
								• 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org **Note** Non richiesto per i gateway ospitati su Amazon EC2.

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Storage Gateway	Macchina virtuale Storage Gateway	Supporto Endpoint	TCP/SSH	22	✓	✓	✓	Consente di accedere Supporto al gateway per aiutarti a risolvere i problemi relativi al gateway. Non è necessario che la porta sia aperta per il normale funzionamento del gateway, tuttavia è necessario per la risoluzione dei problemi.

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
								Per un elenco degli endpoint di supporto, consulta Supporto endpoints.
Storage Gateway	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	443	✓	✓	✓	Controllo della gestione
Amazon CloudFront	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	443	✓	✓	✓	Per l'attivazione
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	443	✓	✓	✓*	Controllo della gestione *Richiesto solo quando si utilizzano gli endpoint VPC

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	1026		✓	✓*	Endpoint del Control Plane *Richiesto solo quando si utilizzano gli endpoint VPC
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	1027		✓	✓*	Anon Control Plane (per l'attivazione) *Richiesto solo quando si utilizzano gli endpoint VPC

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	1028		✓	✓*	Endpoint proxy *Richiesto solo quando si utilizzano gli endpoint VPC
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	1031		✓	✓*	Piano dei dati *Richiesto solo quando si utilizzano gli endpoint VPC

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	2222		✓	✓*	Canale di supporto SSH per VPCe *Necessario solo per l'apertura del canale di supporto quando si utilizzano gli endpoint VPC
VPC	Macchina virtuale Storage Gateway	AWS	TCP/ HTTPS	443	✓	✓	✓*	Controllo della gestione *Richiesto solo quando si utilizzano gli endpoint VPC

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Client della condivisione file	Client SMB	Macchina virtuale Storage Gateway	TCP o UDP SMBv3	445	✓	✓	✓	Servizio di sessione di trasferimento dati per la condivisione di file. Sostituisce le porte 137-139 per Microsoft Windows NT e versioni successive.
Microsoft Active Directory	Macchina virtuale Storage Gateway	Server Active Directory	UDP per NetBIOS	137	✓	✓	✓	Servizio di denominazione
Microsoft Active Directory	Macchina virtuale Storage Gateway	Server Active Directory	UDP per NetBIOS	138	✓	✓	✓	Servizio datagramma

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
Microsoft Active Directory	Macchina virtuale Storage Gateway	Server Active Directory	TCP E UDP LDAP	389	✓	✓	✓	Connessione client Directory System Agent (DSA)
Microsoft Active Directory	Macchina virtuale Storage Gateway	Server Active Directory	Kerberos TCP e UDP	88	✓	✓	✓	Kerberos
Microsoft Active Directory	Macchina virtuale Storage Gateway	Server Active Directory	TCP Distributed Computing Environment/End Point Mapper (DCE/EMAP)	135	✓	✓	✓	RPC

Elemento di rete	Da	Per	Protocollo	Porta	In entrata	In uscita	Richiesto	Note
FSx Connessione Amazon	Macchina virtuale Storage Gateway	FSx per Windows File Server	TCP o UDP SMBv3	445	✓	✓	✓	Servizio di sessione di trasferimento dati per la condivisione di file

Requisiti di rete e di firewall per l'appliance hardware Storage Gateway

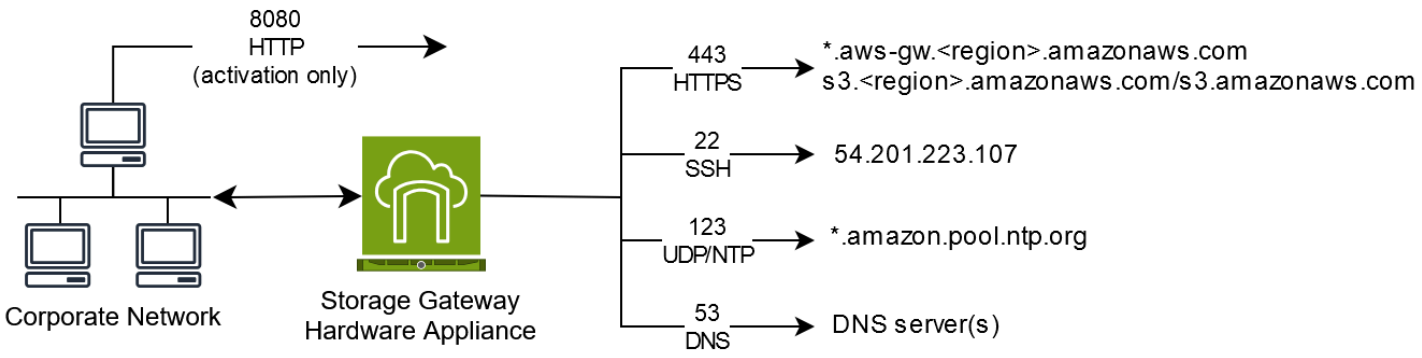
Ogni appliance hardware Storage Gateway richiede i seguenti servizi di rete:

- Accesso a Internet: una connessione di rete a Internet sempre attiva tramite un'interfaccia di rete sul server.
- Servizi DNS: servizi DNS per la comunicazione tra l'appliance hardware e il server DNS.
- Tempo di sincronizzazione: un servizio orario Amazon NTP configurato automaticamente deve essere sempre raggiungibile.
- Indirizzo IP: un indirizzo DHCP o statico IPv4 assegnato. Non è possibile assegnare un IPv6 indirizzo.

Sul retro del server Dell PowerEdge R640 sono presenti cinque porte di rete fisiche. Da sinistra a destra (guardando la parte posteriore del server) queste porte sono le seguenti:

1. iDRAC
2. `em1`
3. `em2`
4. `em3`
5. `em4`

È possibile utilizzare la porta iDRAC per la gestione remota del server.



Un'appliance hardware richiede le seguenti porte per il funzionamento.

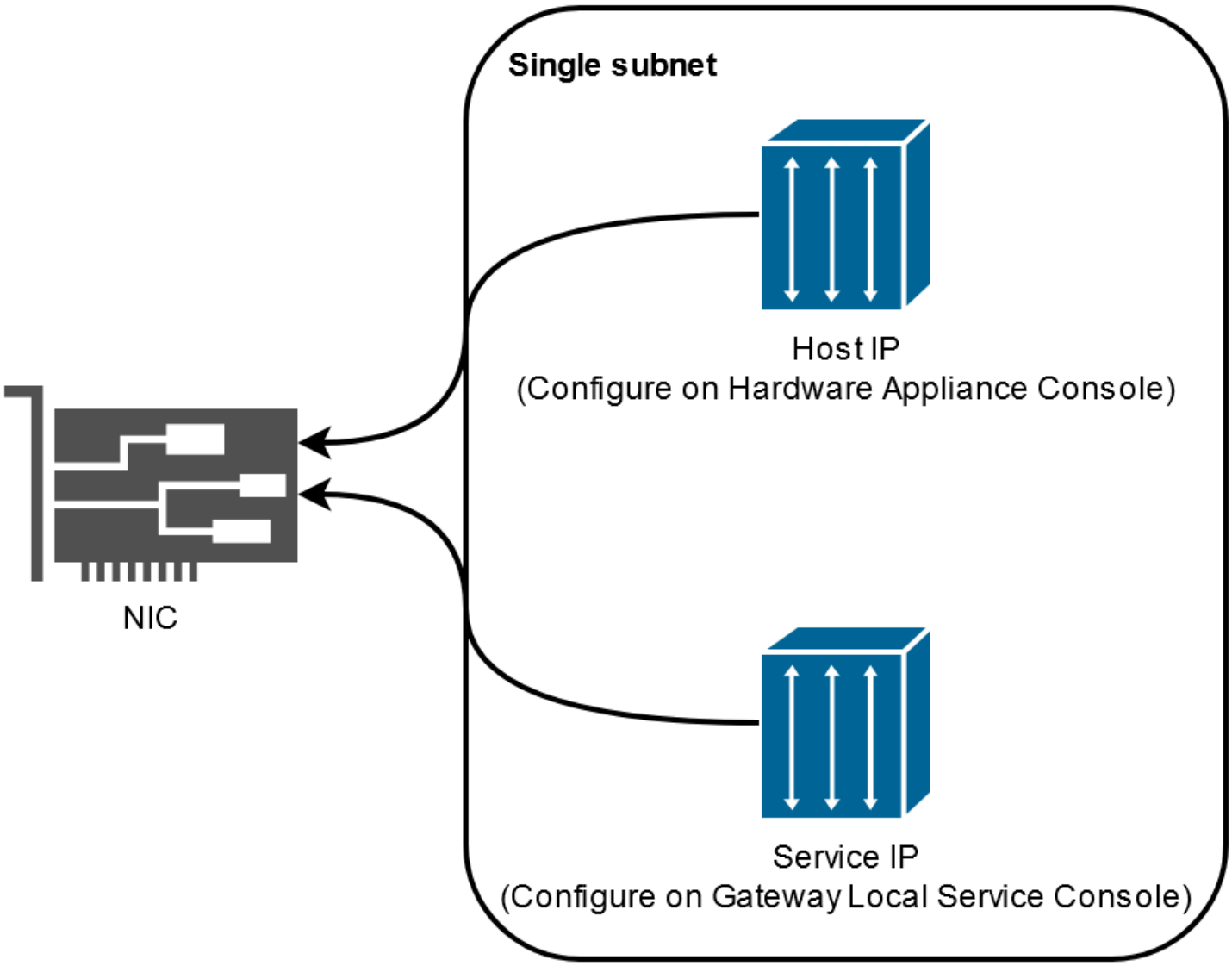
Protocollo	Porta	Direzione	Origine	Destinazione	Utilizzo
SSH	22	In uscita	Appliance hardware	`54.201.223.107`	Canale di supporto
DNS	53	In uscita	Appliance hardware	Server DNS	Risoluzione dei nomi
UDP/NTP	123	In uscita	Appliance hardware	`*.amazon.pool.ntp.org`	Sincronizzazione oraria
HTTPS	443	In uscita	Appliance hardware	`*.amazonaws.com`	Trasferimento dei dati
HTTP	8080	In entrata	AWS	Appliance hardware	Attivazione (solo brevemente)

Per funzionare in modo corretto, un'appliance hardware richiede le seguenti impostazioni di rete e firewall:

- Configurare tutte le interfacce di rete connesse nella console hardware.
- Assicurarsi che ogni interfaccia di rete si trovi in una sottorete univoca.
- Fornire a tutte le interfacce di rete connesse l'accesso in uscita agli endpoint elencati nel diagramma precedente.
- Configurare almeno un'interfaccia di rete per supportare l'appliance hardware. Per ulteriori informazioni, consulta Configurazione dei parametri di rete dell'apparecchiatura hardware.

> **Note**
>
> Per un'illustrazione che mostra la parte posteriore del server con le relative porte, vedere. Installazione fisica del dispositivo hardware

Tutti gli indirizzi IP sulla stessa interfaccia di rete (NIC), sia per un gateway che per un host, devono trovarsi nella stessa sottorete. La figura seguente illustra lo schema di assegnazione di indirizzi.



Per ulteriori informazioni sull'attivazione e la configurazione di un dispositivo hardware, vedere. [Utilizzo dell'appliance hardware AWS Storage Gateway]

Consentire Gateway di archiviazione AWS l'accesso tramite firewall e router

Il gateway richiede l'accesso ai seguenti endpoint del servizio Storage Gateway con AWS cui comunicare. Durante la configurazione del gateway, seleziona il tipo di endpoint per il gateway in base all'ambiente di rete. Se si utilizza un firewall o un router per filtrare o limitare il traffico di rete, è necessario configurare il firewall e/o il router affinché consentano questi endpoint di servizio per le comunicazioni in uscita ad AWS.

> **Note**
>
> Se si configurano endpoint VPC privati per lo Storage Gateway da utilizzare per la connessione e il trasferimento di dati da e verso AWS, il gateway non richiede l'accesso alla rete Internet pubblica. Per ulteriori informazioni, consulta Attivazione di un gateway in un cloud privato virtuale.

> **Important**
>
> Sostituisci *region* i seguenti esempi di endpoint con la Regione AWS stringa corretta per il tuo gateway, ad esempio. `us-west-2`
> Sostituiscilo *amzn-s3-demo-bucket* con il nome effettivo del bucket Amazon S3 nella tua distribuzione. Puoi anche utilizzare un asterisco (*) al posto di *amzn-s3-demo-bucket* per creare una voce jolly nelle regole del firewall, che consentirà di elencare gli endpoint del servizio per tutti i nomi dei bucket.
> Se i gateway sono distribuiti negli Stati Uniti d'America o Regioni AWS in Canada e richiedono connessioni endpoint conformi allo standard FIPS (Federal Information Processing Standard), sostituiscili con. *s3* `s3-fips`

Tipi di endpoint

Endpoint standard

Questi endpoint supportano il IPv4 traffico tra l'appliance gateway e. AWS

Il seguente endpoint di servizio è richiesto da tutti i gateway per le operazioni head-bucket.

```
bucket-name.s3.region.amazonaws.com:443
```

I seguenti endpoint di servizio sono richiesti da tutti i gateway per le operazioni control path (`anon-cp`,`client-cp`,`proxy-app`) e data path (). `dp-1`

```
anon-cp.storagegateway.region.amazonaws.com:443
client-cp.storagegateway.region.amazonaws.com:443
proxy-app.storagegateway.region.amazonaws.com:443
dp-1.storagegateway.region.amazonaws.com:443
```

Il seguente endpoint di servizio gateway è obbligatorio per effettuare chiamate API.

```
storagegateway.region.amazonaws.com:443
```

L'esempio seguente è un endpoint di servizio gateway nella regione Stati Uniti occidentali (Oregon) (`us-west-2`).

```
storagegateway.us-west-2.amazonaws.com:443
```

Oltre agli endpoint del servizio Storage Gateway e Amazon S3, Storage Gateway richiede VMs anche l'accesso di rete ai seguenti server NTP:

```
time.aws.com
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

Per ulteriori informazioni sugli endpoint supportati Regioni AWS e di servizio, vedere Storage Gateway nel Riferimenti generali di AWS.

Configurazione dei gruppi di sicurezza per l'istanza del gateway Amazon EC2

Nel Gateway di archiviazione AWS, un gruppo di sicurezza controlla il traffico verso la tua istanza gateway Amazon EC2. Quando configuri un gruppo di sicurezza, tieni presente quanto segue:

- Il gruppo di sicurezza non deve permettere connessioni in entrata dall'esterno di Internet. Deve consentire solo alle istanze al suo interno di comunicare con il gateway.

  Se devi consentire alle istanze di connettersi al gateway dall'esterno del relativo gruppo di sicurezza, ti consigliamo di consentire le connessioni solo sulla porta 80 (per l'attivazione).
- Per attivare il gateway da un host Amazon EC2 al di fuori del suo gruppo di sicurezza, consenti le connessioni in entrata sulla porta 80 dall'indirizzo IP di tale host. Se non puoi determinare l'indirizzo IP dell'host di attivazione, apri la porta 80, attiva il gateway e, ad attivazione eseguita, chiudi l'accesso alla porta.

- Consenti l'accesso alla porta 22 solo se la utilizzi Supporto per la risoluzione dei problemi. Per ulteriori informazioni, consulta Vuoi aiutarci Supporto a risolvere i problemi del tuo gateway Amazon EC2.

Hypervisor supportati e requisiti di hosting

È possibile eseguire Storage Gateway in locale come appliance di macchina virtuale (VM) o dispositivo hardware fisico oppure come istanza AWS Amazon EC2.

> **Note**
>
> La modalità di avvio UEFI con avvio sicuro disabilitato (loader_secure=no) è richiesta per File Gateway 2.x, Volume Gateway 3.x e Tape Gateway 3.x. Un file xml viene fornito con ogni download di qcow come configurazione di configurazione rapida.

Storage Gateway supporta le seguenti versioni di hypervisor e host:

- VMware ESXi Hypervisor (versione 7.0 o 8.0): per questa configurazione, è necessario anche un client VMware vSphere per connettersi all'host.
- Microsoft Hyper-V Hypervisor (2019, 2022 o 2025): per questa configurazione, è necessario un Microsoft Hyper-V Manager su un computer client Microsoft Windows per connettersi all'host.
- Macchina virtuale basata su kernel (KVM) Linux: una tecnologia di virtualizzazione gratuita e open-source. KVM è incluso in tutte le versioni di Linux 2.6.20 e successive. Storage Gateway è testato e supportato per le distribuzioni CentOS/RHEL 7.7, RHEL 8.6 Ubuntu 16.04 LTS e Ubuntu 18.04 LTS. Qualsiasi altra distribuzione Linux moderna può funzionare, ma la funzione o le prestazioni non sono garantite. Si consiglia questa opzione se si dispone già di un ambiente KVM attivo e si ha già familiarità con il funzionamento di KVM. Per le configurazioni di avvio suggerite, fare riferimento al file.xml fornito. aws-storage-gateway La modalità di avvio UEFI con avvio sicuro disabilitato (loader_secure=no) è richiesta per File Gateway 2.x, Volume Gateway 3.x e Tape Gateway 3.x.
- Nutanix AHV (Acropolis Hypervisor) a partire dalla versione 10.0.1.1: una piattaforma di virtualizzazione basata su KVM integrata nella soluzione di infrastruttura iperconvergente (HCI) Nutanix.
- Istanza Amazon EC2: Storage Gateway fornisce un'Amazon Machine Image (AMI) che contiene l'immagine della macchina virtuale del gateway. Per informazioni su come distribuire un gateway su Amazon EC2, consulta Implementa un host FSx Amazon EC2 predefinito per File Gateway.

- Storage Gateway Hardware Appliance: Storage Gateway fornisce un'appliance hardware fisica come opzione di implementazione locale per sedi con un'infrastruttura di macchine virtuali limitata.

> **Note**
>
> Storage Gateway non supporta il recupero di un gateway da una macchina virtuale che è stata creata da una snapshot o da un clone di un'altra macchina virtuale gateway o dall'immagine macchina Amazon di Amazon EC2. Se la macchina virtuale gateway non funziona correttamente, attivare un nuovo gateway e ripristinare i dati su quel gateway. Per ulteriori informazioni, consulta Ripristino da un arresto imprevisto della macchina virtuale. Storage Gateway non supporta il ballooning di memoria dinamica e memoria virtuale.

Client SMB supportati per File Gateway

File Gateway supporta i seguenti client Service Message Block (SMB):

- Microsoft Windows Server 2008 R2 e versioni successive
- Versioni desktop Windows: 10, 8 e 7.
- Windows Terminal Server in esecuzione su Windows Server 2008 e versioni successive

> **Note**
>
> La crittografia Server Message Block richiede client che supportano i dialetti SMB v3.x.

Operazioni di file system supportate per File Gateway

Il tuo client SMB può scrivere, leggere, eliminare e troncare i file. Quando i client inviano scritture a Storage Gateway, queste scrivono nella cache locale in modo sincrono. Quindi scrive su Amazon in modo FSx asincrono tramite trasferimenti ottimizzati. Le letture vengono servite automaticamente tramite la cache locale. Se i dati non sono disponibili, vengono recuperati tramite Amazon FSx come cache di lettura.

Le operazioni di lettura e scrittura sono ottimizzate in modo tale che solo le parti modificate o richieste vengano tramite gateway. Elimina i file rimossi da Amazon FSx.

Gestione dei dischi locali per il gateway

La macchina virtuale (VM) del gateway usa i dischi locali allocati on-premises per il buffering e lo storage. Un File Gateway creato su un'istanza Amazon EC2 utilizzerà i volumi Amazon EBS come dischi locali. Il numero e la dimensione dei dischi da allocare per il gateway dipende da te. Il gateway utilizza lo storage cache allocato per fornire un accesso a bassa latenza ai dati a cui hai avuto accesso di recente. Lo storage cache funge da archivio durevole locale per i dati in attesa di caricamento su Amazon . FSx I File Gateway richiedono almeno un disco da 150 GiB da utilizzare come cache. Dopo la configurazione e l'implementazione iniziali del gateway, è possibile aggiungere altri dischi per l'archiviazione della cache man mano che le richieste di carico di lavoro aumentano. Questa sezione contiene i seguenti argomenti, che descrivono concetti e procedure relativi alla gestione dei dischi locali.

Argomenti

- Determinazione della quantità di archiviazione su disco locale- Scopri come determinare il numero e la dimensione dei dischi di cache locale da allocare per File Gateway.
- Configurazione di una memoria cache aggiuntiva- Scoprite come aumentare la capacità di archiviazione della cache di File Gateway man mano che le esigenze dell'applicazione cambiano.
- Utilizzo dello storage temporaneo con i gateway EC2- Scopri come prevenire la perdita di dati quando utilizzi lo storage temporaneo su disco con File Gateway.

Determinazione della quantità di archiviazione su disco locale

Quando implementate un , considerate la quantità di disco di cache da allocare. utilizza un algoritmo utilizzato meno di recente per eliminare automaticamente i dati dalla cache. La cache su un è condivisa tra tutte le condivisioni di file su quel gateway. Se disponi di più condivisioni attive, è importante notare che un utilizzo intensivo di una condivisione potrebbe influire sulla quantità di risorse di cache a cui un'altra condivisione ha accesso, con possibili ripercussioni sulle prestazioni.

Quando si determina la quantità di disco di cache necessaria per un determinato carico di lavoro, è importante notare che è sempre possibile aggiungere un disco cache al gateway (fino alle quote correnti su), ma non è possibile ridurre la cache per un determinato gateway. È possibile eseguire un'analisi di base sul set di dati per determinare la giusta quantità di disco di cache, ma non esiste un modo per determinare esattamente quanti dati siano «caldi» e debbano essere archiviati localmente, anziché «freddi» e possano essere trasferiti su più livelli nel cloud. I carichi di lavoro cambiano nel

tempo e offre flessibilità ed elasticità legate alla quantità di risorse che possono essere consumate. La quantità di cache può sempre essere aumentata, quindi l'approccio più conveniente è spesso partire da piccole dimensioni e aumentare in base alle necessità.

È possibile utilizzare un'approssimazione iniziale di 150 GiB per effettuare il provisioning dei dischi per l'archiviazione della cache durante la configurazione del gateway. Puoi quindi utilizzare i parametri CloudWatch operativi di Amazon per monitorare l'utilizzo dello storage della cache e fornire più spazio di archiviazione in base alle esigenze utilizzando la console. Per informazioni sull'uso dei parametri e sull'impostazione di allarmi, consulta Prestazioni e ottimizzazione.

> **Note**
>
> Le risorse di storage fisico sottostanti sono rappresentate come un archivio dati in VMware. Quando si distribuisce la macchina virtuale del gateway, si sceglie un datastore in cui archiviare i file VM. Quando si esegue il provisioning di un disco locale (ad esempio, da utilizzare come archiviazione cache), è possibile archiviare il disco virtuale nello stesso archivio dati della macchina virtuale o in un archivio dati diverso.
> Se disponi di più di un data store, ti consigliamo vivamente di scegliere un data store per l'archiviazione nella cache. Un data store supportato da un solo disco fisico sottostante può portare a prestazioni scadenti in alcune situazioni quando viene utilizzato per il backup di entrambi gli archivi della cache. Questo vale anche se il backup è una configurazione RAID meno performante come. RAID1

Configurazione di una memoria cache aggiuntiva

Man mano che le esigenze dell'applicazione cambiano, è possibile aumentare la capacità di archiviazione della cache del gateway. È possibile aggiungere capacità di archiviazione al gateway senza interrompere la funzionalità o causare tempi di inattività. Quando aggiungi ulteriore spazio di archiviazione, esegui l'operazione con la macchina virtuale del gateway attivata.

> **Important**
>
> Quando aggiungi cache a un gateway esistente, devi creare nuovi dischi sull'hypervisor host del gateway o sull'istanza Amazon EC2. Non rimuovere o modificare le dimensioni dei dischi esistenti che sono già stati allocati come cache.

Per configurare una memoria cache aggiuntiva per il gateway

1. Effettua il provisioning di uno o più nuovi dischi sull'hypervisor host del gateway o sull'istanza Amazon EC2. Per informazioni su come effettuare il provisioning di un disco in un hypervisor, consulta la documentazione dell'hypervisor. Per informazioni sul provisioning dei volumi Amazon EBS per un'istanza Amazon EC2, consulta Volumi Amazon EBS nella Guida per l'utente di Amazon Elastic Compute Cloud per le istanze Linux. Nei passaggi seguenti, configurerai questo disco come memoria cache.
2. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
3. Nel riquadro di navigazione, scegliere Gateways.
4. Nell'elenco, cerca e seleziona il tuo gateway.
5. Dal menu Azioni, scegli Configura l'archiviazione della cache.
6. Nella sezione Configura l'archiviazione della cache, identifica i dischi di cui hai effettuato il provisioning. Se i dischi non sono visualizzati, scegli l'icona di aggiornamento per aggiornare l'elenco. Per ogni disco, scegli Cache dal menu a discesa Allocato a.

   > **Note**
   >
   > La cache è l'unica opzione disponibile per l'allocazione dei dischi su un File Gateway.

7. Per salvare le impostazioni di configurazione, seleziona Salva.

Utilizzo dello storage temporaneo con i gateway EC2

Si sconsiglia l'uso di dischi temporanei per l'archiviazione della cache su File Gateway. FSx

I dischi temporanei forniscono uno storage temporaneo a livello di blocco per l'istanza Amazon EC2. Quando avvii il gateway con un'Amazon Machine Image di Amazon EC2 e il tipo di istanza selezionato supporta lo storage temporaneo, i dischi temporanei vengono elencati automaticamente. Puoi selezionare uno dei dischi per archiviare i dati della cache del gateway. Per ulteriori informazioni, consulta Amazon EC2 instance store nella Amazon EC2 User Guide.

> **Important**
>
> Se arresti e avvii un gateway Amazon EC2 che utilizza l'archiviazione temporanea, il gateway sarà definitivamente offline. Questo accade perché il disco di storage fisico viene sostituito.

Non esiste alcuna soluzione alternativa per questo problema. L'unica soluzione è eliminare il gateway e attivarne uno nuovo su una nuova istanza EC2.

Utilizzo dell'appliance hardware AWS Storage Gateway

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

L'appliance hardware AWS Storage Gateway è un'appliance hardware fisica con il software Storage Gateway preinstallato su una configurazione server convalidata. È possibile gestire le appliance hardware della distribuzione dalla pagina di panoramica dell'appliance hardware nella console. Gateway di archiviazione AWS

L'appliance hardware è un server 1U ad alte prestazioni che è possibile distribuire nel proprio data center, oppure on-premise all'interno di un firewall aziendale. Quando acquisti e attivi l'appliance hardware, il processo di attivazione associa l'appliance hardware al tuo. Account AWS Dopo l'attivazione, l'appliance hardware viene visualizzata nella console nella pagina di panoramica dell'appliance hardware. È possibile configurare l'appliance hardware come tipo S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway. La procedura utilizzata per distribuire questi tipi di gateway su un'appliance hardware è la stessa utilizzata su una piattaforma virtuale.

Per un elenco delle aree supportate Regioni AWS in cui l'appliance hardware AWS Storage Gateway è disponibile per l'attivazione e l'uso, vedere AWS Storage Gateway Hardware Appliance Regions nel. Riferimenti generali di AWS

Nelle sezioni seguenti sono disponibili istruzioni su come configurare, montare su rack, alimentare, configurare, attivare, avviare, utilizzare ed eliminare un'appliance hardware AWS Storage Gateway.

Argomenti

Configurazione dell'appliance hardware AWS Storage Gateway

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Dopo aver ricevuto l'appliance hardware Storage Gateway, si utilizza la console locale dell'appliance hardware per configurare la rete in modo da fornire una connessione sempre attiva e attivare l'appliance. AWS L'attivazione associa l'appliance all' AWS account utilizzato durante il processo di attivazione. Dopo l'attivazione dell'appliance, è possibile avviare S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway dalla console Storage Gateway.

Installare e configurare l'appliance hardware

1. Montare l'appliance su rack e collegare l'alimentazione e le connessioni di rete. Per ulteriori informazioni, consulta Installazione fisica del dispositivo hardware.
2. Imposta gli indirizzi Internet Protocol versione 4 (IPv4) per l'appliance hardware (l'host). Per ulteriori informazioni, consulta Configurazione dei parametri di rete dell'apparecchiatura hardware.
3. Attiva l'appliance hardware nella pagina di panoramica dell'appliance hardware della console nella AWS regione di tua scelta. Per ulteriori informazioni, consulta Attivazione del dispositivo hardware AWS Storage Gateway.

4. Crea un gateway sul tuo dispositivo hardware. Per ulteriori informazioni, consulta Crea il tuo gateway.

   Si configurano i gateway sull'appliance hardware nello stesso modo in cui si configurano i gateway su VMware ESXi, Microsoft Hyper-V, macchina virtuale basata su kernel (KVM) Linux o Amazon EC2.

Aumento dello storage della cache utilizzabile

È possibile aumentare lo spazio di archiviazione utilizzabile sull'appliance hardware da 5 TB a 12 TB. In questo modo si ottiene una cache più ampia per l'accesso a bassa latenza ai dati in ingresso. AWS Se hai ordinato il modello da 5 TB, puoi aumentare lo spazio di archiviazione utilizzabile a 12 TB acquistando cinque unità a stato solido da 1,92 SSDs TB.

È quindi possibile aggiungerli all'appliance hardware prima di attivarla. Se l'appliance hardware è già stata attivata e di desidera aumentare l'archiviazione utilizzabile sull'appliance a 12 TB, procedere nel seguente modo:

1. Ripristina le impostazioni di fabbrica dell'appliance hardware. Contatta l' AWS assistenza per istruzioni su come eseguire questa operazione.
2. Aggiungi cinque 1,92 TB SSDs all'appliance.

Opzioni della scheda di interfaccia di rete

A seconda del modello di dispositivo ordinato, può essere fornito con una scheda di rete 10G-Base-T in RJ45 rame o una scheda di rete DA/SFP+ 10G.

- Configurazione 10 NIC: G-Base-T
  - Utilizzare CAT6 cavi per 10G o CAT5 (e) per 1G
- Configurazione NIC 10G DA/SFP+:
  - Utilizzare cavi Twinax in rame Direct Attach fino a 5 metri
  - Moduli ottici SFP+ compatibili con Dell/Intel (SR o LR)
  - Ricetrasmettitore in rame SFP/SFP+ per 1 o 10G-Base-T G-Base-T

Installazione fisica del dispositivo hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

L'appliance ha un fattore di forma 1U e si inserisce in un rack da 19 pollici standard conforme alla Commissione elettrotecnica internazionale (IEC).

Prerequisiti

Per installare l'appliance hardware, sono necessari i seguenti componenti:

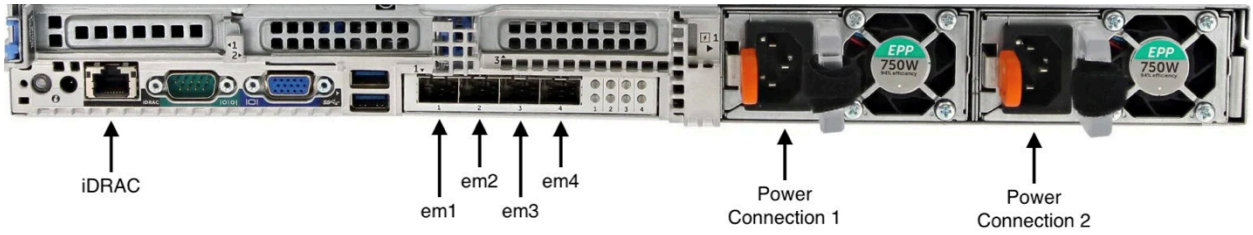
- Cavi di alimentazione: uno necessario, due consigliati.
- Cablaggio di rete supportato (a seconda della scheda di interfaccia di rete (NIC) incluso nell'appliance hardware). DAC Twinax in rame, modulo ottico SFP+ (compatibile con Intel) o ricetrasmettitore in rame da SFP a Base-T.
- Tastiera e monitor, oppure una soluzione tastiera, video e mouse (KVM).

> **Note**
>
> Prima di effettuare la procedura seguente, verificare di soddisfare tutti i requisiti per l'appliance hardware Storage Gateway come descritto in Requisiti di rete e di firewall per l'appliance hardware Storage Gateway.

Per installare fisicamente il dispositivo hardware

1. Estrai dalla confezione il dispositivo hardware e segui le istruzioni contenute nella confezione per montare il server su rack.

L'immagine seguente mostra la parte posteriore del dispositivo hardware con porte per il collegamento di alimentazione, ethernet, monitor, tastiera USB e iDRAC.
dispositivo hardware (uno posteriore) con etichette per connettori di rete e di alimentazione.



dispositivo hardware sul retro con etichette per connettori di rete e di alimentazione.

2. Collegare all'alimentazione ciascuno dei due alimentatori. È possibile collegarlo a una sola connessione di alimentazione, ma consigliamo di collegare entrambi gli alimentatori per garantire la ridondanza.
3. Inserire il cavo Ethernet nella porta `em1` per una connessione Internet sempre attiva. La porta `em1` è la prima delle quattro porte di rete fisiche nella parte posteriore, da sinistra a destra.

> **Note**
>
> L'appliance hardware non supporta il trunking VLAN. Configurare la porta a cui si sta collegando l'appliance hardware come porta senza trunking VLAN.

4. Collegare la tastiera e il monitor.
5. Accendere il server premendo il pulsante Power sul pannello anteriore, come mostrato nell'immagine seguente.
parte anteriore dell'appliance hardware con etichetta del pulsante di accensione.

parte anteriore dell'appliance hardware con etichetta del pulsante di accensione.

Approfondimenti

[Accesso alla console dell'apparecchiatura hardware]

Accesso alla console dell'apparecchiatura hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Quando si accende l'appliance hardware, la console dell'appliance hardware viene visualizzata sul monitor. La console dell'appliance hardware presenta un'interfaccia utente specifica AWS che è possibile utilizzare per impostare una password di amministratore, configurare i parametri di rete iniziali e aprire un canale di supporto per. AWS

Per utilizzare la console dell'appliance hardware, immettete il testo dalla tastiera e utilizzate i `Left Arrow` tasti Up `DownRight`,, e per spostarvi sullo schermo nella direzione indicata. Utilizzare il tasto `Tab` per andare avanti in ordine tra gli elementi sullo schermo. In alcune configurazioni, è possibile utilizzare la combinazione di tasti `Shift+Tab` per spostarsi sequenzialmente all'indietro. Utilizzare il tasto `Enter` per salvare le selezioni oppure per scegliere un pulsante sullo schermo.

La prima volta che viene visualizzata la console dell'appliance hardware, viene visualizzata la pagina di benvenuto e all'utente viene richiesto di impostare una password per l'account utente amministratore prima di poter accedere alla console.

Per impostare una password di amministratore

- Alla richiesta di impostazione della password di accesso, procedi come segue:

  a. In Set Password (Imposta password), immettere una password e premere `Down arrow`.
  b. In Confirm (Conferma), immettere nuovamente la password e quindi scegliere Save Password (Salva password).

Dopo aver impostato la password, viene visualizzata la home page della console hardware. La home page mostra le informazioni di rete per le interfacce di rete em1, em2, em3 ed em4 e presenta le seguenti opzioni di menu:

- Configura rete
- Apri Service Console
- Modifica della password
- Disconnettersi
- Apri Support Console

Approfondimenti

[Configurazione dei parametri di rete dell'apparecchiatura hardware]

Configurazione dei parametri di rete dell'apparecchiatura hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Dopo l'avvio dell'appliance hardware e aver impostato la password dell'utente amministratore nella console hardware come descritto in[Accesso alla console dell'apparecchiatura hardware], utilizzare la procedura seguente per configurare i parametri di rete a cui l'appliance hardware possa connettersi. AWS

Per impostare un indirizzo di rete

1. Dalla home page, scegli Configura rete, quindi premi. `Enter` Viene visualizzata la pagina Configura rete. La pagina Configura rete mostra le informazioni IP e DNS per ciascuna delle 4 interfacce di rete dell'appliance hardware e include le opzioni di menu per configurare gli indirizzi DHCP o statici per ciascuna.
2. Per l'interfaccia em1, effettuate una delle seguenti operazioni:

   - Scegliete DHCP e premete `Enter` per utilizzare l' IPv4 indirizzo assegnato dal server DHCP (Dynamic Host Configuration Protocol) alla porta di rete fisica.

Annota questo indirizzo per utilizzarlo successivamente nella fase di attivazione.

- Scegli Statico e premi `Enter` per configurare un IPv4 indirizzo statico.

  Inserisci un indirizzo IP, una subnet mask, un gateway e un indirizzo del server DNS validi per l'interfaccia di rete em1.

  Al termine, scegli Salva, quindi premi `Enter` per salvare la configurazione.

> **Note**
>
> È possibile utilizzare questa procedura per configurare altre interfacce di rete oltre a em1. Se configuri altre interfacce, queste devono fornire la stessa connessione sempre attiva agli endpoint elencati nei requisiti. AWS
> Il Network Bonding e il Link Aggregation Control Protocol (LACP) non sono supportati dall'appliance hardware o da Storage Gateway.
> Si sconsiglia di configurare più interfacce di rete sulla stessa sottorete, in quanto ciò può talvolta causare problemi di routing.

Per disconnettersi dalla console hardware

1. Scegli Indietro e premi **`Enter`** per tornare alla home page.
2. Scegli Logout e premi `Enter` per tornare alla pagina di benvenuto.

Approfondimenti

Attivazione del dispositivo hardware AWS Storage Gateway

Attivazione del dispositivo hardware AWS Storage Gateway

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione

AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Dopo aver configurato l'indirizzo IP, inserite questo indirizzo IP nella pagina Hardware della Gateway di archiviazione AWS console per attivare il dispositivo hardware. Il processo di attivazione registra l'appliance nell'account dell'utente. AWS

È possibile scegliere di attivare il dispositivo hardware in uno dei sistemi supportati. Regioni AWS Per un elenco delle aree supportate Regioni AWS, vedere Storage Gateway Hardware Appliance Regions nel Riferimenti generali di AWS.

Per attivare l'appliance hardware AWS Storage Gateway

1. Apri la Console di gestione Gateway di archiviazione AWS e accedi con le credenziali dell'account che desideri utilizzare per attivare l'hardware.

   > **Note**
   >
   > I seguenti requisiti sono necessari solo per l'attivazione:
   >
   > - Il browser deve trovarsi nella stessa rete dell'appliance hardware.
   > - Il firewall deve consentire l'accesso HTTP all'appliance sulla porta 8080 per il traffico in entrata.

2. Dal menu di navigazione a sinistra della pagina, scegli Hardware.
3. Scegli Attiva dispositivo.
4. Per Indirizzo IP, inserisci l'indirizzo IP che hai configurato per il dispositivo hardware, quindi scegli Connetti.

   Per ulteriori informazioni sulla configurazione dell'indirizzo IP, consulta Configurazione dei parametri di rete.
5. Per Nome, inserisci un nome per il dispositivo. I nomi possono contenere fino a 255 caratteri e non possono includere uno slash.
6. Per Fuso orario del dispositivo hardware inserisci il fuso orario locale da cui verrà generata la maggior parte del carico di lavoro per il gateway, quindi scegli Avanti.

Il fuso orario determina quando l'hardware effettua gli aggiornamenti; con l'orario pianificato per impostazione predefinita sulle 2 di notte ora locale. Idealmente, se il fuso orario è impostato correttamente, per impostazione predefinita gli aggiornamenti avverranno al di fuori dell'orario di lavoro.

7. Consulta i parametri di attivazione nella sezione relativa ai dettagli dell'apparecchiatura hardware. Puoi scegliere Precedente per tornare indietro e apportare modifiche, se necessario. Altrimenti, scegli Attiva per completare l'attivazione.

Nella pagina Panoramica del dispositivo hardware verrà visualizzato un banner che indica che il dispositivo hardware è stato attivato correttamente.

A questo punto, l'appliance è associata all'account. Il passaggio successivo consiste nel configurare e avviare un S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway sulla nuova appliance.

Approfondimenti

Creazione di un gateway sul tuo dispositivo hardware

Creazione di un gateway sul tuo dispositivo hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l' Gateway di archiviazione AWS Hardware Appliance non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

È possibile creare un S3 File Gateway, FSx File Gateway, Tape Gateway o Volume Gateway su qualsiasi appliance hardware AWS Storage Gateway presente nell'implementazione.

Per creare un gateway sull'appliance hardware

1. Accedi Console di gestione AWS e apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.

2. Segui le procedure descritte in Creazione del gateway per configurare, connettere e configurare il tipo di Storage Gateway che desideri implementare.

Al termine della creazione del gateway nella console Storage Gateway, il software Storage Gateway inizia automaticamente l'installazione sull'appliance hardware. Se si utilizza il Dynamic Host Configuration Protocol (DHCP), possono essere necessari dai 5 ai 10 minuti prima che un gateway venga visualizzato come online nella console. Per assegnare un indirizzo IP statico al gateway installato, vedere Configurazione di un indirizzo IP per il gateway per il gateway.

Per assegnare un indirizzo IP statico al gateway installato, è necessario configurare le interfacce di rete del gateway in modo che le applicazioni possano utilizzarlo.

Approfondimenti

Configurazione di un indirizzo IP del gateway sull'appliance hardware

Configurazione di un indirizzo IP del gateway sull'appliance hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l' Gateway di archiviazione AWS Hardware Appliance non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Prima di attivare l’appliance hardware, è stato assegnato un indirizzo IP alla relativa interfaccia di rete fisica. Dopo aver attivato l'appliance e avviato lo Storage Gateway su di essa, è necessario assegnare un altro indirizzo IP alla macchina virtuale Storage Gateway in esecuzione sull'appliance hardware. Per assegnare un indirizzo IP statico a un gateway installato sul dispositivo hardware, configura l'indirizzo IP dalla console locale del gateway per quel gateway. Le applicazioni (come il client NFS o SMB) si connettono a questo indirizzo IP. È possibile accedere alla console locale del gateway dalla console dell'appliance hardware utilizzando l'opzione Open Service Console.

Per configurare l'indirizzo IP sull'appliance per farla funzionare con le applicazioni.

1. Sulla console hardware, scegli Open Service Console, quindi premi `Enter` per aprire la pagina di accesso per la console locale del gateway.
2. La pagina di accesso alla console Gateway di archiviazione AWS locale richiede di effettuare il login per modificare la configurazione di rete e altre impostazioni.

   L'account predefinito è `admin` e la password predefinita è `password`.

   > **Note**
   >
   > Si consiglia di modificare la password predefinita inserendo il numero corrispondente per Console del gateway dal menu principale Attivazione dell'appliance AWS : configurazione, eseguendo poi il comando `passwd`. Per informazioni su come eseguire il comando, consulta Esecuzione di comandi Storage Gateway sulla console locale. È inoltre possibile impostare la password dalla console Storage Gateway. Per ulteriori informazioni, consulta Impostazione della password della console locale dalla console Storage Gateway.

3. La pagina Attivazione dell'AWS appliance - Configurazione include le seguenti opzioni di menu:

   - Configurazione del proxy HTTP/SOCKS
   - Configurazione di rete
   - Test della connettività di rete
   - Visualizza il controllo delle risorse di sistema
   - Gestione del tempo di sistema
   - Informazioni sulla licenza
   - Prompt dei comandi

   > **Note**
   >
   > Alcune opzioni sono disponibili solo per tipi di gateway o piattaforme host specifici.

   Immettete il numero corrispondente per accedere alla pagina di configurazione della rete.

4. Effettuate una delle seguenti operazioni per configurare l'indirizzo IP del gateway:

- Per utilizzare l'indirizzo IP assegnato dal server DHCP (Dynamic Host Configuration Protocol), immettete il numero corrispondente per Configura DHCP, quindi immettete informazioni di configurazione DHCP valide nella pagina seguente.
- Per assegnare un indirizzo IP statico, inserisci il numero corrispondente per Configura IP statico, quindi inserisci un indirizzo IP e informazioni DNS valide nella pagina seguente.

> **Note**
>
> L'indirizzo IP specificato qui deve trovarsi nella stessa sottorete dell'indirizzo IP utilizzato durante l'attivazione dell'appliance hardware.

Per uscire dalla console locale del gateway

- Premere la sequenza di tasti `Crtl+]` (parentesi di chiusura). Viene visualizzata la console hardware.

> **Note**
>
> La combinazione di tasti precedente è l'unico modo per uscire dalla console locale del gateway.

Dopo che l'appliance hardware è stata attivata e configurata, l'appliance viene visualizzata nella console. Ora è possibile continuare la procedura di installazione e configurazione del gateway nella console Storage Gateway. Per istruzioni, consulta Configura il tuo Amazon FSx File Gateway.

Rimozione del software gateway dal dispositivo hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l' Gateway di archiviazione AWS Hardware Appliance non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per

fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Se non è più necessario uno Storage Gateway specifico distribuito su un'appliance hardware, è possibile rimuovere il software del gateway dall'appliance hardware. Dopo aver rimosso il software del gateway, è possibile scegliere di installare un nuovo gateway al suo posto o eliminare l'appliance hardware stessa dalla console Storage Gateway. Per rimuovere un software del gateway dall'appliance hardware, utilizzare la procedura seguente.

Rimuovere un gateway da un'appliance hardware

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Hardware dal pannello di navigazione sul lato sinistro della pagina della console, quindi scegli il nome dell'appliance hardware per l'appliance da cui desideri rimuovere il software gateway.
3. Dal menu a discesa Azioni, scegli Rimuovi gateway.

   Viene visualizzata la finestra di dialogo di conferma.
4. Verifica di voler rimuovere il software del gateway dall'appliance hardware specificata, quindi digita la parola `remove` nella casella di conferma.
5. Scegliete Rimuovi per rimuovere definitivamente il software del gateway.

> **Note**
>
> Dopo aver rimosso il software del gateway, non puoi annullare l'azione. Per determinati tipi di gateway, è possibile che con l'eliminazione si perdano dei dati, soprattutto quelli memorizzati nella cache. Per ulteriori informazioni sull'eliminazione di un gateway, consulta Eliminazione del gateway e rimozione delle risorse associate.

La rimozione di un gateway non elimina l'appliance hardware dalla console. L'appliance hardware rimane disponibile per future implementazioni del gateway.

Eliminazione del dispositivo hardware AWS Storage Gateway

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Se non è più necessario un dispositivo hardware AWS Storage Gateway già attivato, è possibile eliminare completamente l'appliance dal proprio account AWS .

> **Note**
>
> Per spostare l'appliance su un altro AWS account o Regione AWS, è necessario prima eliminarla utilizzando la procedura seguente, quindi aprire il canale di supporto del gateway e contattarla Supporto per eseguire un soft reset. Per ulteriori informazioni, consulta Attivazione dell' Supporto accesso per risolvere i problemi del gateway ospitato in locale.

Per eliminare l'appliance hardware

1. Se è stato installato un gateway nell'appliance hardware, è necessario prima rimuovere il gateway per eliminare l'appliance. Per istruzioni su come rimuovere un gateway dall'appliance hardware, consulta Rimozione del software gateway dal dispositivo hardware.
2. Nella pagina Hardware della console Storage Gateway, scegliere l'appliance hardware che si desidera eliminare.
3. Per Actions (Operazioni), scegli Delete stack (Elimina stack). Viene visualizzata la finestra di dialogo di conferma.
4. Verifica di voler eliminare l'appliance hardware specificata, quindi digita la parola delete nella casella di conferma e scegli Elimina.

   Quando si elimina l'appliance hardware, vengono eliminate anche tutte le risorse associate con il gateway installato sull'appliance, ma i dati sull'appliance hardware stessa non vengono eliminati.

Crea il tuo gateway

Le sezioni di panoramica di questa pagina forniscono un riepilogo di alto livello di come funziona il processo di creazione dello Storage Gateway. Per step-by-step le procedure per creare un tipo specifico di gateway utilizzando la console Storage Gateway, vedere i seguenti argomenti:

- Creare e attivare un Amazon S3 File Gateway
- Crea e attiva un Amazon FSx File Gateway
- Crea e attiva un Tape Gateway
- Crea e attiva un Volume Gateway

> **Important**
>
> 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.

Panoramica: attivazione del gateway

L'attivazione del gateway prevede la configurazione del gateway, la sua connessione AWS, quindi la revisione delle impostazioni e l'attivazione.

Configurazione di un gateway

Per configurare Storage Gateway, è necessario innanzitutto scegliere il tipo di gateway che si desidera creare e la piattaforma host su cui eseguire l'appliance virtuale gateway. È quindi necessario scaricare il modello di appliance virtuale gateway per la piattaforma prescelta e distribuirlo nell'ambiente on-premise. Puoi anche implementare lo Storage Gateway come appliance hardware fisica che ordini dal tuo rivenditore preferito o come istanza Amazon EC2 nel tuo ambiente cloud. AWS Quando si distribuisce l'appliance gateway, si alloca lo spazio fisico locale su disco sull'host di virtualizzazione.

Connect a AWS

Il passaggio successivo consiste nel connettere il gateway a AWS. A tale scopo, devi innanzitutto scegliere il tipo di endpoint di servizio che desideri utilizzare per le comunicazioni tra l'appliance

virtuale gateway e AWS i servizi nel cloud. Questo endpoint può essere accessibile dalla rete Internet pubblica o solo dall'interno del tuo Amazon VPC, dove hai il pieno controllo sulla configurazione di sicurezza della rete. È quindi necessario specificare l'indirizzo IP del gateway o la relativa chiave di attivazione, che è possibile ottenere collegandosi alla console locale sull'appliance gateway.

Rivedi e attiva

A questo punto, avrai l'opportunità di rivedere il gateway e le opzioni di connessione che hai scelto e, se necessario, apportare modifiche. Una volta che tutto è configurato come desideri puoi attivare il gateway. Prima di poter iniziare a utilizzare il gateway attivato, è necessario configurare alcune impostazioni aggiuntive e creare le risorse di archiviazione.

Panoramica: configurazione del gateway

Dopo aver attivato Storage Gateway, è necessario eseguire una configurazione aggiuntiva. In questa fase, si alloca lo storage fisico fornito sulla piattaforma host del gateway per utilizzarlo come cache o buffer di caricamento dall'appliance gateway. Quindi configuri le impostazioni per monitorare lo stato del gateway utilizzando Amazon CloudWatch Logs and CloudWatch alarms e aggiungi tag per identificare il gateway, se lo desideri. Prima di poter iniziare a utilizzare il gateway attivato e configurato, è necessario creare le risorse di archiviazione.

Panoramica: risorse di archiviazione

Dopo aver attivato e configurato Storage Gateway, è necessario creare risorse di archiviazione cloud da utilizzare. A seconda del tipo di gateway creato, utilizzerai la console Storage Gateway per creare volumi, nastri o condivisioni di file Amazon S3 o FSx Amazon Amazon da associare. Ogni tipo di gateway utilizza le rispettive risorse per emulare il tipo correlato di infrastruttura di archiviazione di rete e trasferisce i dati che scrivi su di esso nel cloud AWS .

Crea un file system Amazon FSx per Windows File Server

Per creare un Amazon FSx File Gateway in Gateway di archiviazione AWS, il primo passaggio consiste nel creare un file system Amazon FSx per Windows File Server. Se hai già creato un FSx file system Amazon, vai al passaggio successivo,Crea e attiva un Amazon FSx File Gateway.

Note

Le seguenti limitazioni si applicano quando si scrive su un FSx file system Amazon da un FSx File Gateway:

- Il FSx file system Amazon e il FSx File Gateway devono appartenere allo stesso AWS account e trovarsi nella stessa AWS regione.
- Ogni gateway può supportare cinque file system collegati. Quando si collega un file system, la console Storage Gateway notifica all'utente se il gateway selezionato è al massimo della capacità. In tal caso, è necessario scegliere un gateway diverso o scollegare un file system prima di collegarne un altro.
- FSx File Gateway supporta le quote di storage software (emettendo avvisi quando gli utenti superano i limiti di dati), ma non supporta le quote rigide (imposizione dei limiti ai dati negando l'accesso in scrittura). Le quote soft sono supportate per tutti gli utenti tranne l'utente FSx amministratore di Amazon. Per ulteriori informazioni sull'impostazione delle quote di storage, consulta la sezione Quote di storage nella Amazon FSx for Windows File Server User Guide.
- Non consigliamo di utilizzare Microsoft Distributed File System (DFS) per reindirizzare gli utenti al tuo file system Amazon tramite FSx FSx File Gateway. Invece, configura DFS per il reindirizzamento diretto al FSx file system Amazon Cloud AWS come descritto in Raggruppamento di più file system con DFS Namespaces nella FSx Amazon for Windows File Server User Guide.
- Alcune operazioni sui file su FSx File Gateway, come la ridenominazione delle cartelle di primo livello o la modifica delle autorizzazioni, possono comportare più operazioni sui file che comportano un I/O carico elevato sul file system per Windows File Server. FSx Se il file system non dispone di risorse prestazionali sufficienti per il carico di lavoro, il file system potrebbe eliminare le copie shadow perché dà priorità alla disponibilità per la conservazione continua I/O rispetto alla conservazione delle copie shadow storiche.

  Nella FSx console Amazon, consulta la pagina Monitoraggio e prestazioni per verificare se il provisioning del file system è insufficiente. In tal caso, puoi passare allo storage SSD, aumentare la capacità di throughput o aumentare gli IOPS SSD per gestire il tuo carico di lavoro.

Per creare un file system FSx per Windows File Server

1. Apri Console di gestione AWS at https://console.aws.amazon.com/fsx/home/ e scegli la regione in cui vuoi creare il gateway.
2. Segui le istruzioni in Getting Started with Amazon FSx nella Amazon FSx for Windows File Server User Guide.

Crea e attiva un Amazon FSx File Gateway

In questa sezione, puoi trovare istruzioni su come creare, distribuire e attivare un File Gateway in Gateway di archiviazione AWS.

Argomenti

- Configura un Amazon FSx File Gateway
- Connect Amazon FSx File Gateway a AWS
- Rivedi le impostazioni e attiva Amazon FSx File Gateway
- Configura il tuo Amazon FSx File Gateway

Configura un Amazon FSx File Gateway

Per configurare un nuovo FSx File Gateway

1. Apri Console di gestione AWS at https://console.aws.amazon.com/storagegateway/home/ e scegli Regione AWS dove vuoi creare il tuo gateway.
2. Scegli Create gateway (Crea gateway) per aprire la pagina Set up gateway (Configura gateway).
3. Nella sezione Impostazioni gateway, procedi nel seguente modo:

    a. Per Gateway name (Nome gateway), inserire un nome per il gateway. Dopo aver creato il gateway, puoi cercare questo nome per trovarlo nelle pagine di elenco della Gateway di archiviazione AWS console.

    b. Per il Fuso orario del gateway, scegli il fuso orario locale per la parte del mondo in cui desideri implementare il gateway.
4. Nella sezione Opzioni gateway, per il tipo di gateway, scegli Amazon FSx File Gateway.
5. Nella sezione Opzioni piattaforma, procedi nel modo seguente:

a. Per la piattaforma Host, scegli la piattaforma su cui vuoi implementare il tuo gateway. Quindi segui le istruzioni specifiche della piattaforma visualizzate nella pagina della console Storage Gateway per configurare la piattaforma host. Scegliere tra le seguenti opzioni:

   - VMware ESXi— Scarica, distribuisci e configura la macchina virtuale gateway utilizzando. VMware ESXi
   - Microsoft Hyper-V: scarica, distribuisci e configura la macchina virtuale gateway utilizzando Microsoft Hyper-V.
   - Linux KVM: scarica, distribuisci e configura la macchina virtuale gateway utilizzando Linux Kernel-based Virtual Machine (KVM). Fate riferimento al file.xml fornito aws-storage-gateway per le configurazioni di avvio suggerite. La modalità di avvio UEFI con avvio sicuro disabilitato (loader_secure=no) è richiesta per File Gateway 2.x, Volume Gateway 3.x e Tape Gateway 3.x.
   - Amazon EC2: configura e avvia un'istanza Amazon EC2 per ospitare il tuo gateway.
   - Dispositivo hardware: ordina un dispositivo hardware fisico dedicato da AWS cui ospitare il gateway.

b. In Confirm set up gateway (Conferma configurazione gateway), seleziona la casella di controllo per confermare di aver eseguito i passaggi di implementazione per la piattaforma host scelta. Questo passaggio non è applicabile alla piattaforma host dell'appliance hardware.

6. Ora che il gateway è configurato, devi scegliere come connetterlo e comunicare. AWS Scegli Successivo per continuare.

Connect Amazon FSx File Gateway a AWS

Per connettere un nuovo FSx File Gateway a AWS

1. Se non l'hai già fatto, completa la procedura descritta in Configurare un Amazon FSx File Gateway. Al termine, scegli Avanti per aprire la AWS pagina Connect to nella Gateway di archiviazione AWS console.
2. Nella sezione Opzioni endpoint, per Service endpoint, scegli il tipo di endpoint con cui il gateway utilizzerà per comunicare. AWS Scegliere tra le seguenti opzioni:

- Accessibile al pubblico: il gateway comunica tramite la rete AWS Internet pubblica. Se si seleziona questa opzione, utilizza la casella di controllo Endpoint abilitato FIPS per specificare se la connessione deve essere conforme ai Federal Information Processing Standards (FIPS).

  > **Note**
  >
  > Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint conforme a FIPS. Per ulteriori informazioni, consulta Federal Information Processing Standard (FIPS) 140-2. L'endpoint del servizio FIPS è disponibile solo in alcune regioni. AWS Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS nella Riferimenti generali di AWS.

- VPC ospitato: il gateway comunica AWS tramite una connessione privata con il cloud privato virtuale (VPC), che consente di controllare le impostazioni di rete. Se si seleziona questa opzione, è necessario specificare un endpoint VPC esistente scegliendo il relativo ID endpoint VPC dall'elenco a discesa. Puoi anche fornire il nome o l'indirizzo IP del suo endpoint VPC Domain Name System (DNS).

3. Nella sezione Opzioni di connessione del gateway, per Opzioni di connessione, scegli come identificare il gateway verso AWS. Scegliere tra le seguenti opzioni:

   - Indirizzo IP: fornisci l'indirizzo IP del gateway nel campo corrispondente. Questo indirizzo IP deve essere pubblico o accessibile dall'interno della rete corrente e devi essere in grado di connetterti ad esso dal tuo browser web.

     Puoi ottenere l'indirizzo IP del gateway accedendo alla console locale del gateway dal tuo client hypervisor o copiandolo dalla pagina dei dettagli dell'istanza Amazon EC2.

   - Chiave di attivazione: fornite la chiave di attivazione per il gateway nel campo corrispondente. È possibile generare una chiave di attivazione utilizzando la console locale del gateway. Se l'indirizzo IP del gateway non è disponibile, scegli questa opzione.

4. Ora che hai scelto la modalità di connessione del gateway AWS, devi attivare il gateway. Scegli Successivo per continuare.

Rivedi le impostazioni e attiva Amazon FSx File Gateway

Per attivare un nuovo FSx File Gateway

1. Se non l'avete già fatto, completate le procedure descritte nei seguenti argomenti:

   - Configura un Amazon FSx File Gateway
   - Connect Amazon FSx File Gateway a AWS

   Al termine, scegli Avanti per aprire la pagina di revisione e attivazione nella Gateway di archiviazione AWS console.
2. Rivedi i dettagli iniziali del gateway per ogni sezione della pagina.
3. Se una sezione contiene errori, scegli Modifica per tornare alla pagina delle impostazioni corrispondente e apportare modifiche.

   > **Important**
   >
   > Non è possibile modificare le opzioni o le impostazioni di connessione del gateway dopo l'attivazione del gateway.

4. Dopo aver attivato il gateway, è necessario eseguire la prima configurazione per allocare i dischi di archiviazione locali e configurare la registrazione. Scegli Successivo per continuare.

Configura il tuo Amazon FSx File Gateway

Per eseguire la prima configurazione su un nuovo FSx File Gateway

1. Se non l'avete già fatto, completate le procedure descritte nei seguenti argomenti:

   - Configura un Amazon FSx File Gateway
   - Connect Amazon FSx File Gateway a AWS
   - Rivedi le impostazioni e attiva Amazon FSx File Gateway

   Al termine, scegli Avanti per aprire la pagina Configura gateway nella Gateway di archiviazione AWS console.

2. Nella sezione Configura archiviazione, utilizza gli elenchi a discesa per allocare almeno un disco locale con almeno 150 gibibyte (GiB) di capacità alla cache. I dischi locali elencati in questa sezione corrispondono allo spazio di archiviazione fisico fornito sulla piattaforma host.
3. Nella sezione dei gruppi di CloudWatch log, scegli come configurare Amazon CloudWatch Logs per monitorare lo stato del tuo gateway. Scegliere tra le seguenti opzioni:

   - Crea un nuovo gruppo di log: configura un nuovo gruppo di log per monitorare il tuo gateway.
   - Usa un gruppo di log esistente: scegli un gruppo di log esistente dall'elenco a discesa corrispondente.
   - Disattiva la registrazione: non utilizzare Amazon CloudWatch Logs per monitorare il gateway.

   > **Note**
   >
   > Per ricevere i log di integrità dello Storage Gateway, nella politica delle risorse del gruppo di log devono essere presenti le seguenti autorizzazioni. Sostituisci le *highlighted section* informazioni ResourceArn con il gruppo di log specifico per la tua distribuzione.
   >
   > ```
   > "Sid": "AWSLogDeliveryWrite20150319",
   >       "Effect": "Allow",
   >       "Principal": {
   >         "Service": [
   >           "delivery.logs.amazonaws.com"
   >         ]
   >       },
   >       "Action": [
   >         "logs:CreateLogStream",
   >         "logs:PutLogEvents"
   >       ],
   >       "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
   > ```
   >
   > L'elemento «Resource» è richiesto solo se si desidera che le autorizzazioni si applichino esplicitamente a un singolo gruppo di log.

4. Nella sezione CloudWatch allarmi, scegli come configurare gli CloudWatch allarmi Amazon per avvisarti quando le metriche del tuo gateway si discostano dai limiti definiti. Scegliere tra le seguenti opzioni:

- Crea allarmi consigliati da Storage Gateway: crea automaticamente tutti gli allarmi consigliati quando CloudWatch viene creato il gateway. Per ulteriori informazioni sugli allarmi consigliati, vedere Comprensione degli allarmi. CloudWatch

  > **Note**
  >
  > Questa funzionalità richiede autorizzazioni di CloudWatch policy che non vengono concesse automaticamente come parte della policy di accesso completo preconfigurata di Storage Gateway. Assicurati che la tua politica di sicurezza conceda le seguenti autorizzazioni prima di tentare di creare allarmi consigliati: CloudWatch
  >
  > - `cloudwatch:PutMetricAlarm`: creazione di allarmi
  > - `cloudwatch:DisableAlarmActions`: disattivazione delle azioni di allarme
  > - `cloudwatch:EnableAlarmActions`: attivazione delle azioni di allarme
  > - `cloudwatch:DeleteAlarms`: eliminazione di allarmi

- Crea un allarme personalizzato: configura un nuovo CloudWatch allarme per ricevere notifiche sulle metriche del gateway. Scegli Crea allarme per definire le metriche e specificare le azioni di allarme nella CloudWatch console Amazon. Per istruzioni, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.
- Nessun allarme: non utilizzare gli CloudWatch allarmi per ricevere notifiche sulle metriche del gateway.

5. (Facoltativo) Nella sezione Tag, scegli Aggiungi nuovo tag, quindi inserisci una coppia chiave-valore con distinzione tra maiuscole e minuscole per aiutarti a cercare e filtrare il gateway nelle pagine di elenco della console. Gateway di archiviazione AWS Ripeti questo passaggio per aggiungere quanti tag necessiti.
6. (Facoltativo) Nella sezione di configurazione Verify VMware High Availability, se il gateway è distribuito su un VMware host che fa parte di un cluster VMware High Availability (HA), scegli Verify VMware HA per verificare se la configurazione HA funziona correttamente.

   > **Note**
   >
   > Questa sezione viene visualizzata solo per i gateway in esecuzione sulla piattaforma VMware host.

Questo passaggio non è necessario per completare il processo di configurazione del gateway. È possibile testare la configurazione HA del gateway in qualsiasi momento. La verifica richiede alcuni minuti e riavvia la macchina virtuale (VM) Storage Gateway.

7. Scegli Configura per completare la creazione del gateway.

   Per verificare lo stato del nuovo gateway, cercalo nella pagina di panoramica del gateway della Gateway di archiviazione AWS console.

Dopo aver creato il gateway, è necessario allegare un file system da utilizzare. Per istruzioni, consulta Collegare un file system Amazon FSx for Windows File Server.

Se non disponi di un FSx file system Amazon esistente da allegare, devi crearne uno. Per istruzioni, consulta la sezione Guida introduttiva ad Amazon FSx.

Attivazione di un gateway in un cloud privato virtuale

È possibile creare una connessione privata tra l'applicazione gateway on-premise e l'infrastruttura di archiviazione basata sul cloud. È possibile utilizzare questa connessione per attivare il gateway e configurarlo per trasferire dati ai servizi AWS di archiviazione senza comunicare sulla rete Internet pubblica. Utilizzando il servizio Amazon VPC, puoi avviare AWS risorse, inclusi endpoint di interfaccia di rete privata, in un cloud privato virtuale (VPC) personalizzato. Un VPC fornisce il controllo delle impostazioni di rete, come l'intervallo di indirizzi IP, le sottoreti, le tabelle di routing e i gateway di rete. Per ulteriori informazioni su VPCs, consulta Cos'è Amazon VPC? nella Guida per l'utente di Amazon VPC.

Per attivare il gateway in un VPC, utilizza la console Amazon VPC per creare e ottieni l'ID dell'endpoint VPC, quindi specifica questo ID endpoint VPC quando crei e attivi il gateway. Per ulteriori informazioni, consulta Amazon FSx File Gateway a. AWS

Per configurare FSx File Gateway per il trasferimento di dati tramite VPC, è necessario stabilire una VPN o un AWS DirectConnect collegamento tra il VPC Amazon FSx for Windows File Server e la rete in cui è distribuito il gateway.

> **Note**
>
> È necessario attivare il gateway nella stessa regione in cui si crea l'endpoint VPC per Storage Gateway.

Crea un endpoint VPC per Storage Gateway

Per creare un endpoint VPC, attenersi alle istruzioni seguenti. Se disponi già di un endpoint VPC per Storage Gateway, puoi utilizzarlo.

Per creare un endpoint VPC per Storage Gateway

1. Accedi Console di gestione AWS e apri la console Amazon VPC all'indirizzo. https://console.aws.amazon.com/vpc/
2. Nel riquadro di navigazione, selezionare Endpoint e scegliere Create Endpoint (Crea endpoint).
3. Nella pagina Crea endpoint, scegliere Servizi AWS per Categoria del servizio.
4. Per Service Name (Nome del servizio), selezionare `com.amazonaws.region.storagegateway`. Ad esempio, `com.amazonaws.us-east-2.storagegateway`.
5. Per VPC, scegliere il VPC e annotare le zone di disponibilità e le sottoreti.
6. Verifica che l'opzione Abilita nome DNS non sia selezionata.
7. Per Gruppo di sicurezza, scegliere il gruppo di sicurezza che si desidera utilizzare per il VPC. È possibile accettare il gruppo di sicurezza predefinito. Verificare che tutte le seguenti porte TCP siano consentite nel gruppo di sicurezza:
   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. Seleziona Crea endpoint. Lo stato iniziale dell'endpoint è pending (in sospeso). Quando l'endpoint viene creato, prendere nota dell'ID dell'endpoint VPC appena creato.
9. Quando l'endpoint viene creato, scegliere Endpoint quindi il nuovo endpoint VPC.
10. Nella scheda Dettagli dell'endpoint del gateway di archiviazione selezionato, in Nomi DNS, utilizza il primo nome DNS che non specifica una zona di disponibilità. Il nome DNS dovrebbe essere simile al seguente esempio: `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

Ora che hai un endpoint VPC, puoi creare e attivare il tuo gateway. Per ulteriori informazioni, consulta Creare e attivare un Amazon FSx File Gateway.

Per informazioni su come ottenere una chiave di attivazione, consulta Ottenere una chiave di attivazione per il gateway.

Configurazione delle impostazioni di accesso al dominio Microsoft Active Directory

In questo passaggio, configuri le impostazioni di accesso per aggiungere Amazon FSx File Gateway a un dominio Microsoft Active Directory.

Per configurare le impostazioni di Active Directory

1. Nella console Storage Gateway, scegli i FSx file system dal menu di navigazione.
2. Scegli Allega FSx file system.
3. Nella pagina Conferma gateway, scegli il gateway che desideri aggiungere al tuo dominio Active Directory dal menu a discesa.

   Se non disponi di un gateway, devi crearne uno. Assicurati che il gateway sia in grado di risolvere il nome del controller di dominio Active Directory. Per informazioni, consulta Prerequisiti.
4. Immettete i valori per le impostazioni di Active Directory:

   > **Note**
   >
   > Se il gateway è già aggiunto a un dominio, non è necessario eseguire nuovamente l'accesso. Vai al passaggio successivo.

   - Per Nome di dominio, inserisci il nome di dominio dell'Active Directory che desideri utilizzare.
   - Per Utente di dominio, inserisci il nome utente dell'utente di Active Directory che desideri utilizzare per aggiungere il gateway al dominio. Questo utente deve disporre delle autorizzazioni necessarie. Per ulteriori informazioni, vedere Requisiti di dell'account del servizio Active Directory.
   - Per Password di dominio, inserisci la password per l'utente.
   - Per Unità organizzativa: facoltativo, è possibile specificare un'unità organizzativa a cui appartiene Active Directory.

     > **Note**
     >
     > Se si lascia vuoto questo campo, l'aggiunta a un dominio crea un account computer Active Directory nel contenitore predefinito dei computer (che non è un'unità

organizzativa), utilizzando l'ID gateway del gateway come nome dell'account (ad esempio, SGW-1234ADE). Non è possibile personalizzare il nome di questo account. Se l'ambiente Active Directory richiede la preconfigurazione degli account per facilitare il processo di aggiunta al dominio, sarà necessario creare questo account in anticipo. Se l'ambiente Active Directory dispone di un'unità organizzativa designata per i nuovi oggetti del computer, è necessario specificare tale unità organizzativa al momento dell'accesso al dominio.

- Immettere un valore per i controller di dominio, facoltativo.

5. Scegli Avanti per aprire la pagina Allega FSx file system.

Approfondimenti

Collega un file system Amazon FSx per Windows File Server

Collega un file system Amazon FSx per Windows File Server

È necessario disporre di un file system FSx per Windows File Server prima di poterlo collegare a un FSx File Gateway. Se non si dispone di un file system, è necessario crearne uno. Per istruzioni, consulta la Fase 1: Crea il tuo file system nella Guida FSx per l'utente di Amazon for Windows File Server.

Il passaggio successivo consiste nel collegare un FSx file system Amazon al gateway. Quando colleghi un FSx file system Amazon, tutte le condivisioni di file sul file system vengono rese disponibili ad Amazon FSx File Gateway (FSx File Gateway) per il montaggio.

> **Note**
>
> Le seguenti limitazioni si applicano quando si scrive su un FSx file system Amazon da Amazon FSx File Gateway:
>
> - Il tuo FSx file system Amazon e il tuo FSx File Gateway devono essere di proprietà dello stesso Account AWS e collocati nello stesso Regione AWS.
> - Ogni gateway può supportare fino a cinque file system collegati. Quando colleghi un file system, la console Storage Gateway ti avvisa se il gateway selezionato è al massimo della capacità. In tal caso, è necessario scegliere un gateway diverso o scollegare un file system prima di collegarne un altro.
> - FSx File Gateway supporta le quote di storage software (che avvisano l'utente quando gli utenti superano i limiti di dati), ma non supporta le quote rigide (che impongono i limiti dei dati negando l'accesso in scrittura). Le quote soft sono supportate per tutti gli utenti tranne l'utente FSx amministratore di Amazon. Per ulteriori informazioni sull'impostazione delle quote di archiviazione, consulta la sezione Quote di archiviazione nella Amazon FSx User Guide.
> - Non consigliamo di utilizzare Microsoft Distributed File System (DFS) per reindirizzare gli utenti al tuo file system Amazon tramite FSx FSx File Gateway. Invece, configura DFS per il reindirizzamento diretto al FSx file system Amazon Cloud AWS come descritto in Raggruppamento di più file system con DFS Namespaces nella FSx Amazon for Windows File Server User Guide.

Per allegare un FSx file system Amazon

1. Nella console Storage Gateway, nella pagina FSx File system > Allega FSx file system, completare i seguenti campi nella sezione delle impostazioni del FSx file system:

   - Per FSx il nome del file system, selezionare il file system da allegare dall'elenco a discesa.
   - Per l'indirizzo IP dell'endpoint locale, inserisci l'indirizzo IP del gateway che i client utilizzeranno per sfogliare le condivisioni di file sul FSx file system.

   > **Note**
   >
   > - È necessario specificare un indirizzo IP per ogni file system collegato al gateway.
   > - Per i EC2 gateway Amazon, puoi specificare l'indirizzo IP privato dell' EC2 istanza, a meno che non sia già utilizzato da un file system diverso, nel qual caso devi aggiungere un nuovo indirizzo privato al gateway, quindi riavviarlo. Per ulteriori informazioni, consulta Indirizzi IP multipli nella Amazon EC2 User Guide.
   > - Per i gateway locali, puoi specificare l'indirizzo IP dell'interfaccia di rete principale (statica o DHCP), a meno che non sia già utilizzata da un file system diverso, nel qual caso devi fornire un indirizzo IP diverso dalla stessa sottorete dell'interfaccia principale, che sarà resa disponibile come IP virtuale. Non utilizzare un indirizzo IP assegnato a un'interfaccia di rete diversa da quella principale.

2. Nella sezione Impostazioni dell'account di servizio, fornisci le credenziali di accesso dell'account di servizio associate al FSx file system Amazon.

   > **Note**
   >
   > Questo account di servizio deve disporre dei privilegi di Operatore di Backup del servizio Active Directory associato ai tuoi FSx file system Amazon o avere autorizzazioni equivalenti.

   > **Important**
   >
   > Per garantire autorizzazioni sufficienti per file, cartelle e metadati dei file, ti consigliamo di rendere l'account del servizio un membro del gruppo degli amministratori del file system.

Se utilizzi AWS Directory Service Microsoft Active Directory con Amazon FSx for Windows File Server, l'account del servizio deve essere un membro del gruppo AWS Delegated FSx Administrators.
Se utilizzi un Active Directory autogestito con Amazon FSx for Windows File Server, ti consigliamo che l'account di servizio sia un membro del gruppo di amministratori di file system delegati personalizzati che hai specificato per l'amministrazione del file system quando hai creato il tuo file system Amazon FSx .
Se hai scelto di non creare un gruppo di amministratori di file system delegati personalizzato quando hai creato il FSx filesystem Amazon, il gruppo predefinito è Domain Admins. Sebbene sia possibile invece rendere l'account di servizio un membro di questo gruppo, questa procedura non è consigliata come best practice.
Per ulteriori informazioni, consulta la sezione Delegare i privilegi al tuo account di FSx servizio Amazon nella Guida per l'utente di Amazon FSx for Windows File Server.

3. Nella sezione Registri di controllo, scegli Gruppi di log esistenti e scegli il log che desideri utilizzare per monitorare l'accesso al tuo FSx file system Amazon. Puoi crearne uno nuovo. Se non vuoi monitorare il tuo sistema, scegli Disabilita registrazione.
4. Per l'impostazione di aggiornamento automatico della cache, se desideri che la cache si aggiorni automaticamente, scegli Imposta intervallo di aggiornamento e specifica un intervallo compreso tra 5 minuti e 30 giorni.
5. (Facoltativo) Nella sezione Tag, scegli Aggiungi nuovo tag per aggiungere una o più chiavi e un valore per etichettare le impostazioni.
6. Selezionare Next (Successivo) e rivedere le impostazioni. Per modificare le impostazioni, puoi scegliere Modifica in ogni sezione.
7. Al termine, seleziona Finish (Fine).

Approfondimenti

Monta e usa la tua condivisione di FSx file Amazon

Monta e usa la tua condivisione di FSx file Amazon

Prima di montare la condivisione di file sul client, attendi che lo stato del FSx file system Amazon passi a Disponibile. Dopo aver montato la condivisione di file, puoi iniziare a utilizzare Amazon FSx File Gateway (FSx File Gateway).

Argomenti

Installa la tua condivisione di file SMB sul tuo client

In questo passaggio, monti la condivisione di file SMB e la mappi su un'unità accessibile al tuo client. La sezione File Gateway della console mostra i comandi di montaggio supportati che è possibile utilizzare per i client SMB. Di seguito sono riportate alcune opzioni aggiuntive da provare.

Esistono più metodi per montare una condivisione file SMB, tra cui i seguenti:

- Il `net use` comando: non persiste dopo i riavvii del sistema, a meno che non si utilizzi lo `/persistent:(yes:no)` switch.
- L'utilità da riga di `CmdKey` comando: crea una connessione permanente a una condivisione di file SMB montata che rimane dopo il riavvio.
- Un'unità di rete mappata in File Explorer: configura la condivisione di file montata per riconnettersi all'accesso e per richiedere l'immissione delle credenziali di rete.
- PowerShell script — Può essere persistente e può essere visibile o invisibile al sistema operativo durante il montaggio.

> **Note**
>
> Se sei un utente di Microsoft Active Directory, contatta il tuo amministratore per assicurarti di avere accesso alla condivisione di file SMB prima di installarla sul tuo sistema locale. Amazon FSx File Gateway non supporta il blocco SMB o gli attributi estesi SMB.

Per montare una condivisione di file SMB per gli utenti di Active Directory utilizzando il comando net use

1. Accertarsi di avere accesso alla condivisione file SMB prima di montarla sul sistema locale.
2. Per i client Microsoft Active Directory, immettere il seguente comando al prompt dei comandi:

   ```
   net use [WindowsDriveLetter]: \\[Gateway IP Address]\[Name of the share on the FSx file system]
   ```

Per montare una condivisione di file SMB su Windows utilizzando CmdKey

1. Premi il tasto Windows e invio **cmd** per visualizzare la voce del menu del prompt dei comandi.
2. Apri il menu contestuale (fai clic con il pulsante destro del mouse) per il prompt dei comandi e scegli Esegui come amministratore.
3. Immetti il comando seguente:

   ```
   C:\>cmdkey /add:[Gateway VM IP address] /user:[DomainName]\[UserName] /pass:[Password]
   ```

> **Note**
>
> Quando monti delle condivisioni di file, potresti dover rimontare la condivisione di file dopo aver riavviato il client.

Montaggio di una condivisione file SMB con Esplora file di Windows

1. Premi il tasto Windows e inserisci **File Explorer** nella casella Cerca in Windows, oppure premi. **Win+E**
2. Nel riquadro di navigazione, scegli Questo PC. Quindi, nella scheda Computer, scegli Map network drive.
3. Nella finestra di dialogo Mappa unità di rete, scegli una lettera di unità per Drive.
4. Per Cartella**\\[File Gateway IP]\[SMB File Share Name]**, inserisci o scegli Sfoglia per selezionare la condivisione di file SMB dalla finestra di dialogo.
5. (Facoltativo) Selezionare Riconnetti all'accesso se si desidera che il punto di montaggio persista anche dopo un riavvio.

6. (Facoltativo) Seleziona Connetti utilizzando credenziali diverse se desideri che un utente inserisca la password di accesso ad Active Directory o l'account ospite.
7. Scegliere Fine per completare il punto di montaggio.

Metti alla prova il tuo FSx File Gateway

Puoi copiare file e directory sull'unità mappata. I file vengono caricati automaticamente nel file system FSx per Windows File Server.

Per caricare file dal tuo client Windows su Amazon FSx

1. Sul client Windows, accedi all'unità su cui hai montato il file system. Il nome dell'unità è preceduto dal nome del file system.
2. Copia i file o una directory sull'unità.

> **Note**
>
> I File Gateway non supportano la creazione di link fissi o simbolici su una condivisione di file.

Gestione delle risorse di Amazon FSx File Gateway

Le seguenti sezioni forniscono informazioni su come gestire le risorse di Amazon FSx File Gateway (FSx File Gateway), tra cui collegare e scollegare i FSx file system Amazon e configurare le impostazioni di Microsoft Active Directory.

Argomenti

Comprendere lo stato del gateway

A ogni gateway nell'implementazione AWS di Storage Gateway è associato uno stato che indica a colpo d'occhio lo stato del gateway. Nella maggior parte dei casi, lo stato indica che il gateway funziona normalmente e che non è necessaria alcuna azione da parte dell'utente. In alcuni casi, lo stato indica un problema che potrebbe richiedere un'operazione da parte tua.

È possibile visualizzare lo stato di ogni gateway nella distribuzione nella pagina Gateway della console Storage Gateway. Lo stato del gateway viene visualizzato nella colonna Stato accanto al nome del gateway. Un gateway che funziona normalmente ha lo stato di`RUNNING`.

Nella tabella seguente, è possibile trovare una descrizione dello stato di ogni gateway e l'opportunità di agire in base allo stato. Un gateway deve avere `RUNNING` lo stato per tutto o per la maggior parte del tempo in cui è in uso.

Status	Significato
`RUNNING`	Il gateway è configurato correttamente ed è disponibile per l'uso.

Status	Significato
`OFFLINE`	Il gateway potrebbe essere in uno `OFFLINE` stato attivo per uno o più dei seguenti motivi: • Il gateway non può raggiungere gli endpoint del servizio Storage Gateway. • Il gateway ha avuto un arresto imprevisto. • Al gateway è associato un disco di cache che è disconnesso, è stato modificato o ha avuto un errore.

Comprendere lo stato del file system

È possibile visualizzare lo stato di salute di un file system a colpo d'occhio esaminandone lo stato. Se lo stato indica che il file system funziona normalmente, non è necessaria alcuna azione da parte dell'utente. Se lo stato indica che c'è un problema, puoi indagare per determinare se è necessario intervenire.

È possibile visualizzare lo stato di un file system sulla console Storage Gateway nella colonna Status. Un file system che funziona correttamente mostra lo stato AVAILABLE. Questo dovrebbe essere lo stato per la maggior parte del tempo.

La tabella seguente descrive gli stati delle condivisioni di file, il loro significato e se potrebbe essere necessaria un'azione.

Status	Significato
DISPONIBILE	Il file system è configurato correttamente ed è disponibile per l'uso. Questo è lo stato standard per un file system che funziona correttam ente.
CREAZIONE IN CORSO	Il file system non è ancora stato creato completamente e non è pronto per l'uso. Lo stato CREATING (CREAZIONE IN CORSO) è transitorio. Nessuna operazione richiesta. Se il file system rimane bloccato in questo stato, probabilmente è perché la VM gateway ha perso la connessione a AWS.

Status	Significato
AGGIORNAMENTO IN CORSO	La configurazione del file system è attualmente in fase di aggiornam ento. Lo stato UPDATING è transitorio. Nessuna operazione richiesta. Se un file system si blocca in questo stato, probabilmente è perché la VM gateway ha perso la connessione a. AWS
ELIMINAZIONE IN CORSO	Il file system viene eliminato. Il file system non viene eliminato finché tutti i dati non vengono caricati su AWS. Lo stato DELETING (ELIMINAZ IONE IN CORSO) è transitorio e non è richiesta alcuna operazione.
FORCE_DEL ETING (ELIMINAZ IONE_FORZATA)	Il file system viene eliminato con la forza. Il file system viene eliminato immediatamente e i dati non vengono caricati su. AWS Lo stato FORCE_DELETING (ELIMINAZIONE_FORZATA) è transitorio e non è richiesta alcuna operazione.
ERRORE	Lo stato del file system non è integro. È richiesta un'azione. Alcune possibili cause includono problemi con le credenziali o i privilegi di accesso, problemi di connettività o spazio di archiviazione insufficiente sul file system. Quando il problema che ha causato lo stato non integro viene risolto, il file system torna allo stato AVAILABLE.

Modifica le informazioni di base per un FSx File Gateway

È possibile utilizzare la console Storage Gateway per modificare le informazioni di base per un gateway esistente, tra cui il nome del gateway, il fuso orario e il gruppo di CloudWatch log.

Per modificare le informazioni di base per un gateway esistente

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le informazioni di base.
3. Dal menu a discesa Operazioni, scegli Modifica le informazioni sul gateway.
4. Per Gateway name (Nome gateway), inserire un nome per il gateway. È possibile cercare questo nome per trovare il gateway nelle pagine di elenco della console Storage Gateway.

> **Note**
>
> I nomi dei gateway devono contenere tra 2 e 255 caratteri e non possono includere una barra (\o/).
> La modifica del nome di un gateway disconnetterà tutti gli CloudWatch allarmi impostati per monitorare il gateway. Per ricollegare gli allarmi, aggiorna il file GatewayNameper ogni allarme nella console. CloudWatch

5. Per il Fuso orario del gateway, scegli il fuso orario locale per la parte del mondo in cui desideri implementare il gateway.
6. Per Scegli come configurare un gruppo di log, scegli come configurare Amazon CloudWatch Logs per monitorare lo stato del tuo gateway. Scegliere tra le seguenti opzioni:
   - Crea un nuovo gruppo di log: configura un nuovo gruppo di log per monitorare il tuo gateway.
   - Usa un gruppo di log esistente: scegli un gruppo di log esistente dall'elenco a discesa corrispondente.
   - Disattiva la registrazione: non utilizzare Amazon CloudWatch Logs per monitorare il gateway.
7. Quando hai finito di modificare le impostazioni che desideri modificare, scegli Salva modifiche.

Imposta un livello di sicurezza per il tuo gateway

È possibile configurare il livello di sicurezza SMB per il FSx File Gateway per specificare se il gateway deve richiedere la firma Server Message Block (SMB) o la crittografia SMB.

Per configurare il livello di sicurezza

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le impostazioni SMB.
3. Dal menu a discesa Azioni, scegli Modifica impostazioni SMB, quindi scegli Impostazioni di sicurezza SMB.
4. Per Security level (Livello di sicurezza), selezionare una delle opzioni seguenti:

> **Note**
>
> Per informazioni sulla configurazione di questa impostazione utilizzando l' AWS API, consulta Update SMBSecurity Strategy nel riferimento API.Gateway di archiviazione AWS
> Un livello di sicurezza più elevato può influire sulle prestazioni del gateway.

- Crittografia obbligatoria: se si sceglie questa opzione, FSx File Gateway consente solo connessioni da SMBv3 client che utilizzano algoritmi di crittografia AES a 256 bit. Gli algoritmi a 128 bit non sono consentiti. Questa opzione è consigliata per ambienti che gestiscono dati sensibili. Funziona con client SMB su Microsoft Windows 8, Windows Server 2012 o versioni successive.
- Applica la crittografia: se scegli questa opzione, FSx File Gateway consente solo le connessioni da SMBv3 client con crittografia attivata. Sono consentiti sia algoritmi a 256 bit che a 128 bit. Questa opzione è consigliata per ambienti che gestiscono dati sensibili. Funziona con client SMB su Microsoft Windows 8, Windows Server 2012 o versioni successive.
- Applica la firma: se scegli questa opzione, FSx File Gateway consente solo le connessioni da SMBv2 o SMBv3 i client che hanno la firma attivata. Questa opzione funziona con i client SMB su Microsoft Windows Vista, Windows Server 2008 o versioni successive.

> **Note**
>
> Il livello di sicurezza predefinito per FSx File Gateway è Enforce encryption.

5. Scegli Save (Salva).

Modifica delle impostazioni di Active Directory per n FSx File Gateway

Per utilizzare il tuo Microsoft Active Directory aziendale o AWS Managed Microsoft AD per l'accesso autenticato dall'utente al tuo FSx file system Amazon, modifica le impostazioni SMB per il gateway e

fornisci le credenziali del dominio Active Directory. In questo modo, il gateway può entrare a far parte del dominio Active Directory e i membri del dominio possono accedere al file system.

> **Note**
>
> Utilizzando Directory Service, è possibile creare un servizio di dominio Active Directory ospitato in Cloud AWS.
> Per utilizzarla AWS Managed Microsoft AD con un gateway Amazon EC2, devi creare l'istanza Amazon EC2 nello stesso VPC di, aggiungere il gruppo di sicurezza AWS Managed Microsoft AD_WorkspaceMembers all'istanza Amazon EC2 e unirti al dominio AD utilizzando le credenziali di amministratore di. AWS Managed Microsoft AD
> Per ulteriori informazioni in merito, consulta la Guida all'amministrazione. AWS Managed Microsoft ADAWS Directory Service
> Per ulteriori informazioni su Amazon EC2, consulta la documentazione di Amazon Elastic Compute Cloud.

Per attivare l'autenticazione Active Directory

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli Gateway, quindi scegli il gateway per il quale desideri modificare le impostazioni SMB.
3. Dal menu a discesa Azioni, scegli Modifica impostazioni SMB, quindi scegli Impostazioni Active Directory.
4. Per Nome di dominio, inserisci il nome del dominio Active Directory a cui desideri che il gateway si unisca.

   > **Note**
   >
   > Active Directory status (Stato di Active Directory) mostra la voce Detached (Scollegato) quando un gateway non è mai entrato a far parte di un dominio.
   > L'account del servizio Active Directory deve disporre delle autorizzazioni necessarie. Per ulteriori informazioni, vedere Requisiti di account del servizio Active Directory.
   > L'aggiunta a un dominio crea un account computer Active Directory nel contenitore predefinito dei computer (che non è un'unità organizzativa), utilizzando l'ID Gateway del gateway come nome dell'account (ad esempio, SGW-1234ADE). Non è possibile personalizzare il nome di questo account.

Se l'ambiente Active Directory richiede la preconfigurazione degli account per facilitare il processo di aggiunta al dominio, sarà necessario creare questo account in anticipo.
Se l'ambiente Active Directory dispone di un'unità organizzativa designata per i nuovi oggetti del computer, è necessario specificare tale unità organizzativa al momento dell'accesso al dominio.
Se il gateway non può accedere a una directory di Active Directory, prova a connetterti con l'indirizzo IP della directory utilizzando l'operazione JoinDomainAPI.

5. Per Utente di dominio e Password di dominio, inserisci le credenziali per l'account del servizio Active Directory che il gateway utilizzerà per aggiungere il dominio.
6. (Facoltativo) Per Unità organizzativa (OU), immettere l'unità organizzativa designata utilizzata da Active Directory per i nuovi oggetti del computer.
7. (Facoltativo) Per i controller di dominio (DC), immettete il nome di uno o più DCs tramite i quali il gateway si connetterà ad Active Directory. È possibile immetterne più di uno DCs come elenco separato da virgole. Puoi lasciare vuoto questo campo per consentire al DNS di selezionare automaticamente un DC.
8. Scegli Save changes (Salva modifiche).

Modifica delle impostazioni per un FSx file system Amazon

Dopo aver creato un file system Amazon FSx for Windows File Server, puoi modificare le impostazioni per CloudWatch i log, l'aggiornamento automatico della cache e le credenziali dell'account di FSx servizio Amazon.

Per modificare le impostazioni FSx del file system Amazon

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel pannello di navigazione, scegli File system e scegli il file system di cui desideri modificare le impostazioni.
3. Per Azioni, scegli Modifica impostazioni del file system.
4. Nella sezione delle impostazioni del file system, verifica le informazioni sul gateway, FSx sulla posizione Amazon e sull'indirizzo IP.

> **Note**
>
> Non è possibile modificare l'indirizzo IP di un file system dopo averlo collegato a un gateway. Per modificare l'indirizzo IP, è necessario scollegare e ricollegare il file system.

5. Nella sezione Audit logs, scegli un'opzione per utilizzare i gruppi di CloudWatch log per monitorare l'accesso ai FSx file system di Amazon. Puoi utilizzare un gruppo di log esistente.
6. Per le impostazioni di aggiornamento automatico della cache, scegli un'opzione. Se scegli Imposta intervallo di aggiornamento, imposta l'ora in giorni, ore e minuti per aggiornare la cache del file system utilizzando Time To Live (TTL).

   TTL è il periodo di tempo trascorso dall'ultimo aggiornamento. Quando si accede alla directory dopo tale periodo di tempo, File Gateway aggiorna il contenuto della directory dal FSx file system Amazon.

   > **Note**
   >
   > I valori degli intervalli di aggiornamento validi sono compresi tra 5 minuti e 30 giorni.

7. Nella sezione Impostazioni dell'account di servizio, facoltativa, inserisci un nome utente e una password. Queste credenziali sono per un utente con il ruolo di Amministratore di Backup del servizio Active Directory associato ai tuoi FSx file system Amazon.
8. Scegli Save changes (Salva modifiche).

Scollegare un FSx file system Amazon

Lo scollegamento di un file system non comporta l'eliminazione dei dati in FSx Windows File Server. I dati scritti su questi file system prima di scollegarli verranno comunque caricati sul file server FSx per Windows.

Per scollegare un FSx file system Amazon

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegli i FSx file system, quindi seleziona uno o più file system da scollegare.
3. Per Azioni, scegli Scollega il file system. Viene visualizzata la finestra di dialogo di conferma.

4. Verifica di voler scollegare i file system specificati, quindi digita la parola distacca nella casella di conferma e scegli Scollega.

Monitoraggio di Storage Gateway

Gli argomenti di questa sezione descrivono come monitorare un gateway utilizzando Amazon CloudWatch, incluso il monitoraggio dello storage della cache e di altre risorse associate al gateway. È possibile utilizzare la console Storage Gateway per visualizzare i parametri e gli allarmi per il gateway. Ad esempio, puoi visualizzare il numero di byte utilizzati nelle operazioni di lettura e scrittura, il tempo impiegato nelle operazioni di lettura e scrittura e il tempo impiegato per recuperare i dati dal cloud. AWS I parametri consentono di monitorare l'integrità del gateway e di impostare allarmi di notifica quando uno o più parametri sono al di fuori di una soglia definita.

Storage Gateway fornisce CloudWatch metriche senza costi aggiuntivi. I parametri Storage Gateway sono registrati per un periodo di due settimane. Utilizzando queste metriche, è possibile accedere alle informazioni storiche e avere una prospettiva migliore sulle prestazioni dei gateway. Storage Gateway fornisce anche CloudWatch allarmi, ad eccezione degli allarmi ad alta risoluzione, senza costi aggiuntivi. Per ulteriori informazioni sui CloudWatch prezzi, consulta la pagina CloudWatch dei prezzi di Amazon. Per ulteriori informazioni CloudWatch, consulta la Amazon CloudWatch User Guide.

Argomenti

- CloudWatch Comprensione degli allarmi- Scopri le informazioni di base sugli CloudWatch allarmi, inclusi gli stati degli allarmi e le configurazioni consigliate.
- Crea allarmi consigliati CloudWatch - Scopri come configurare in modo rapido e automatico tutti gli CloudWatch allarmi consigliati come parte del processo di configurazione iniziale di File Gateway.
- Crea un CloudWatch allarme personalizzato- Scopri come creare un CloudWatch allarme personalizzato per monitorare una metrica specifica utilizzando criteri di valutazione specifici per attivare gli stati di allarme e inviare notifiche.
- Monitoraggio di FSx- Scopri come visualizzare CloudWatch i log e i log di controllo e trova informazioni sullo specifico gateway e sulle metriche del file system di condivisione file riportate dal gateway.

CloudWatch Comprensione degli allarmi

CloudWatch gli allarmi monitorano le informazioni sul gateway in base a metriche ed espressioni. È possibile aggiungere CloudWatch allarmi per il gateway e visualizzarne lo stato nella console

Storage Gateway. Per ulteriori informazioni sulle metriche utilizzate per monitorare . Per ogni allarme, si specificano le condizioni che attiveranno lo stato ALARM. Gli indicatori di stato degli allarmi nella console Storage Gateway diventano rossi quando si trova nello stato ALLARME, semplificando il monitoraggio dello stato in modo proattivo. È possibile configurare gli allarmi per richiamare automaticamente le azioni in base a cambiamenti di stato sostenuti. Per ulteriori informazioni sugli CloudWatch allarmi, consulta Using Amazon CloudWatch alarms nella Amazon CloudWatch User Guide.

> **Note**
>
> Se non disponi dell'autorizzazione per la visualizzazione CloudWatch, non puoi visualizzare gli allarmi.

Per ogni gateway attivato, si consiglia di creare i seguenti allarmi CloudWatch:

- Attesa I/O elevata: `IoWaitpercent` >= 20 per 3 antidatato in 15 minuti
- Percentuale di cache dirty: `CachePercentDirty` > 80 per 4 datapoint entro 20 minuti
- File non caricati: `FilesFailingUpload` >= 1 per 1 datapoint entro 5 minuti
- Errore del file system: `FileSystem-ERROR` >= 1 per 1 datapoint entro 5 minuti
- Notifiche Health: `HealthNotifications` >= 1 per 1 datapoint entro 5 minuti. Quando configuri questo allarme, imposta Trattamento dei dati mancanti su notBreaching.

> **Note**
>
> È possibile impostare un avviso di notifica di stato solo se il gateway aveva una precedente notifica di stato in CloudWatch.

Per i gateway su piattaforme VMware host che fanno parte di un cluster VMware ad alta disponibilità, consigliamo anche questo allarme aggiuntivo: CloudWatch

- Notifiche di disponibilità: `AvailabilityNotifications` >= 1 per 1 datapoint entro 5 minuti. Quando configuri questo allarme, imposta Trattamento dei dati mancanti su notBreaching.

La tabella seguente descrive gli stati di allarme. CloudWatch

Stato	Description
OK	Il parametro o espressione rientra nella soglia definita.
Allarme	Il parametro o espressione non rientra nella soglia definita.
Dati insufficienti	L'allarme è stato appena attivato, il parametro non è disponibile o la quantità di dati non è sufficiente affinché il parametro determini lo stato dell'allarme.
Nessuno	Non vengono creati allarmi per il gateway. Per creare un nuovo avviso, vedere Crea un CloudWatch allarme personalizzato per il tuo gateway.
Non disponibile	Lo stato dell'allarme è sconosciuto. Scegliere Unavailable (Non disponibile) per visualizz are le informazioni sugli errori nella scheda Monitoring (Monitoraggio) .

Creazione di CloudWatch allarmi consigliati per il gateway

Quando si crea un nuovo gateway utilizzando la console Storage Gateway, è possibile scegliere di creare automaticamente tutti gli CloudWatch allarmi consigliati come parte del processo di configurazione iniziale. Per ulteriori informazioni, consulta . Se desideri aggiungere o aggiornare gli CloudWatch allarmi consigliati per un gateway esistente dopo aver già completato la prima configurazione, usa la seguente procedura.

Per aggiungere o aggiornare gli CloudWatch allarmi consigliati per un gateway esistente

> **Note**
>
> Questa funzionalità richiede le autorizzazioni relative alle CloudWatch policy, che non vengono concesse automaticamente come parte della policy di accesso completo

preconfigurata di Storage Gateway. Assicurati che la tua politica di sicurezza conceda le seguenti autorizzazioni prima di tentare di creare allarmi consigliati: CloudWatch

- `cloudwatch:PutMetricAlarm`: creazione di allarmi
- `cloudwatch:DisableAlarmActions`: disattivazione delle azioni di allarme
- `cloudwatch:EnableAlarmActions`: attivazione delle azioni di allarme
- `cloudwatch:DeleteAlarms`: eliminazione di allarmi

1. Aprire la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa/.
2. Nel riquadro di navigazione sul lato sinistro della pagina, scegli Gateway, quindi scegli il gateway per il quale desideri creare gli allarmi consigliati CloudWatch .
3. Nella pagina Dettagli del gateway, scegli la scheda Monitoraggio.
4. In Allarmi, scegli Crea allarmi consigliati. Gli allarmi consigliati vengono creati automaticamente.

   La sezione Allarmi elenca tutti gli CloudWatch allarmi per un gateway specifico. Da qui, puoi selezionare ed eliminare uno o più allarmi, attivare o disattivare le azioni di allarme e creare nuovi allarmi.

Crea un CloudWatch allarme personalizzato per il tuo gateway

CloudWatch utilizza Amazon Simple Notification Service (Amazon SNS) per inviare notifiche di allarme quando un 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 Amazon SNS. Puoi creare un argomento Amazon SNS quando crei un CloudWatch allarme. Per ulteriori informazioni su Amazon SNS, consulta Che cos'è Amazon SNS? nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Per creare un CloudWatch allarme nella console Storage Gateway

1. Aprire la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa/.
2. Nel pannello di navigazione scegliere Gateway, quindi scegliere il gateway per cui si desidera creare un allarme.
3. Nella pagina dei dettagli del gateway, scegliere la scheda Monitoraggio.
4. In Allarmi, scegli Crea allarme per aprire la CloudWatch console.

5. Usa la CloudWatch console per creare il tipo di allarme che desideri. Puoi creare i seguenti tipi di allarmi:

   - Allarme di soglia statica: un allarme basato su una soglia impostata per un parametro scelto. L'allarme entra nello stato ALARM quando la metrica supera la soglia per un determinato numero di periodi di valutazione.

     Per creare un allarme con soglia statica, consulta Creazione di un CloudWatch allarme basato su una soglia statica nella Amazon CloudWatch User Guide.

   - Allarme di rilevamento delle anomalie: il rilevamento delle anomalie recupera i dati dei parametri nel tempo e crea un modello di valori previsti. Imposta un valore per la soglia di rilevamento delle anomalie e CloudWatch utilizza questa soglia con il modello per determinare l'intervallo di valori «normale» per la metrica. Un valore più alto per la soglia produce un intervallo più ampio di valori "normali". Puoi decidere se l'allarme viene attivato solo quando il valore del parametro è al di sopra dell'intervallo di valori previsti, solo se si trova al di sotto di tale intervallo oppure è sopra o sotto l'intervallo.

     Per creare un allarme di rilevamento delle anomalie, consulta Creazione di un CloudWatch allarme basato sul rilevamento delle anomalie nella Amazon CloudWatch User Guide.

   - Allarme di espressione matematica del parametro: un allarme basato su uno o più parametri utilizzati in un'espressione matematica. Si specificano l'espressione, la soglia e i periodi di valutazione.

     Per creare un allarme con espressione matematica metrica, consulta Creazione di un CloudWatch allarme basato su un'espressione matematica metrica nella Amazon User Guide. CloudWatch

   - Allarme composito: un allarme che determina il suo stato di allarme osservando gli stati di allarme di altri allarmi. Un allarme composito può aiutare a ridurre il rumore di allarme.

     Per creare un allarme composito, consulta Creazione di un allarme composito nella Amazon CloudWatch User Guide.

6. Dopo aver creato l'allarme nella CloudWatch console, tornare alla console Storage Gateway. È possibile visualizzare l'allarme effettuando una delle seguenti operazioni:

   - Nel pannello di navigazione scegliere Gateway, quindi scegliere il gateway per cui si desidera visualizzare gli allarmi. Nella scheda Dettagli, in Allarmi, scegli CloudWatch Allarmi.

- Nel pannello di navigazione scegliere Gateway, quindi scegliere il gateway per cui si desidera visualizzare gli allarmi e quindi scegliere la scheda Monitoraggio.

  La sezione Allarmi elenca tutti gli CloudWatch allarmi per un gateway specifico. Da qui, puoi selezionare ed eliminare uno o più allarmi, attivare o disattivare le azioni di allarme e creare nuovi allarmi.
- Nel pannello di navigazione scegliere Gateway, quindi scegliere lo stato di allarme del gateway per cui si desidera visualizzare gli allarmi.

Per informazioni su come modificare o eliminare un avviso, consulta Modificare o eliminare un avviso. CloudWatch

> **Note**
>
> Quando si elimina un gateway utilizzando la console Storage Gateway, vengono eliminati automaticamente anche tutti gli CloudWatch allarmi associati al gateway.

Monitoraggio di FSx

Puoi monitorare il tuo e le risorse associate Gateway di archiviazione AWS utilizzando i CloudWatch parametri e i log di controllo di Amazon. Puoi anche utilizzare CloudWatch Events per ricevere notifiche quando le operazioni sui file sono terminate.

Argomenti

- Ottenere i registri di integrità di File Gateway con CloudWatch gruppi di log
- Utilizzo dei CloudWatch parametri di Amazon
- Comprendere i parametri del gateway
- Comprensione delle metriche del file system
- Informazioni sui log di FSx

Ottenere i registri di integrità di File Gateway con CloudWatch gruppi di log

Puoi utilizzare Amazon CloudWatch Logs per ottenere informazioni sullo stato di salute del tuo e delle risorse correlate. Puoi utilizzare i log per monitorare il gateway alla ricerca di eventuali errori. Inoltre,

puoi utilizzare i filtri di CloudWatch abbonamento Amazon per automatizzare l'elaborazione delle informazioni di registro in tempo reale. Per ulteriori informazioni, consulta Elaborazione in tempo reale dei dati di registro con abbonamenti nella Amazon CloudWatch User Guide.

Ad esempio, puoi configurare un gruppo di CloudWatch log per monitorare il gateway e ricevere una notifica quando FSx File Gateway non riesce a caricare file su un FSx file system Amazon. Puoi configurare il gruppo quando attivi il gateway o dopo che il gateway è stato attivato e funzionante. Per informazioni su come configurare un gruppo di log CloudWatch durante l'attivazione di un gateway, consulta Configura il tuo Amazon FSx File Gateway. Per informazioni generali sui gruppi di CloudWatch log, consulta Working with Log Groups and Log Streams nella Amazon CloudWatch User Guide.

Per informazioni su come risolvere gli errori che possono essere segnalati da , vedere. Risoluzione dei problemi: problemi relativi a File Gateway

Configurazione di un gruppo di CloudWatch log dopo l'attivazione del gateway

La procedura seguente mostra come configurare un gruppo di CloudWatch log dopo l'attivazione del gateway.

Per configurare un gruppo di CloudWatch log in modo che funzioni con

1. Accedi Console di gestione AWS e apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel riquadro di navigazione, scegli Gateway, quindi scegli il gateway per cui desideri configurare il gruppo di CloudWatch log.
3. Per Azioni, scegli Modifica le informazioni sul gateway.
4. Per Scegli come configurare il gruppo di log, scegli una delle seguenti opzioni:
   - Crea un nuovo gruppo di log per creare un nuovo gruppo di CloudWatch log.
   - Utilizza un gruppo di log esistente per utilizzare un gruppo di CloudWatch log già esistente.

     Scegli un gruppo di log dall'elenco dei gruppi di log esistenti.
   - Disattiva la registrazione se non desideri monitorare il gateway utilizzando i gruppi di CloudWatch log.
5. Scegli Save changes (Salva modifiche).
6. Per visualizzare i log sullo stato del gateway, procedi come indicato di seguito:

1. Nel riquadro di navigazione, scegli Gateway, quindi scegli il gateway per cui hai configurato il gruppo di CloudWatch log.
2. Scegli la scheda Dettagli e, in Health logs, scegli CloudWatchLogs. La pagina dei dettagli del gruppo di log si apre nella CloudWatch console.

Utilizzo dei CloudWatch parametri di Amazon

Puoi ottenere i dati di monitoraggio per il tuo File Gateway utilizzando Console di gestione AWS o l' CloudWatch API. La console mostra una serie di grafici basati sui dati grezzi dell' CloudWatch API. L' CloudWatch API può essere utilizzata anche tramite uno dei AWS SDKsnostri strumenti CloudWatch API di Amazon. In base alle tue esigenze, potresti decidere di utilizzare i grafici visualizzati nella console o quelli recuperati dall'API.

Indipendentemente dal metodo utilizzato per lavorare con le metriche, devi specificare le seguenti informazioni:

- Dimensione del parametro da usare. Una dimensione è una coppia nome-valore che consente di identificare una metrica in modo univoco. Le dimensioni di Storage Gateway sono `GatewayId` e `GatewayName`. Nella CloudWatch console, puoi utilizzare la `Gateway Metrics` vista per selezionare dimensioni specifiche del gateway. Per ulteriori informazioni sulle dimensioni, consulta Dimensions nella Amazon CloudWatch User Guide.
- Il nome del parametro, ad esempio `ReadBytes`.

La tabella seguente contiene un riepilogo dei tipi di dati dei parametri di Storage Gateway disponibili.

Spazio dei CloudWatch nomi Amazon	Dimensione	Description
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	Queste dimensioni filtrano in base ai dati dei parametri che descrivono gli aspetti del gateway. Puoi identificare un con cui lavorare specificando sia le dimensioni che le `GatewayId` dimensioni. `GatewayName` I dati di throughput e latenza di un gateway si basano su tutte le condivisioni file nel gateway.

Spazio dei CloudWatch nomi Amazon	Dimensione	Description
		I dati sono disponibili gratuitamente e automaticamente in intervalli di 5 minuti.

L'uso di parametri di gateway e file è simile all'uso di altri parametri del servizio. Puoi trovare una presentazione delle attività dei parametri più comuni nella documentazione di CloudWatch elencata di seguito:

- Visualizzazione delle metriche disponibili
- Ottenere statistiche per una metrica
- Creazione di allarmi CloudWatch

Comprendere i parametri del gateway

La tabella seguente descrive le metriche che riguardano FSx i File Gateway. A ogni gateway è associata una serie di metriche. Alcune metriche specifiche del gateway hanno lo stesso nome di alcune metriche. file-system-specific Queste metriche rappresentano gli stessi tipi di misurazioni, ma si riferiscono al gateway anziché al file system.

Specificate sempre se desiderate lavorare con un gateway o un file system quando lavorate con una metrica particolare. In particolare, quando si lavora con le metriche del gateway, è necessario specificare le metriche `Gateway Name` per il gateway di cui si desidera visualizzare i dati metrici. Per ulteriori informazioni, consulta Utilizzo dei CloudWatch parametri di Amazon.

> **Note**
>
> Alcuni parametri restituiscono punti dati solo quando sono stati generati nuovi dati durante il periodo di monitoraggio più recente.

La tabella seguente descrive le metriche che è possibile utilizzare per ottenere informazioni su FSx s.

Metrica	Description
`AvailabilityNotifications`	Questa metrica riporta il numero di notifiche sanitarie relative alla disponibilità generate dal gateway nel periodo di riferimento. Unità: numero
`CacheDirectorySize`	Questa metrica tiene traccia della dimension e delle cartelle nella cache del gateway. La dimensione della cartella è determinata dal numero di file e sottocartelle presenti nel primo livello e non viene conteggiata in modo ricorsivo nelle sottocartelle. Utilizza questa metrica con la `Average` statistic a per misurare la dimensione media di una cartella nella cache del gateway. Utilizza questa metrica con la `Max` statistica per misurare la dimensione massima di una cartella nella cache del gateway. Unità: numero
`CacheFileSize`	Questa metrica tiene traccia della dimensione dei file nella cache del gateway. Utilizza questa metrica con la `Average` statistic a per misurare la dimensione media di un file nella cache del gateway. Utilizza questa metrica con la `Max` statistica per misurare la dimensione massima di un file nella cache del gateway. Unità: byte
`CacheFree`	Questa metrica riporta il numero di byte disponibili nella cache del gateway.

Metrica	Description
	Unità: byte
CacheHitPercent	Percentuale di operazioni di lettura delle applicazioni dal gateway servite dalla cache. Il campione si riferisce al termine del periodo di reporting. Quando non ci sono operazioni di lettura delle applicazioni dal gateway, questa metrica riporta il 100%. Unità: percentuale
CachePercentDirty	La percentuale complessiva della cache del gateway che non è stata mantenuta in modo persistente. AWS Il campione si riferisce al termine del periodo di reporting. Unità: percentuale
CachePercentUsed	La percentuale complessiva dello storage cache del gateway utilizzato. Il campione si riferisce al termine del periodo di reporting. Unità: percentuale
CacheUsed	Questa metrica riporta il numero di byte utilizzati nella cache del gateway. Unità: byte

Metrica	Description
`CloudBytesDownloaded`	Il numero totale di byte da cui il gateway è stato scaricato AWS durante il periodo di riferimento. Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni IOPS. Unità: byte
`CloudBytesUploaded`	Il numero totale di byte in cui il gateway è stato caricato AWS durante il periodo di riferimento. Utilizza questa metrica con la `Sum` statistica per misurare la velocità effettiva e con la `Samples` statistica per misurare le input/output operazion i al secondo (IOPS). Unità: byte
`FilesFailingUpload`	Questa metrica tiene traccia del numero di file su cui non viene eseguito il caricamento. AWS Questi file genereranno notifiche sanitarie che contengono ulteriori informazioni sul problema. Utilizza questa metrica con la `Sum` statistica per mostrare il numero di file su cui attualmente non è possibile caricare. AWS Unità: numero
`FileShares`	Questa metrica riporta il numero di condivisioni di file sul gateway. Unità: numero

Metrica	Description
`FileSystem-ERROR`	Questa metrica fornisce il numero di associazi oni di file system su questi gateway che si trovano nello stato ERROR. Se questa metrica riporta che eventuali associazioni di file system si trovano nello stato ERROR, è probabile che vi sia un problema con il gateway che potrebbe causare un'interr uzione del flusso di lavoro. Si consiglia di creare un allarme quando questa metrica riporta un valore diverso da zero. Unità: numero
`HealthNotifications`	Questa metrica riporta il numero di notifiche sanitarie generate da questo gateway nel periodo di riferimento. Unità: numero
`IndexEvictions`	Questa metrica riporta il numero di file i cui metadati sono stati rimossi dall'indice dei metadati dei file memorizzato nella cache per fare spazio a nuove voci. Il gateway mantiene questo indice di metadati, che viene compilato dal Cloud on demand. AWS Unità: numero
`IndexFetches`	Questa metrica riporta il numero di file per i quali sono stati recuperati i metadati. Il gateway mantiene un indice memorizzato nella cache dei metadati dei file, che viene compilato dal Cloud su richiesta. AWS Unità: numero

Metrica	Description
`IoWaitPercent`	Questa metrica riporta la percentuale di tempo in cui la CPU è in attesa di una risposta dal disco locale. Unità: percentuale
`MemTotalBytes`	Questa metrica riporta la quantità totale di memoria sul gateway. Unità: byte
`MemUsedBytes`	Questa metrica riporta la quantità di memoria utilizzata sul gateway. Unità: byte
`RootDiskFreeBytes`	Questa metrica riporta il numero di byte disponibili sul disco principale del gateway. Se questa metrica riporta che meno di 20 GB sono gratuiti, è necessario aumentare la dimensione del disco principale. Per aumentare la dimensione del disco root, è possibile aumentare la dimensione del disco root esistente sulla macchina virtuale. Quando la macchina virtuale viene riavviata, il gateway riconosce l'aumento delle dimensioni sul disco principale. Unità: byte

Metrica	Description
SmbV2Sessions	Questa metrica riporta il numero di SMBv2 sessioni attive sul gateway. Questa metrica viene emessa una volta per ogni file system associato al gateway. Utilizzate la statistica SUM per calcolare il numero totale di SMBv2 sessioni attive su tutti i file system. Unità: numero
SmbV3Sessions	Questa metrica riporta il numero di SMBv3 sessioni attive sul gateway. Questa metrica viene emessa una volta per ogni file system associato al gateway. Utilizzate la statistica SUM per calcolare il numero totale di SMBv3 sessioni attive su tutti i file system. Unità: numero
TotalCacheSize	Questa metrica riporta la dimensione totale della cache. Unità: byte
UserCpuPercent	Questa metrica riporta la percentuale di tempo dedicata all'elaborazione del gateway. Unità: percentuale

Comprensione delle metriche del file system

Di seguito sono riportate le informazioni sulle metriche di Storage Gateway relative ai file system. A ogni file system è associata una serie di metriche. Alcune metriche specifiche del file system hanno lo stesso nome di alcune metriche specifiche del gateway. Queste metriche rappresentano gli stessi tipi di misurazioni, ma sono invece limitate al file system.

Specificate sempre se desiderate utilizzare un gateway o una metrica del file system prima di utilizzare una metrica. In particolare, quando si lavora con le metriche del file system, è necessario

specificare quelle `File system ID` che identificano il file system per cui si desidera visualizzare le metriche. Per ulteriori informazioni, consulta Utilizzo dei CloudWatch parametri di Amazon.

> **Note**
>
> Alcuni parametri restituiscono punti dati solo quando sono stati generati nuovi dati durante il periodo di monitoraggio più recente.

La tabella seguente descrive le metriche di Storage Gateway che è possibile utilizzare per ottenere informazioni sulle condivisioni di file.

Metrica	Description
`CacheHitPercent`	Percentuale di operazioni di lettura delle applicazioni dalle condivisioni di file servite dalla cache. Il campione si riferisce al termine del periodo di reporting. Quando non ci sono operazioni di lettura delle applicazioni dalla condivisione di file, questa metrica riporta il 100%. Unità: percentuale
`CachePercentDirty`	Il contributo della condivisione di file alla percentuale complessiva della cache del gateway che non è stata mantenuta in modo persistente. AWS Il campione si riferisce al termine del periodo di reporting. Utilizza questa metrica con la `Sum` statistica. Idealmente, questa metrica dovrebbe rimanere bassa.

Metrica	Description
	Note Utilizza la `CachePercentDirty` metrica del gateway per visualizzare la percentuale complessiva della cache del gateway che non è stata salvata in modo persistente. AWS Unità: percentuale
`CachePercentUsed`	La percentuale di cache di dati utilizzata nell'intero gateway. Il campione si riferisce al termine del periodo di reporting. Questa metrica specifica per la condivisione di file riporta lo stesso valore della metrica specifica del gateway corrispondente. Unità: percentuale
`CloudBytesUploaded`	Il numero totale di byte in cui il gateway è stato caricato durante il periodo di riferimento. AWS Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni IOPS. Unità: byte

Metrica	Description
`CloudBytesDownloaded`	Il numero totale di byte da cui il gateway è stato scaricato AWS durante il periodo di riferimento. Utilizzate questa metrica con la `Sum` statistic a per misurare la velocità effettiva e con la `Samples` statistica per misurare le input/output operazioni al secondo (IOPS). Unità: byte
`FilesFailingUpload`	Questa metrica tiene traccia del numero di file su cui non viene eseguito il caricamento. AWS Questi file genereranno notifiche sanitarie che contengono ulteriori informazioni sul problema. Utilizza questa metrica con la `Sum` statistica per mostrare il numero di file su cui attualmente non è possibile caricare. AWS Unità: numero
`ReadBytes`	Numero totale di byte letti dalle applicazioni on-premise durante il periodo di reporting per una condivisione file. Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni IOPS. Unità: byte

Metrica	Description
`WriteBytes`	Numero totale di byte scritti nelle applicazioni in locale durante il periodo di reporting. Usa questo parametro con la statistica `Sum` per misurare il throughput e con la statistica `Samples` per misurare le operazioni IOPS. Unità: byte

Informazioni sui log di FSx

I log di controllo di Amazon FSx FSx File Gateway (File Gateway) forniscono dettagli sull'accesso degli utenti a file e cartelle all'interno di un'associazione di file system. Puoi utilizzare i log di controllo per monitorare le attività degli utenti e intervenire se vengono identificati modelli di attività inappropriati. I registri sono formattati in modo simile agli eventi dei registri di sicurezza di Windows Server, per supportare la compatibilità con gli strumenti di elaborazione dei log esistenti per gli eventi di sicurezza di Windows.

Operazioni

La tabella seguente descrive le operazioni di File Gateway File Gateway.

Nome operazione	Definizione
Leggere i dati	Leggi il contenuto di un file.
Scrivere i dati	Modifica il contenuto di un file.
Crea	Creare un nuovo file o una cartella.
Assegnazione di un nuovo nome	Rinominare un file o una cartella esistente.
Elimina	Eliminare un file o una cartella.
Attributi di scrittura	Aggiorna i metadati di file o cartelle (propriet arioACLs, gruppo, autorizzazioni).

Attributes

La tabella seguente descrive gli attributi di accesso al file di registro di controllo di FSx File Gateway.

Attributo	Definizione
`securityDescriptor`	Visualizza l'elenco di controllo di accesso discrezionale (DACL) impostato su un oggetto, in formato SDDL.
`sourceAddress`	L'indirizzo IP del computer client di condivisione file.
`SubjectDomainName`	Il dominio Active Directory (AD) a cui appartien e l'account client.
`SubjectUserName`	Il nome utente Active Directory del client.
`source`	L'ID dello Storage Gateway `FileSyste mAssociation` che viene verificato.
`mtime`	Ora in cui il contenuto dell'oggetto è stato modificato, impostata dal client.
`version`	Versione del formato del log di audit.
`ObjectType`	Definisce se l'oggetto è un file o una cartella.
`locationDnsName`	Il nome DNS del sistema FSx File Gateway.
`objectName`	Il percorso completo dell'oggetto.
`ctime`	L'ora in cui il contenuto o i metadati dell'oggetto sono stati modificato, impostata dal client.
`shareName`	Il nome della condivisione a cui si accede.
`operation`	Il nome dell'operazione di accesso dell'oggetto.
`newObjectName`	Il percorso completo del nuovo oggetto dopo che è stato rinominato.

Attributo	Definizione
`gateway`	L'ID gateway di storage.
`status`	Stato dell'operazione. Viene registrato solo l'esito positivo (gli errori vengono registrati ad eccezione degli errori derivanti da autorizza zioni negate).
`fileSizeInBytes`	La dimensione del file in byte, impostata dal client al momento della creazione del file.

Attributi registrati per operazione

La tabella seguente descrive gli attributi del registro di controllo di FSx File Gateway registrati in ogni operazione di accesso ai file.

	Leggi i dati	Scrivi dati	Crea cartella	Crea un file	Rinomina file/ cart ella	Eliminare file/ cart ella	Attributi di scrittura (modifica ACL)	Scrivi gli attributi (chown)	Scrivi attributi (chmod)	Scrivi attributi (chgrp)
`securi escrip`							X			
`source ress`	X	X	X	X	X	X	X	X	X	X
`Subjec mainNa`	X	X	X	X	X	X	X	X	X	X
`Subjec erName`	X	X	X	X	X	X	X	X	X	X
`source`	X	X	X	X	X	X	X	X	X	X

	Leggi i dati	Scrivi dati	Crea cartella	Crea un file	Rinomina file/ cartella	Eliminare file/ cartella	Attributi di scrittura (modifica ACL)	Scrivi gli attributi (chown)	Scrivi attributi (chmod)	Scrivi attributi (chgrp)
mtime			X	X						
versic	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
locati nsName	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
ctime			X	X						
shareN	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
newObj Name					X					
gatewa	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
fileSi nBytes				X						

Manutenzione del gateway

Manutenzione di Amazon FSx File Gateway implica la manutenzione generale per ottimizzare le prestazioni del gateway. Queste attività sono comuni a tutti i tipi di gateway.

Questa sezione contiene i seguenti argomenti, che descrivono concetti e procedure relativi alla manutenzione di Amazon FSx File Gateway Amazon Gateway:

Argomenti

- Gestione degli aggiornamenti del gateway— Scopri come attivare o disattivare gli aggiornamenti di manutenzione e modificare la pianificazione della finestra di manutenzione per File Gateway.
- Esecuzione delle attività di manutenzione utilizzando la console locale— Scopri come eseguire le attività di manutenzione utilizzando la console locale del gateway.
- Spegnimento della macchina virtuale gateway— Scopri cosa fare se devi spegnere o riavviare la macchina virtuale gateway per motivi di manutenzione, ad esempio quando applichi una patch all'hypervisor.
- Sostituzione del tuo una nuova istanza FSx— Scopri come sostituire il tuo con una nuova istanza quando desideri migliorare le prestazioni o rispondere a una notifica di migrazione del gateway.
- Eliminazione del gateway e rimozione delle risorse associate— Scopri come eliminare il gateway utilizzando la Gateway di archiviazione AWS console e ripulire le risorse associate per evitare che ti venga addebitato alcun costo per il loro uso continuato.

Gestione degli aggiornamenti del gateway

Storage Gateway è costituito da un componente di servizi cloud gestiti e da un componente di appliance gateway che puoi distribuire in locale o su un'istanza Amazon EC2 nel cloud. AWS Entrambi i componenti ricevono aggiornamenti regolari. Gli argomenti di questa sezione descrivono la frequenza di questi aggiornamenti, il modo in cui vengono applicati e come configurare le impostazioni relative agli aggiornamenti sui gateway della distribuzione.

> **Important**
>
> È necessario trattare l'appliance Storage Gateway come una macchina virtuale gestita e non tentare di accedere o modificare l'installazione o il contenuto in alcun modo. Il tentativo di installare o aggiornare qualsiasi pacchetto software utilizzando metodi diversi dal

normale meccanismo di aggiornamento del AWS gateway (ad esempio, SSM o strumenti dell'hypervisor) potrebbe causare il malfunzionamento del gateway.
Storage Gateway aggiorna automaticamente e regolarmente l'appliance per mantenere sicurezza e stabilità. Le appliance Storage Gateway utilizzano Amazon Linux come sistema operativo di base. Puoi controllare lo stato dei problemi CVE (Common Vulnerabilities and Exposures) rilevati su Amazon Linux Security Center. Le patch CVE vengono applicate automaticamente entro 30 giorni dal rilascio, come mostrato in Amazon Linux Security Center. Le patch vengono installate durante il programma di manutenzione del gateway, a condizione che il gateway sia online.
Storage Gateway non supporta l'aggiornamento manuale di un gateway Amazon EC2 utilizzando le direttive cloud-init. Se utilizzi questo metodo per aggiornare un gateway, potresti riscontrare problemi di interoperabilità che impediscono l'attivazione o l'utilizzo dell'appliance gateway.

Frequenza di aggiornamento e comportamento previsto

AWS aggiorna il componente dei servizi cloud in base alle esigenze senza causare interruzioni ai gateway implementati. I dispositivi gateway distribuiti ricevono i seguenti tipi di aggiornamenti:

- Manutenzione: aggiornamenti regolari che possono includere aggiornamenti del sistema operativo e del software, correzioni relative a stabilità, prestazioni e sicurezza e accesso a nuove funzionalità.
- Urgente: aggiornamenti critici che includono le correzioni necessarie per problemi che hanno un impatto immediato sulla sicurezza, le prestazioni o la durabilità del gateway. Gli aggiornamenti urgenti possono essere rilasciati in qualsiasi momento, al di fuori della normale cadenza degli aggiornamenti mensili di manutenzione e funzionalità.

Tutti gli aggiornamenti sono cumulativi e consentono di aggiornare i gateway alla versione corrente quando applicati. Per informazioni sulle modifiche specifiche incluse in ogni aggiornamento, consulta le

Tutti gli aggiornamenti delle appliance gateway possono causare una breve interruzione del servizio. Non è necessario riavviare l'host VM del gateway durante gli aggiornamenti, ma il gateway non sarà disponibile per un breve periodo durante l'aggiornamento e il riavvio dell'appliance gateway.

Quando si installa e si attiva il gateway, viene impostata una finestra di manutenzione predefinita. È possibile modificare la pianificazione della finestra di manutenzione in qualsiasi momento. Puoi anche disattivare gli aggiornamenti di manutenzione, ma ti consigliamo di lasciarli attivi.

> **Note**
>
> Gli aggiornamenti urgenti verranno applicati in base alla pianificazione della finestra di manutenzione, anche se gli aggiornamenti di manutenzione regolari sono disattivati.

Prima di applicare qualsiasi aggiornamento al gateway, ti AWS avvisa con un messaggio sulla console di Storage Gateway e sul tuo Dashboard AWS Health. Per ulteriori informazioni, consulta Dashboard AWS Health. Per modificare l'indirizzo e-mail a cui vengono inviate le notifiche di aggiornamento del software, consulta Aggiornare i contatti alternativi per l' AWS account nella Guida di riferimento per la gestione degli AWS account.

Quando gli aggiornamenti sono disponibili, nella scheda Dettagli del gateway viene visualizzato un messaggio di manutenzione. È inoltre possibile visualizzare la data e l'ora in cui è stato applicato l'ultimo aggiornamento riuscito nella scheda Dettagli.

Attiva o disattiva gli aggiornamenti di manutenzione

Quando gli aggiornamenti di manutenzione sono attivati, il gateway applica automaticamente questi aggiornamenti in base alla pianificazione della finestra di manutenzione configurata. Per ulteriori informazioni, vedere della finestra di manutenzione del gateway.

Se gli aggiornamenti di manutenzione sono disattivati, il gateway non li applicherà automaticamente, ma è sempre possibile applicarli manualmente utilizzando la console, l'API o la CLI di Storage Gateway. A volte gli aggiornamenti urgenti vengono applicati durante la finestra di manutenzione configurata, indipendentemente da questa impostazione.

> **Note**
>
> La procedura seguente descrive come attivare o disattivare gli aggiornamenti del gateway utilizzando la console Storage Gateway. Per modificare questa impostazione a livello di codice utilizzando l'API, vedere UpdateMaintenanceStartTimelo Storage Gateway API Reference.

Per attivare o disattivare gli aggiornamenti di manutenzione utilizzando la console Storage Gateway:

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel pannello di navigazione, scegli Gateway, quindi scegli il gateway per il quale desideri configurare gli aggiornamenti di manutenzione.
3. Scegli Azioni, quindi scegli Modifica impostazioni di manutenzione.
4. Per gli aggiornamenti di manutenzione, seleziona Attivato o Disattivato.
5. Al termine, scegli Salva modifiche.

È possibile verificare l'impostazione aggiornata nella scheda Dettagli per il gateway selezionato nella console Storage Gateway.

Modifica la pianificazione della finestra di manutenzione del gateway

Se gli aggiornamenti di manutenzione sono attivati, il gateway li applica automaticamente in base alla pianificazione della finestra di manutenzione. A volte vengono applicati aggiornamenti urgenti durante la finestra di manutenzione configurata, indipendentemente dall'impostazione degli aggiornamenti di manutenzione.

> **Note**
>
> La procedura seguente descrive come modificare la pianificazione della finestra di manutenzione utilizzando la console Storage Gateway. Per modificare questa impostazione a livello di codice utilizzando l'API, vedere UpdateMaintenanceStartTimelo Storage Gateway API Reference.

Per modificare la pianificazione della finestra di manutenzione utilizzando la console Storage Gateway:

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel pannello di navigazione, scegli Gateway, quindi scegli il gateway per il quale desideri configurare gli aggiornamenti di manutenzione.
3. Scegli Azioni, quindi scegli Modifica impostazioni di manutenzione.
4. In Ora di inizio della finestra di manutenzione, procedi come segue:

a. Per Pianificazione, scegli Settimanale o Mensile per impostare la cadenza della finestra di manutenzione.

b. Se scegli Settimanale, modifica i valori di Giorno della settimana e Ora per impostare il momento specifico durante ogni settimana in cui inizierà la finestra di manutenzione.

   Se scegli Mensile, modifica i valori di Giorno del mese e Ora per impostare il momento specifico durante ogni mese in cui inizierà la finestra di manutenzione.

   > **Note**
   >
   > Il valore massimo che può essere impostato per il giorno del mese è 28. Non è possibile impostare il programma di manutenzione in modo che inizi nei giorni dal 29 al 31.
   > Se ricevi un errore durante la configurazione di questa impostazione, è possibile che il software del gateway non sia aggiornato. Valuta la possibilità di aggiornare prima il gateway manualmente e poi di riprovare a configurare la pianificazione della finestra di manutenzione.

5. Al termine, scegli Salva le modifiche.

È possibile verificare le impostazioni aggiornate nella scheda Dettagli per il gateway selezionato nella console Storage Gateway.

Applica un aggiornamento manualmente

Se è disponibile un aggiornamento software per il gateway, è possibile applicarlo manualmente seguendo la procedura riportata di seguito. Questo processo di aggiornamento manuale ignora la pianificazione della finestra di manutenzione e applica l'aggiornamento immediatamente, anche se gli aggiornamenti di manutenzione sono disattivati.

> **Note**
>
> La procedura seguente descrive come applicare manualmente un aggiornamento utilizzando la console Storage Gateway. Per eseguire questa azione a livello di codice utilizzando l'API, vedere UpdateGatewaySoftwareNowlo Storage Gateway API Reference.

Per applicare manualmente un aggiornamento software del gateway utilizzando la console Storage Gateway:

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel pannello di navigazione, scegli Gateway, quindi scegli il gateway che desideri aggiornare.

   Se è disponibile un aggiornamento, la console visualizza un banner di notifica blu nella scheda Dettagli del gateway, che include un'opzione per applicare l'aggiornamento.
3. Scegli Applica aggiornamento ora per aggiornare immediatamente il gateway.

> **Note**
>
> Questa operazione causa un'interruzione temporanea della funzionalità del gateway durante l'installazione dell'aggiornamento. Durante questo periodo, lo stato del gateway appare OFFLINE nella console Storage Gateway. Al termine dell'installazione dell'aggiornamento, il gateway riprende il normale funzionamento e il suo stato passa a RUNNING.

È possibile verificare che il software del gateway sia stato aggiornato alla versione più recente controllando la scheda Dettagli per il gateway selezionato nella console Storage Gateway.

Esecuzione delle attività di manutenzione utilizzando la console locale

Questa sezione contiene i seguenti argomenti, che forniscono informazioni su come eseguire le attività di manutenzione utilizzando la console locale dell'appliance gateway. Puoi eseguire queste attività accedendo alla console locale tramite la macchina virtuale locale o l'istanza Amazon EC2 che ospita il tuo dispositivo gateway. La maggior parte delle attività è comune tra le diverse piattaforme host, ma ci sono anche alcune differenze.

Argomenti

- Accesso alla console locale del gateway- Scopri come accedere alla console locale per un gateway locale ospitato su una macchina virtuale (KVM) basata su Linux Kernel VMware ESXi o una piattaforma Microsoft Hyper-V Manager.

- Esecuzione di attività sulla console locale della macchina virtuale- Scopri come utilizzare la console locale per eseguire attività di configurazione di base e attività di configurazione avanzate per un gateway locale, come la configurazione di un proxy HTTP, la visualizzazione dello stato delle risorse di sistema o l'esecuzione di comandi del terminale.
- Esecuzione di attività sulla console locale del gateway Amazon EC2- Scopri come accedere alla console locale per eseguire attività di configurazione di base e avanzate per un gateway Amazon EC2, come configurare un proxy HTTP, visualizzare lo stato delle risorse di sistema o eseguire comandi da terminale.

Accesso alla console locale del gateway

L'accesso alla console locale di una VM dipende dal tipo di Hypervisor su cui è stata distribuita la VM del gateway. In questa sezione, puoi trovare informazioni su come accedere alla console locale della macchina virtuale utilizzando Linux Kernel-based Virtual Machine (KVM) VMware ESXi e Microsoft Hyper-V Manager.

Argomenti

- Accesso alla console locale del gateway con Linux KVM
- Accesso alla console locale del gateway con VMware ESXi
- Accesso alla console locale del gateway con Microsoft Hyper-V

Accesso alla console locale del gateway con Linux KVM

Esistono diversi modi per configurare le macchine virtuali in esecuzione su KVM, a seconda della distribuzione Linux utilizzata. Istruzioni per accedere alle opzioni di configurazione KVM dalla riga di comando. Le istruzioni potrebbero differire a seconda dell'implementazione KVM.

Per accedere alla console locale del gateway con KVM

1. Usa il seguente comando per elencare VMs quelli attualmente disponibili in KVM.

   ```
   # virsh list
   ```

   Il comando restituisce un elenco di informazioni relative VMs all'ID, al nome e allo stato per ciascuna di esse. Annota `Id` la macchina virtuale per la quale desideri avviare la console locale del gateway.

2. Utilizzare il comando seguente per accedere alla console locale.

```
# virsh console Id
```

Sostituisci *Id* con l'ID della macchina virtuale annotato nel passaggio precedente.

La console locale di AWS Appliance gateway richiede di effettuare il login per modificare la configurazione di rete e altre impostazioni.

3. Immettete il nome utente e la password per accedere alla console locale del gateway. Per ulteriori informazioni, vedere File Gateway.

Dopo aver effettuato l'accesso, viene visualizzato il menu Attivazione AWS dell'appliance - Configurazione. È possibile selezionare le opzioni del menu per eseguire le attività di configurazione del gateway. Per ulteriori informazioni, vedere Esecuzione di attività sulla console locale della macchina virtuale.

Accesso alla console locale del gateway con VMware ESXi

Per accedere alla console locale del gateway con VMware ESXi

1. Nel client VMware vSphere, selezionare la macchina virtuale gateway.
2. Assicurati che la VM gateway sia accesa.

> **Note**
>
> Se la macchina virtuale gateway è accesa, viene visualizzata un'icona a forma di freccia verde con l'icona della macchina virtuale nel pannello del browser della macchina virtuale sul lato sinistro della finestra dell'applicazione. Se la tua VM gateway non è accesa, puoi accenderla scegliendo l'icona verde Power On sulla barra degli strumenti nella parte superiore della finestra dell'applicazione.

3. Scegli la scheda Console nel pannello delle informazioni principale sul lato destro della finestra dell'applicazione.

Dopo alcuni istanti, la console locale del gateway dell' AWS appliance richiede di effettuare il login per modificare la configurazione di rete e altre impostazioni.

> **Note**
>
> Per rilasciare il cursore dalla finestra della console, premi Ctrl+Alt.

4. Immettete il nome utente e la password per accedere alla console locale del gateway. Per ulteriori informazioni, vedere File Gateway.

   Dopo aver effettuato l'accesso, viene visualizzato il menu Attivazione AWS dell'appliance - Configurazione. È possibile selezionare le opzioni del menu per eseguire le attività di configurazione del gateway. Per ulteriori informazioni, vedere Esecuzione di attività sulla console locale della macchina virtuale.

Accesso alla console locale del gateway con Microsoft Hyper-V

Per accedere alla console locale del gateway (Microsoft Hyper-V)

1. Seleziona la macchina virtuale dell'appliance gateway dal pannello Macchine virtuali sul lato sinistro della finestra dell'applicazione Microsoft Hyper-V Manager.
2. Verifica che il gateway sia attivo.

> **Note**
>
> Se la macchina virtuale gateway è accesa, `Running` viene visualizzata nella colonna Stato della macchina virtuale nel pannello Macchine virtuali sul lato sinistro della finestra dell'applicazione. Se la VM gateway non è accesa, puoi accenderla scegliendo Avvia nel pannello Azioni sul lato destro della finestra dell'applicazione.

3. Scegliete Connect dal pannello Azioni.

   Verrà visualizzata la finestra Virtual Machine Connection (Connessione macchina virtuale). Se viene visualizzata una finestra di autenticazione, digitare le credenziali di accesso fornite dall'amministratore dell'hypervisor.

   Dopo alcuni istanti, la console locale del gateway dell' AWS appliance richiede di effettuare il login per modificare la configurazione di rete e altre impostazioni.

4. Immettete il nome utente e la password per accedere alla console locale del gateway. Per ulteriori informazioni, vedere File Gateway.

   Dopo aver effettuato l'accesso, viene visualizzato il menu Attivazione AWS dell'appliance - Configurazione. È possibile selezionare le opzioni del menu per eseguire le attività di configurazione del gateway. Per ulteriori informazioni, vedere Esecuzione di attività sulla console locale della macchina virtuale.

Esecuzione di attività sulla console locale della macchina virtuale

Per un File Gateway distribuito in locale, è possibile eseguire le seguenti attività di manutenzione utilizzando la console locale dell'host VM. Queste attività sono comuni agli VMware hypervisor Microsoft Hyper-V e Linux Kernel-based Virtual Machine (KVM).

Argomenti

- Accesso alla console locale File Gateway- Scopri come accedere alla console locale dove puoi configurare le impostazioni di rete del gateway e modificare la password predefinita.
- Configurazione di un proxy HTTP- Scopri come configurare Storage Gateway per instradare tutto il traffico AWS degli endpoint attraverso un server proxy.
- Configurazione delle impostazioni di rete del gateway- Scopri come configurare il gateway per utilizzare DHCP o un indirizzo IP statico.
- Verifica della connettività di rete del gateway- Scopri come utilizzare la console locale del gateway per testare la connettività di rete.
- Visualizzazione dello stato relativo alle risorse di sistema del gateway- Scopri come controllare i core della CPU virtuale, le dimensioni del volume root e la RAM del gateway.
- Configurazione di un server Network Time Protocol (NTP) per il gateway- Scopri come visualizzare e modificare le configurazioni del server NTP (Network Time Protocol) e sincronizzare l'ora del gateway con l'host dell'hypervisor.
- Esecuzione di comandi Storage Gateway sulla console locale- Scopri come eseguire i comandi della console locale per eseguire attività come il salvataggio delle tabelle di routing, la connessione e altro ancora. Supporto

Accesso alla console locale File Gateway

Quando la VM è pronta per l'accesso, è visualizzata la schermata di autenticazione. Se è la prima volta che si accede alla console locale della macchina virtuale, si utilizzano le credenziali di accesso temporanee per accedere. Queste credenziali temporanee consentono di accedere ai menu in cui è possibile configurare le impostazioni di rete del gateway e modificare la password dalla console locale. Il nome utente iniziale è `admin` e la password temporanea è. `password` È necessario modificare la password al primo accesso.

Per modificare la password temporanea

1. Nel menu principale AWS Appliance Activation - Configuration, immettere il numero corrispondente per Gateway Console.
2. Esegui il comando `passwd`. Per informazioni su come eseguire il comando, consulta Esecuzione di comandi Storage Gateway sulla console locale.

Impostazione della password della console locale dalla console Storage Gateway

È inoltre possibile gestire la password della console locale dalla console basata sul Web di Storage Gateway. Qualsiasi aggiornamento della password eseguito con successo con la console basata sul Web sostituirà la password utilizzata dalla console locale della VM del gateway, inclusa la password temporanea se non è mai stato effettuato l'accesso localmente. Se il gateway non è attualmente raggiungibile tramite la rete, il processo di aggiornamento della password avrà esito negativo.

Per impostare la password della console locale sulla console Storage Gateway

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel pannello di navigazione, scegli Gateway, quindi seleziona il gateway per il quale desideri impostare una nuova password.
3. In Actions (Operazioni), selezionare Set Local Console Password (Imposta la password della console locale).
4. Nella finestra di dialogo di Set Local Console Password (Imposta la password della console locale), digitare la nuova password, poi confermarla e, infine, selezionare Save (Salva).

   La nuova password sostituisce la password attuale. Il servizio Storage Gateway non salva, archivia o registra la password, ma la trasmette in modo sicuro tramite un canale crittografato alla macchina virtuale, dove viene archiviata in modo sicuro.

> **Note**
>
> La password può essere composta da qualsiasi carattere sulla tastiera e può contenere da 1 a 512 caratteri.

Configurazione di un proxy HTTP

I File Gateway supportano la configurazione di un proxy HTTP.

> **Note**
>
> L'unica configurazione proxy supportata da File Gateway è HTTP.

Se il gateway deve usare un server proxy per comunicare con Internet, devi configurare le impostazioni del proxy HTTP per il gateway. A tale scopo, basta specificare un indirizzo IP e un numero di porta per l'host che esegue il proxy. Dopo averlo fatto, Storage Gateway indirizza tutto il traffico AWS degli endpoint attraverso il server proxy. Le comunicazioni tra il gateway e gli endpoint sono crittografate, anche quando si utilizza il proxy HTTP. Per informazioni sui requisiti di rete del gateway, consulta Requisiti di rete e firewall.

Per configurare un proxy HTTP per un File Gateway

1. Accedere alla console locale del gateway:
   - Per ulteriori informazioni sull'accesso alla console VMware ESXi locale, vedereAccesso alla console locale del gateway con VMware ESXi.
   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
   - Per ulteriori informazioni sull'accesso alla console locale per la macchina virtuale basata su kernel Linux (KVM), consulta Accesso alla console locale del gateway con Linux KVM.
2. Dal menu principale Attivazione dell'AWS appliance: configurazione, immettere il numero corrispondente per selezionare Configurazione del proxy HTTP.
3. Dal menu di Configurazione del proxy HTTP per l'attivazione dell'appliance AWS , immettere il numero corrispondente per l'operazione che si desidera eseguire:

- Configurazione del proxy HTTP: specificare un nome host e una porta per completare la configurazione.
- Visualizzazione della configurazione del proxy HTTP corrente: se il proxy HTTP non è configurato, viene visualizzato il messaggio `HTTP Proxy not configured`. Se un proxy HTTP è configurato, vengono visualizzati il nome host e la porta del proxy HTTP.
- Rimozione di una configurazione del proxy HTTP: viene visualizzato il messaggio `HTTP Proxy Configuration Removed`.

4. Per applicare le impostazioni della configurazione HTTP, riavviare la VM.

Configurazione delle impostazioni di rete del gateway

L'impostazione predefinita per la configurazione di rete del gateway è DHCP (Dynamic Host Configuration Protocol). Con DHCP, al gateway viene assegnato automaticamente un indirizzo IP. In alcuni casi, può essere necessario assegnare manualmente un indirizzo IP statico al gateway, come descritto di seguito.

Per configurare il gateway affinché utilizzi indirizzi IP statici

1. Accedere alla console locale del gateway:
   - Per ulteriori informazioni sull'accesso alla console VMware ESXi locale, vedereAccesso alla console locale del gateway con VMware ESXi.
   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
   - Per ulteriori informazioni sull'accesso alla console locale di KVM, consulta Accesso alla console locale del gateway con Linux KVM.
2. Dal menu principale Attivazione dell'AWS appliance - Configurazione, immettere il numero corrispondente per selezionare Configurazione di rete.
3. Dal menu Network Configuration, effettuate una delle seguenti operazioni:

Per eseguire questa operazione	eseguire questa operazione
Ottenere informazioni sulla scheda di rete	Immettere il numero corrispondente per selezionare Descrivi adattatore.

Per eseguire questa operazione	eseguire questa operazione
	Viene visualizzato un elenco di nomi di adattatore e viene richiesto di immettere un nome di adattatore, ad esempio. **`eth0`** Se la scheda specificata è in uso, vengono mostrate le seguenti informazioni: • Indirizzo MAC (Media Access Control) • IP address (Indirizzo IP) • Netmask • Indirizzo IP del gateway • Stato DHCP abilitato I nomi degli adattatori elencati qui vengono utilizzati quando si configura un indirizzo IP statico o quando si imposta l'adattatore predefinito del gateway.
Configura il routing DHCP	Inserisci il numero corrispondente per seleziona re Configura DHCP. Per l'utilizzo di DHCP, viene richiesto di configurare l'interfaccia di rete.

Per eseguire questa operazione	eseguire questa operazione
Configurare un indirizzo IP statico per il gateway	Inserisci il numero corrispondente per seleziona re Configura IP statico. Per configurare un indirizzo IP statico, viene chiesto di digitare le informazioni riportate di seguito: • Nome scheda di rete • IP address (Indirizzo IP) • Netmask • Indirizzo del gateway predefinito • Indirizzo DNS (Domain Name Service) primario • Indirizzo DNS (Domain Name Service) secondario **Important** Se il gateway è già stato attivato, affinché le impostazioni abbiano effetto è necessario arrestarlo e riavviarlo dalla console Storage Gateway. Per ulteriori informazioni, consulta Spegnimento della macchina virtuale gateway.

Per eseguire questa operazione	eseguire questa operazione
	Se il gateway utilizza più di un'interfaccia di rete, è necessario impostare tutte le interfacce attive in modo che utilizzino DHCP o indirizzi IP statici. Ad esempio, supponiamo che la VM del gateway utilizzi due interfacce configurate come DHCP. Se in un secondo momento si imposta un'interfaccia con un IP statico, l'altra interfaccia viene disattivata. Per riattivarla, sarà necessario configurarla con un indirizzo IP statico. Se entrambe le interfacce sono inizialmente configurate per l'utilizzo di indirizzi IP statici e poi si imposta il gateway in modo che si avvalga di DHCP, entrambe le interfacce, infine, utilizzeranno DHCP.

Per eseguire questa operazione	eseguire questa operazione
Configura un nome host per il gateway	Immettere il numero corrispondente per selezionare Configura nome host. Ti viene richiesto di scegliere se il gateway utilizzerà un nome host statico specificato dall'utente o ne acquisirà uno automaticamente tramite DCHP o rDNS. Se si seleziona Statico, viene richiesto di fornire un nome host statico, ad esempio. `testgateway.example.com` Entra y per applicare la configurazione. **Note** Se configuri un nome host statico per il gateway, assicurati che il nome host fornito si trovi nel dominio a cui è unito il gateway. È inoltre necessario creare un record A nel sistema DNS che punti l'indirizzo IP del gateway al relativo nome host statico.
Visualizza la configurazione del nome host del gateway	Inserisci il numero corrispondente per selezionare Visualizza la configurazione del nome host. Vengono visualizzati il nome host, la modalità di acquisizione, il dominio e il realm di Active Directory del gateway.

Per eseguire questa operazione	eseguire questa operazione
Reimpostare tutte le configurazioni di rete del gateway su DHCP	Immettere il numero corrispondente per selezionare Reimposta tutto su DHCP. Tutte le interfacce di rete sono impostate per l'utilizzo di DHCP. **Important** Se il gateway è già stato attivato, affinché le impostazioni abbiano effetto è necessario arrestare il gateway stesso e riavviarlo dalla console Storage Gateway. Per ulteriori informazioni, consulta Spegnimento della macchina virtuale gateway.
Impostare l'adattatore di routing predefinito del gateway	Immettere il numero corrispondente per selezionare Imposta scheda predefinita. Vengono visualizzati gli adattatori disponibili per il gateway e viene richiesto di scegliere uno degli adattatori, ad esempio. **`eth0`**
Modificare la configurazione DNS del gateway	Inserisci il numero corrispondente per seleziona re Modifica configurazione DNS. Vengono visualizzate le schede disponibili dei server DNS primario e secondario. Viene richiesto di fornire il nuovo indirizzo IP.

Per eseguire questa operazione	eseguire questa operazione
Visualizzare la configurazione DNS del gateway	Immettere il numero corrispondente per selezionare Visualizza configurazione DNS. Vengono visualizzate le schede disponibili dei server DNS primario e secondario. **Note** Per alcune versioni dell' VMware hypervisor, puoi modificare la configura zione dell'adattatore in questo menu.
Visualizzare le tabelle di routing	Immettere il numero corrispondente per selezionare Visualizza instradamenti. Viene visualizzato l'instradamento predefinito del gateway.

Verifica della connettività di rete del gateway

Puoi utilizzare la console locale del gateway per testare la connettività di rete. Questo test può essere utile per risolvere eventuali problemi di rete del gateway.

Per testare la connettività di rete del gateway

1. Accedere alla console locale del gateway:

   - Per ulteriori informazioni sull'accesso alla console VMware ESXi locale, vedereAccesso alla console locale del gateway con VMware ESXi.
   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
   - Per ulteriori informazioni sull'accesso alla console locale di KVM, consulta Accesso alla console locale del gateway con Linux KVM.

2. Dal menu principale Attivazione dell'AWS appliance: configurazione, inserisci il numero corrispondente per selezionare Verifica connettività di rete.

   Se il gateway è già stato attivato, il test di connettività inizia immediatamente. Per i gateway che non sono ancora stati attivati, è necessario specificare il tipo di endpoint e seguire la procedura descritta nei passaggi Regione AWS seguenti.
3. Se il gateway non è ancora attivato, inserisci il numero corrispondente per selezionare il tipo di endpoint per il gateway.
4. Se hai selezionato il tipo di endpoint pubblico, inserisci il numero corrispondente per selezionare Regione AWS quello che desideri testare. Per gli endpoint supportati Regioni AWS e un elenco degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere Gateway di archiviazione AWS endpoint e quote nel. Riferimenti generali di AWS

Man mano che il test procede, ogni endpoint visualizza [PASSED] o [FAILED], indicando lo stato della connessione nel modo seguente:

Messaggio	Description
[PASSED]	Storage Gateway dispone di connettività di rete.
[FAILED]	Storage Gateway non dispone di connettività di rete.

Visualizzazione dello stato relativo alle risorse di sistema del gateway

Quando viene avviato, il gateway verifica i core CPU virtuali, la dimensione del volume root e la RAM. Quindi stabilisce se tali risorse di sistema sono sufficienti per il corretto funzionamento del gateway. I risultati di questi controlli sono riportati nella console locale del gateway.

Per visualizzare lo stato di un controllo delle risorse di sistema

1. Accedere alla console locale del gateway:

   - Per ulteriori informazioni sull'accesso alla VMware ESXi console, vedereAccesso alla console locale del gateway con VMware ESXi.
   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.

- Per ulteriori informazioni sull'accesso alla console locale di KVM, consulta Accesso alla console locale del gateway con Linux KVM.

2. Dal menu principale Attivazione dell'appliance AWS : configurazione, immettere il numero corrispondente per selezionare Visualizzazione del controllo relativo alle risorse di sistema.

   Ogni risorsa visualizza [OK], [ATTENZIONE] o [ERRORE], che indicano lo stato della risorsa nel modo seguente:

Messaggio	Description
[OK]	La risorsa ha superato il controllo delle risorse di sistema.
[WARNING]	La risorsa non soddisfa i requisiti raccomandati, ma il gateway può continuare a funzionare. Storage Gateway mostra un messaggio che descrive i risultati del controllo delle risorse.
[FAIL]	La risorsa non soddisfa i requisiti minimi. Il gateway potrebbe non funzionare correttamente. Storage Gateway mostra un messaggio che descrive i risultati del controllo delle risorse.

   La console visualizza inoltre il numero di errori e avvisi accanto all'opzione del menu di controllo delle risorse.

Configurazione di un server Network Time Protocol (NTP) per il gateway

Puoi visualizzare e modificare le configurazioni del server Network Time Protocol (NTP) e sincronizzare l'ora della VM associata al gateway con l'host dell'hypervisor.

Per gestire l'ora di sistema

1. Accedere alla console locale del gateway:

- Per ulteriori informazioni sull'accesso alla console VMware ESXi locale, vedere. Accesso alla console locale del gateway con VMware ESXi
- Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
- Per ulteriori informazioni sull'accesso alla console locale di KVM, consulta Accesso alla console locale del gateway con Linux KVM.

2. Dal menu principale Attivazione dell'AWS appliance - Configurazione, immettere il numero corrispondente per selezionare System Time Management.
3. Dal menu System Time Management, immettete il numero corrispondente per eseguire una delle seguenti attività.

Per eseguire questa operazione	eseguire questa operazione
Visualizza e sincronizza l'ora della VM con quella del server NTP.	Immettete il numero corrispondente per selezionare Visualizza e sincronizza l'ora di sistema. Viene visualizzata l'ora corrente della VM. Il File Gateway determina la differenza di fuso orario rispetto alla VM del gateway e l'ora del server NTP richiede di sincronizzare l'ora della VM con l'ora NTP. Dopo la distribuzione e l'esecuzione del gateway, in alcune situazioni l'ora impostata sulla VM a esso associata può presentare degli scostamenti. Ad esempio, se si verifica un'interruzione di rete prolungata e l'host dell'hypervisor e il gateway non ricevono gli aggiornamenti dell'ora, l'ora della VM del gateway divergerà dall'ora esatta. Quando si verifica uno scostamento dell'ora, si genera una discrepanza tra l'ora di esecuzione indicata in caso di operazioni quali gli snapshot e l'ora

Per eseguire questa operazione	eseguire questa operazione
	effettiva alla quale le operazioni vengono eseguite. Per un gateway distribuito su VMware ESXi, è sufficiente impostare l'ora dell'host dell'hype rvisor e sincronizzare l'ora della VM con l'host per evitare variazioni di orario. Per ulteriori informazioni, consulta Sincronizza l'ora della macchina virtuale con l'ora dell'host VMware. In caso, invece, di gateway distribuito su Microsoft Hyper-V, è necessario controllare periodicamente l'ora impostata sulla VM. Per ulteriori informazioni, consulta Sincronizza l'ora della macchina virtuale con l'ora dell'host KVM Hyper-V o Linux. Per un gateway distribuito su KVM, è possibile controllare e sincronizzare l'ora della macchina virtuale utilizzando l'interfaccia della riga di comando `virsh` per KVM.
Modifica della configurazione del server NTP	Immettere il numero corrispondente per selezionare Modifica configurazione NTP. Ti viene richiesto di fornire un server NTP preferito e un server secondario.
Visualizzazione della configurazione del server NTP	Immettere il numero corrispondente per selezionare Visualizza configurazione NTP. Viene visualizzata la configurazione del server NTP.

Esecuzione di comandi Storage Gateway sulla console locale

La console locale della VM in Storage Gateway offre un ambiente sicuro per la configurazione e la diagnostica dei problemi del gateway. Utilizzando i comandi della console locale, è possibile eseguire attività di manutenzione come il salvataggio delle tabelle di routing, la connessione e così via. Supporto

Per eseguire un comando di diagnostica o di configurazione

1. Accedere alla console locale del gateway:
   - Per ulteriori informazioni sull'accesso alla console VMware ESXi locale, vedere. Accesso alla console locale del gateway con VMware ESXi
   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
   - Per ulteriori informazioni sull'accesso alla console locale di KVM, consulta Accesso alla console locale del gateway con Linux KVM.
2. Dal menu principale Attivazione dell'appliance AWS : configurazione, immettere il numero corrispondente per selezionare Console del gateway.
3. Dal prompt dei comandi della console del gateway, immettere **h**.

   La console mostra il menu COMANDI DISPONIBILI che elenca i comandi disponibili:

Comando	Funzione
dig	Raccogli l'output da dig per la risoluzione dei problemi DNS.
Esci	Torna al menu di configurazione.
h	Visualizza l'elenco dei comandi disponibili.
ifconfig	Visualizza o configura le interfacce di rete. **Note** Si consiglia di configurare le impostazioni di rete o IP utilizzando la console

Comando	Funzione
	Storage Gateway o l'opzione del menu della console locale dedicata. Per istruzioni, vedere Configurazione delle impostazioni della rete gateway Configurazione delle impostazioni .
ip	Mostra/manipola routing, dispositivi e tunnel. **Note** Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata. Per istruzioni, vedere Configurazione delle impostazioni della rete gateway delle impostazioni della rete gateway.
iptables	Strumento di amministrazione per il filtraggio dei IPv4 pacchetti e NAT.
ncport	Verifica la connettività a una porta TCP specifica su una rete.
nping	Raccogli l'output da nping per la risoluzione dei problemi di rete.
open-support-channel	Connect to AWS Support. Per istruzioni su come attivare l'accesso al AWS supporto, vedi EC2.
passwd	Aggiorna i token di autenticazione.
save-iptables	Tabelle IP persistenti.

Comando	Funzione
save-routing-table	Salva la voce della tabella di routing appena aggiunta.
tcptraceroute	Raccogli l'output del traceroute sul traffico TCP verso una destinazione.
sslcheck	Restituisce l'output con l'emittente del certifica to **Note** Storage Gateway utilizza la verifica dell'emittente del certificato e non supporta l'ispezione SSL. Se questo comando restituisce un emittente diverso da aws-appliance@amaz on.com, è probabile che sia un'applic azione che esegue un'ispezione ssl. In tal caso, si consiglia di ignorare l'ispezione SSL per l'appliance Storage Gateway.

4. Dal prompt dei comandi della console del gateway, immettere il comando corrispondente alla funzione che si desidera utilizzare e seguire le istruzioni.

Per informazioni su un comando, digitare **`man`** + *`command name`* al prompt dei comandi.

Esecuzione di attività sulla console locale del gateway Amazon EC2

Per alcune attività di manutenzione devi effettuare l'accesso alla console locale durante l'esecuzione di un gateway distribuito in un'istanza Amazon EC2. Questa sezione descrive come accedere alla console locale ed eseguire attività di manutenzione.

Argomenti

- Accesso alla console locale del gateway Amazon EC2- Scopri come connetterti e accedere alla console locale del gateway, la tua istanza Amazon EC2, utilizzando un client Secure Shell (SSH).
- Routing del gateway distribuito su Amazon EC2 tramite un proxy HTTP- Scopri come configurare un proxy Socket Secure versione 5 (SOCKS5) tra AWS e un gateway distribuito su un'istanza Amazon EC2.
- Verifica della connettività di rete del gateway- Scopri come utilizzare la console locale del gateway per testare la connettività di rete tra il gateway e varie risorse di rete.
- Visualizzazione dello stato relativo alle risorse di sistema del gateway- Scopri come utilizzare la console locale del gateway per controllare i core della CPU virtuale, le dimensioni del volume root e la RAM del gateway.
- Esecuzione dei comandi Storage Gateway sulla console locale per un gateway Amazon EC2- Scopri come eseguire i comandi della console locale per eseguire attività come il salvataggio delle tabelle di routing, la connessione e altro Supporto ancora.
- Configurazione delle impostazioni di rete del gateway Amazon EC2- Scopri come utilizzare la console locale per visualizzare e configurare le impostazioni di rete come DNS e nome host per un gateway su un'istanza Amazon EC2.

Accesso alla console locale del gateway Amazon EC2

Accedi alla console locale del gateway su un'istanza Amazon EC2 utilizzando un client Secure Shell (SSH). Per informazioni dettagliate, consulta Connect to your istance nella Amazon EC2 User Guide. Per connetterti in questo modo, avrai bisogno della coppia di chiavi SSH specificata all'avvio dell'istanza. Per informazioni sulle coppie di chiavi Amazon EC2, consulta le coppie di chiavi Amazon EC2 nella Guida per l'utente di Amazon EC2.

Accedere alla console locale del gateway

1. Connect all'istanza Amazon EC2 tramite SSH e accedi come utente amministratore.
2. Dopo aver effettuato l'accesso, viene visualizzato il menu principale AWS Appliance Activation - Configuration, da cui è possibile eseguire varie attività.

Per ulteriori informazioni su questa attività	vedere questo argomento
Configurare un proxy HTTP per il gateway	Routing del gateway distribuito su Amazon EC2 tramite un proxy HTTP

Per ulteriori informazioni su questa attività	vedere questo argomento
Configurazione delle impostazioni di rete per il gateway	Configurazione delle impostazioni di rete del gateway Amazon EC2
Verificare la connettività di rete	Verifica della connettività di rete del gateway
Visualizzare un controllo delle risorse di sistema	Visualizzazione dello stato relativo alle risorse di sistema del gateway.
Esecuzione dei comandi della console Storage Gateway	Esecuzione dei comandi Storage Gateway sulla console locale per un gateway Amazon EC2

Per arrestare il gateway, digitare **0**.

Per uscire dalla sessione di configurazione, digitare **X**.

Routing del gateway distribuito su Amazon EC2 tramite un proxy HTTP

Storage Gateway supporta la configurazione di un proxy Socket Secure versione 5 (SOCKS5) tra il gateway distribuito in Amazon EC2 e AWS.

Se il gateway deve usare un server proxy per comunicare con Internet, devi configurare le impostazioni del proxy HTTP per il gateway. A tale scopo, basta specificare un indirizzo IP e un numero di porta per l'host che esegue il proxy. Dopo averlo fatto, Storage Gateway indirizza tutto il traffico AWS degli endpoint attraverso il server proxy. Le comunicazioni tra il gateway e gli endpoint sono crittografate, anche quando si utilizza il proxy HTTP.

Per instradare il traffico Internet del gateway attraverso un server proxy locale

1. Accedere alla console locale del gateway. Per istruzioni, consulta Accesso alla console locale del gateway Amazon EC2.
2. Dal menu principale Attivazione dell'AWS appliance: configurazione, immettere il numero corrispondente per selezionare Configurazione del proxy HTTP.
3. Dal menu di Configurazione del proxy HTTP per l'attivazione dell'appliance AWS , immettere il numero corrispondente per l'operazione che si desidera eseguire:

- Configurazione del proxy HTTP: specificare un nome host e una porta per completare la configurazione.
- Visualizzazione della configurazione del proxy HTTP corrente: se il proxy HTTP non è configurato, viene visualizzato il messaggio `HTTP Proxy not configured`. Se un proxy HTTP è configurato, vengono visualizzati il nome host e la porta del proxy HTTP.
- Rimozione di una configurazione del proxy HTTP: viene visualizzato il messaggio `HTTP Proxy Configuration Removed`.

Verifica della connettività di rete del gateway

Puoi utilizzare la console locale del gateway per testare la connettività di rete. Questo test può essere utile per risolvere eventuali problemi di rete del gateway.

Per testare la connettività del gateway

1. Accedere alla console locale del gateway. Per istruzioni, consulta Accesso alla console locale del gateway Amazon EC2.
2. Dal menu principale Attivazione dell'AWS appliance: configurazione, inserisci il numero corrispondente per selezionare Verifica connettività di rete.

   Se il gateway è già stato attivato, il test di connettività inizia immediatamente. Per i gateway che non sono ancora stati attivati, è necessario specificare il tipo di endpoint e procedere Regione AWS come descritto nei passaggi seguenti.
3. Se il gateway non è ancora attivato, inserisci il numero corrispondente per selezionare il tipo di endpoint per il gateway.
4. Se hai selezionato il tipo di endpoint pubblico, inserisci il numero corrispondente per selezionare Regione AWS quello che desideri testare. Per gli endpoint supportati Regioni AWS e un elenco degli endpoint di AWS servizio che è possibile utilizzare con Storage Gateway, vedere Gateway di archiviazione AWS endpoint e quote nel. Riferimenti generali di AWS

Man mano che il test procede, ogni endpoint visualizza [PASSED] o [FAILED], indicando lo stato della connessione nel modo seguente:

Messaggio	Description
[PASSED]	Storage Gateway dispone di connettività di rete.
[FAILED]	Storage Gateway non dispone di connettività di rete.

Visualizzazione dello stato relativo alle risorse di sistema del gateway

All'avvio, File Gateway controlla i core della CPU virtuale, le dimensioni del volume root e la RAM. Quindi determina se le risorse di sistema disponibili sono sufficienti per il corretto funzionamento del gateway. È possibile visualizzare i risultati del controllo delle risorse di sistema utilizzando la console locale del gateway.

Per visualizzare lo stato di un controllo delle risorse di sistema

1. Accedi alla console locale sul tuo Amazon EC2 File Gateway. Per istruzioni, consulta Accesso alla console locale del gateway Amazon EC2.
2. Nel menu principale Attivazione dell'appliance AWS : configurazione, immettere il numero seriale corrispondente per selezionare Visualizzazione del controllo relativo alle risorse di sistema.

   La console locale del gateway visualizza [OK], [WARNING] o [FAIL] per indicare lo stato della risorsa nel modo seguente:

Messaggio	Description
[OK]	La risorsa ha superato il controllo delle risorse di sistema.
[WARNING]	La risorsa non soddisfa i requisiti consigliati, ma il gateway può continuare a funzionare. La console locale del gateway visualizza un messaggio che descrive i risultati del controllo delle risorse.
[FAIL]	La risorsa non soddisfa i requisiti minimi. Il gateway potrebbe non funzionare correttam

Messaggio	Description
	ente. La console locale del gateway visualizz a un messaggio che descrive i risultati del controllo delle risorse.

La console locale visualizza anche il numero di errori e avvisi accanto all'opzione del menu di controllo delle risorse.

Esecuzione dei comandi Storage Gateway sulla console locale per un gateway Amazon EC2

La Gateway di archiviazione AWS console aiuta a fornire un ambiente sicuro per la configurazione e la diagnosi dei problemi relativi al gateway. Utilizzando i comandi della console, è possibile eseguire attività di manutenzione come il salvataggio delle tabelle di routing o la connessione a. Supporto

Per eseguire un comando di diagnostica o di configurazione

1. Accedere alla console locale del gateway. Per istruzioni, consulta Accesso alla console locale del gateway Amazon EC2.
2. Dal menu principale Attivazione dell'AWS appliance: configurazione, inserisci il numero corrispondente per selezionare Console del Gateway.
3. Dal prompt dei comandi della console del gateway, immettere **h**.

   La console mostra il menu COMANDI DISPONIBILI che elenca i comandi disponibili:

Comando	Funzione
dig	Raccogli l'output da dig per la risoluzione dei problemi DNS.
Esci	Torna al menu di configurazione.
h	Visualizza l'elenco dei comandi disponibili.
ifconfig	Visualizza o configura le interfacce di rete.

Comando	Funzione
	Note Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata. Per istruzioni, vedere Configurazione delle impostazioni della rete gateway Configurazione delle impostazioni .
ip	Mostra/manipola routing, dispositivi e tunnel. **Note** Si consiglia di configurare le impostazioni di rete o IP utilizzando la console Storage Gateway o l'opzione del menu della console locale dedicata. Per istruzioni, vedere Configurazione delle impostazioni della rete gateway delle impostazioni della rete gateway.
iptables	Strumento di amministrazione per il filtraggio dei IPv4 pacchetti e NAT.
ncport	Verifica la connettività a una porta TCP specifica su una rete.
nping	Raccogli l'output da nping per la risoluzione dei problemi di rete.
open-support-channel	Connect to AWS Support.
save-iptables	Tabelle IP persistenti.

Comando	Funzione
save-routing-table	Salva la voce della tabella di routing appena aggiunta.
tcptraceroute	Raccogli l'output del traceroute sul traffico TCP verso una destinazione.

4. Dal prompt dei comandi della console del gateway, immettere il comando corrispondente alla funzione che si desidera utilizzare e seguire le istruzioni.

Per informazioni su un comando, digitate **`man`** + *`command name`* al prompt dei comandi.

Configurazione delle impostazioni di rete del gateway Amazon EC2

Puoi visualizzare e configurare le impostazioni di rete per il tuo Amazon EC2 File Gateway utilizzando la console locale del gateway.

Per configurare le impostazioni di rete

1. Accedi alla console locale sul tuo Amazon EC2 File Gateway. Per istruzioni, consulta Accesso alla console locale del gateway Amazon EC2.
2. Dal menu principale AWS Appliance Activation - Configuration, inserisci il numero corrispondente per selezionare Network Configuration.
3. Dal menu Attivazione dell'AWS appliance - Configurazione di rete, immettete il numero corrispondente all'operazione che desiderate eseguire:

   - Modifica configurazione DNS: la console locale del gateway mostra gli adattatori disponibili per i server DNS primari e secondari. La console richiede quindi di fornire il nuovo indirizzo IP.
   - Visualizza la configurazione DNS: la console locale del gateway mostra gli adattatori disponibili per i server DNS primari e secondari.
   - Configura nome host: la console locale del gateway richiede di scegliere se il gateway utilizzerà un nome host statico specificato dall'utente o se acquisirà automaticamente un nome host tramite DCHP o rDNS.

> **Note**
>
> Se si sceglie di configurare un nome host statico per il gateway, è necessario creare un record A nel sistema DNS che punti l'indirizzo IP del gateway al relativo nome host statico.

- Visualizza la configurazione del nome host: la console locale del gateway mostra il nome host, la modalità di acquisizione, il dominio e il realm di Active Directory per il tuo Amazon EC2 File Gateway.

Spegnimento della macchina virtuale gateway

Potrebbe essere necessario arrestare o riavviare la macchina virtuale per la manutenzione, ad esempio durante l'applicazione di una patch al tuo hypervisor. Le macchine virtuali gateway locali vengono disattivate utilizzando l'interfaccia dell'hypervisor e le istanze Amazon EC2 utilizzando la console Amazon EC2.

> **Important**
>
> Se arresti e avvii un gateway Amazon EC2 che utilizza l'archiviazione temporanea, il gateway sarà definitivamente offline. Questo accade perché il disco di storage fisico viene sostituito. Non esiste alcuna soluzione alternativa per questo problema. L'unica soluzione è eliminare il gateway e attivarne uno nuovo su una nuova istanza EC2.

Sostituzione del tuo una nuova istanza FSx

Puoi sostituire un esistente con una nuova istanza man mano che le esigenze di dati e prestazioni aumentano o se ricevi una AWS notifica per la migrazione del gateway. Potrebbe essere necessario eseguire questa operazione se desideri spostare il gateway su una piattaforma host migliore o su istanze Amazon EC2 più recenti o aggiornare l'hardware del server sottostante.

> **Important**
>
> Utilizzare queste istruzioni solo per la migrazione delle appliance gateway che eseguono la versione 1.x. Non è possibile utilizzarle per migrare i dispositivi gateway che eseguono versioni precedenti.

> **Note**
>
> La migrazione può essere eseguita solo tra gateway dello stesso tipo. Ad esempio, non è possibile migrare impostazioni o dati da un FSx File Gateway a un S3 File Gateway.

Per sostituire il gateway FSx File Gateway con una nuova istanza con un disco di cache vuoto e un nuovo ID Gateway:

1. Arresta tutte le applicazioni che stanno scrivendo sull'esistente . Verifica che la `CachePercentDirty` metrica nella scheda Monitoraggio sia quella indicata `0` prima di configurare le associazioni di file system sul nuovo gateway.
2. Utilizzate il AWS Command Line Interface pulsante (AWS CLI) per raccogliere e salvare le informazioni di configurazione relative al vostro FSx esistente e ai file system associati effettuando le seguenti operazioni:

   a. Salvate le informazioni di configurazione del gateway per .

   ```
   aws storagegateway describe-gateway-information --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   Questo comando genera un blocco JSON che contiene metadati sul gateway, come il nome, le interfacce di rete, il fuso orario configurato e il relativo stato (se il gateway è in esecuzione).

   b. Salva le impostazioni Server Message Block (SMB) di S3 File Gateway File . FSx

   ```
   aws storagegateway describe-smb-settings --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

Questo comando genera un blocco JSON che contiene il nome di dominio di Microsoft Active Directory a cui è unito il gateway.

c. Salva le informazioni sulla condivisione dei file per ogni file system associato a FSx :

Utilizzate il seguente comando per ogni file system associato.

```
aws storagegateway describe-file-system-associations --file-system-
association-arn-list "arn:aws:storagegateway:us-east-2:123456789012:fs-
association/fsa-987A654B"
```

Questo comando genera un blocco JSON che contiene metadati sul file system, ad esempio la posizione ARN, la destinazione del registro di controllo, gli attributi di aggiornamento della cache, gli indirizzi IP configurati e i tag.

3. Crea un nuovo con le stesse impostazioni e configurazioni del vecchio gateway. Se necessario, fai riferimento alle informazioni salvate nel passaggio 2.
4. Create nuove associazioni di file system per il nuovo gateway con le stesse impostazioni e configurazioni dei file system configurati sul vecchio gateway. Se necessario, fate riferimento alle informazioni salvate nel passaggio 2.
5. Verificate che il nuovo gateway funzioni correttamente, quindi rimappate/trasferite i client dai vecchi file system ai nuovi file system nel modo più adatto al vostro ambiente.
6. Verifica che il nuovo gateway funzioni correttamente, quindi elimina il vecchio gateway dalla console Storage Gateway.

> **Important**
>
> Prima di eliminare un File Gateway, assicurati che non ci siano applicazioni attualmente in scrittura nella cache di quel gateway. L'eliminazione di un gateway in uso può comportare una perdita di dati.

> **Warning**
>
> Un gateway eliminato non può più essere recuperato.

7. Elimina la vecchia macchina virtuale gateway o l'istanza Amazon EC2.

Eliminazione del gateway e rimozione delle risorse associate

Se non si intende continuare a utilizzarlo, un gateway può essere eliminato con le risorse a esso associate. La rimozione delle risorse non più utili consente di evitarne gli addebiti e quindi di ridurre la fattura mensile.

Quando si elimina un gateway, questo non viene più visualizzato nella console di Gateway di archiviazione AWS gestione e le relative connessioni al dei file vengono chiuse. Pur essendo la procedura di eliminazione uguale per tutti i tipi di gateway, per la rimozione delle risorse associate occorre seguire istruzioni specifiche, distinte in base al tipo di gateway da eliminare e all'host su cui è distribuito.

Puoi eliminare un gateway a livello di codice oppure utilizzando la console Storage Gateway. Seguono informazioni su come eliminare un gateway utilizzando la console Storage Gateway. Per eliminare un gateway in modo programmatico, consulta Documentazione di riferimento delle API Gateway di archiviazione AWS.

Eliminazione del gateway tramite la console Storage Gateway

La procedura di eliminazione è la stessa per tutti i tipi di gateway. Tuttavia, per rimuovere le risorse associate possono rendersi necessarie operazioni aggiuntive, distinte in base al tipo di gateway da eliminare e all'host di distribuzione. Una volta rimosse, le risorse inutilizzate non comporteranno ulteriori costi.

> **Note**
>
> Nel caso di gateway distribuiti su un'istanza Amazon EC2, l'istanza resta disponibile finché non viene eliminata.
> Nel caso di gateway distribuiti su una macchina virtuale (VM), dopo l'eliminazione del gateway la VM resta disponibile nell'ambiente di virtualizzazione. Per rimuovere la macchina virtuale, utilizzare il client VMware vSphere, Microsoft Hyper-V Manager o il client Linux Kernel-based Virtual Machine (KVM) per connettersi all'host e rimuovere la macchina virtuale. Non è possibile riutilizzare la VM di un gateway eliminato per attivare un nuovo gateway.

Come eliminare un gateway

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.

2. Scegli Gateway, quindi seleziona uno o più gateway da eliminare.
3. Per Actions (Operazioni), scegli Delete stack (Elimina stack). Viene visualizzata la finestra di dialogo di conferma.

> **Warning**
>
> Prima di eseguire questa operazione, bisogna accertarsi che non vi siano applicazioni in fase di scrittura sui volumi del gateway. L'eliminazione di un gateway in uso può comportare una perdita di dati. Un gateway eliminato non può più essere recuperato.

4. Verifica di voler eliminare i gateway specificati, quindi digita la parola delete nella casella di conferma e scegli Elimina.
5. (Facoltativo) Se desideri fornire un feedback sul gateway eliminato, completa la finestra di dialogo di feedback, quindi scegli Invia. Altrimenti, seleziona Salta.

> **Important**
>
> Non pagherai più i costi del software dopo aver eliminato un gateway, ma risorse come il bucket Amazon S3 e le istanze Amazon EC2 persistono. È possibile rimuovere l'istanza Amazon EC2 del gateway dopo la rimozione del gateway di file.

Prestazioni e ottimizzazione

Questa sezione descrive linee guida e best practice per ottimizzare le prestazioni di File Gateway.

Argomenti

Linee guida di base sulle prestazioni per FSx

In questa sezione, puoi trovare indicazioni per il provisioning dell'hardware per la tua macchina virtuale FSx File Gateway. Le configurazioni di istanza elencate nella tabella sono esempi e vengono fornite come riferimento.

Per prestazioni ottimali, la dimensione del disco della cache deve essere ottimizzata in base alle dimensioni del set di lavoro attivo. L'utilizzo di più dischi locali per la cache aumenta le prestazioni in scrittura parallelizzando l'accesso ai dati e comportando maggiori IOPS.

> **Note**
>
> Non è consigliabile utilizzare lo storage temporaneo. Per informazioni sull'utilizzo dello storage temporaneo, consulta Utilizzo dello storage temporaneo con i gateway EC2.
> Il limite di dimensione suggerito per le singole directory nei file system di Gateway è di 10.000 file per directory. È possibile utilizzare File Gateway con directory che contengono più di 10.000 file, ma le prestazioni potrebbero risentirne.

Nelle tabelle seguenti, le operazioni di lettura di accesso alla cache vengono lette dai dati dei file che vengono serviti dalla cache. Le operazioni di mancata lettura della cache vengono lette dai dati dei file forniti da Amazon FSx for Windows File Server.

La tabella seguente mostra un esempio di configurazione di FSx File Gateway.

FSx Prestazioni di File Gateway sui client Windows

Configurazione di esempio	Protocollo	Velocità effettiva di scrittura (dimensioni del file 1 GB)	Velocità effettiva di accessi alla cache	Velocità effettiva di mancata lettura della cache
Disco root: 80 GB, io1 SSD, 4.000 IOPS Dischi cache: 2 x 2 TiB NVME Prestazioni di rete minime: 10 Gbps Processore: 32 vCPU | RAM: 244 GB	SMBv3 - 1 filo	162 MiB/sec (1,4 Gbps)	403 MiB/sec (3,4 Gbps)	288 MiB/sec (2,4 Gbps)
	SMBv3 - 8 thread	511 MiB/sec (4,3 Gbps)	571 MiB/sec (4,8 Gbps)	567 MiB/sec (4,8 Gbps)

> **Note**
>
> Le prestazioni potrebbero variare in base alla configurazione della piattaforma host e alla larghezza di banda della rete. Le prestazioni di velocità effettiva di scrittura diminuiscono con la dimensione del file, con la velocità massima raggiungibile per file di piccole dimensioni (meno di 32 MiB) pari a 16 file al secondo.

Ottimizzazione delle prestazioni del gateway

Puoi trovare le informazioni su come ottimizzare le prestazioni del gateway. Le linee guida sono basate sull'aggiunta di risorse al gateway e sull'aggiunta di risorse al server dell'applicazione.

Aggiungere risorse al gateway

È possibile ottimizzare le prestazioni del gateway aggiungendo risorse al gateway in uno o più dei seguenti modi.

Utilizzare dischi a elevate prestazioni

Per ottimizzare le prestazioni del gateway, è possibile aggiungere dischi ad alte prestazioni come unità a stato solido (SSDs) e un controller. NVMe È anche possibile collegare dischi virtuali alla macchina virtuale direttamente da una SAN (Storage Area Network) piuttosto che da Microsoft Hyper-V NTFS. Il miglioramento delle prestazioni del disco si traduce in genere in una migliore velocità di trasmissione e in un maggior numero di input/output operazioni al secondo (IOPS). Per informazioni sull'aggiunta di dischi, vedere. Configurazione di una memoria cache aggiuntiva

Per misurare il throughput, utilizzare i parametri `ReadBytes` e `WriteBytes` con la statistica di `Samples` Amazon CloudWatch . Ad esempio, le statistiche `Samples` del parametro `ReadBytes` in un periodo di 5 minuti divisi 300 secondi forniscono gli IOPS. In generale, quando si prendono in esame questi parametri per un gateway, cercare un throughput basso e andamenti IOPS bassi per indicare colli di bottiglia correlati al disco.

> **Note**
>
> CloudWatch le metriche non sono disponibili per tutti i gateway. Per informazioni sui parametri del gateway, consulta Monitoraggio di FSx.

Aggiungere risorse CPU all'host del gateway

Il requisito minimo per un host server gateway è rappresentato da quattro processori virtuali. Per ottimizzare le prestazioni del gateway, confermare che i quattro processori virtuali assegnati alla macchina virtuale del gateway sono supportati da quattro core. Inoltre, conferma di non aver sottoscritto un numero di sottoscrizioni superiore a quello CPUs del server host.

Quando ne aggiungete altri CPUs al server host del gateway, aumentate la capacità di elaborazione del gateway. In questo modo il gateway può gestire, in parallelo, sia l'archiviazione dei dati dall'applicazione allo storage locale sia il caricamento di questi dati S3 per Windows File Server. CPUs Inoltre, aiuta a garantire che il gateway riceva risorse CPU sufficienti quando l'host è condiviso con altri. VMs Fornire un numero sufficiente di risorse CPU ha l'effetto di migliorare il throughput generale.

Storage Gateway supporta l'utilizzo di 24 CPUs nel server host gateway. È possibile utilizzare 24 CPUs per migliorare in modo significativo le prestazioni del gateway. Ti consigliamo la seguente configurazione gateway per il tuo server host gateway:

- 24 CPUs.
- 16 GiB di RAM riservata per i gateway di file
  - 16 GiB di RAM riservata per gateway con dimensioni della cache fino a 16 TiB
  - 32 GiB di RAM riservata per gateway con dimensioni della cache da 16 TiB a 32 TiB
  - 48 GiB di RAM riservata per gateway con dimensioni della cache da 32 TiB a 64 TiB
- Disco 1 collegato a un controller 1 paravirtuale per essere usato come cache gateway come segue:
  - SSD che utilizza un NVMe controller.
- Adattatore di rete 1 configurato sulla rete macchina virtuale 1:
  - Usa la rete VM 1 e aggiungi VMXnet3 (10 Gbps) da utilizzare per l'ingestione.
- Adattatore di rete 2 configurato sulla rete macchina virtuale 2:
  - Usa la rete VM 2 e aggiungi un VMXnet3 (10 Gbps) da utilizzare per la connessione. AWS

Supportare dischi virtuali gateway con dischi fisici separati

Quando si esegue il provisioning dei dischi gateway, si consiglia vivamente di non effettuare il provisioning di dischi locali per lo storage locale che utilizzano lo stesso disco di archiviazione fisico sottostante. Ad esempio, per VMware ESXi, le risorse di archiviazione fisica sottostanti sono rappresentate come un archivio dati. Quando si distribuisce la macchina virtuale del gateway, si sceglie un datastore in cui archiviare i file VM. Quando viene effettuato il provisioning di un disco virtuale (ad esempio, come buffer di caricamento), è possibile archiviare il disco virtuale nello stesso datastore della macchina virtuale o in un datastore differente.

Se si dispone di più di un datastore, è consigliabile scegliere un datastore per ogni tipo di storage locale che si sta creando. Un datastore che è supportato da un solo disco fisico sottostante può offrire prestazioni non soddisfacenti. Un esempio è quando questo disco viene usato per supportare sia lo storage della cache che il buffer di caricamento in una configurazione del gateway. Analogamente, un datastore supportato da una configurazione RAID con prestazioni minori, ad esempio RAID 1, può portare a prestazioni mediocri.

Aggiungere risorse per l'ambiente applicativo

Aumentare la larghezza di banda tra l'applicazione server e il gateway

Per ottimizzare le prestazioni del gateway, garantire che la larghezza di banda di rete tra l'applicazione e il gateway sia in grado di far fronte alle esigenze dell'applicazione. È possibile utilizzare le `WriteBytes` metriche `ReadBytes` e del gateway per misurare la velocità totale dei dati.

Per l'applicazione, confrontare il throughput misurato con il throughput desiderato. Se il throughput misurato è inferiore al throughput desiderato, aumentando la larghezza di banda tra l'applicazione e il gateway è possibile migliorare le prestazioni se la rete è il collo di bottiglia. Analogamente, è possibile aumentare la larghezza di banda tra la macchina virtuale e i tuoi dischi locali, se non sono collegati direttamente.

Aggiungere risorse CPU per l'ambiente applicativo

Se l'applicazione può utilizzare risorse CPU aggiuntive, aggiungerne altre CPUs può aiutare l'applicazione a scalare il carico. I/O

Alcune operazioni sui file su FSx File Gateway, come la ridenominazione delle cartelle di primo livello o la modifica delle autorizzazioni, possono comportare più operazioni sui file che comportano un I/O carico elevato sul file system FSx per Windows File Server. Se il file system non dispone di risorse prestazionali sufficienti per il carico di lavoro, il file system potrebbe eliminare le copie shadow perché dà priorità alla disponibilità per la conservazione continua I/O rispetto alla conservazione delle copie shadow storiche.

Nella FSx console Amazon, consulta la pagina Monitoraggio e prestazioni per verificare se il provisioning del file system è insufficiente. In tal caso, puoi passare allo storage SSD, aumentare la capacità di throughput o aumentare gli IOPS SSD per gestire il tuo carico di lavoro.

Massimizzazione del throughput di S3 File Gateway

Le sezioni seguenti descrivono le best practice per massimizzare il throughput tra i client NFS e SMB, S3 File Gateway e Amazon S3. Le indicazioni fornite in ogni sezione contribuiscono in modo incrementale a migliorare il throughput complessivo. Sebbene nessuna di queste raccomandazioni sia obbligatoria e non siano interdipendenti, sono state selezionate e ordinate in modo logico che consente di testare e ottimizzare le implementazioni Supporto di S3 File Gateway. Durante

l'implementazione e il test di questi suggerimenti, tieni presente che ogni implementazione di S3 File Gateway è unica, quindi i risultati possono variare.

S3 File Gateway fornisce un'interfaccia di file per archiviare e recuperare oggetti Amazon S3 utilizzando i protocolli di file NFS o SMB standard del settore, con una mappatura 1:1 nativa tra file e oggetto. Implementa S3 File Gateway come macchina virtuale in locale nel tuo ambiente KVM VMware Microsoft Hyper-V o Linux o nel cloud come AWS istanza Amazon EC2. S3 File Gateway non è progettato per fungere da sostituto completo del NAS aziendale. S3 File Gateway emula un file system, ma non è un file system. L'utilizzo di Amazon S3 come storage backend durevole crea un sovraccarico aggiuntivo per ogni I/O operazione, quindi la valutazione delle prestazioni di S3 File Gateway rispetto a un NAS o un file server esistente non è un confronto equivalente.

Implementa il gateway nella stessa posizione dei tuoi client

Ti consigliamo di implementare l'appliance virtuale S3 File Gateway in una posizione fisica con la minore latenza di rete possibile tra l'appliance e i client NFS o SMB. Quando scegli una posizione per il gateway, considera quanto segue:

- Una latenza di rete inferiore rispetto al gateway può contribuire a migliorare le prestazioni dei client NFS o SMB.
- S3 File Gateway è progettato per tollerare una latenza di rete più elevata tra il gateway e Amazon S3 rispetto a quella tra il gateway e i client.
- Per le istanze S3 File Gateway distribuite in Amazon EC2, consigliamo di mantenere il gateway e i client NFS o SMB nello stesso gruppo di collocamento. Per ulteriori informazioni, consulta i gruppi di posizionamento per le tue istanze Amazon EC2 nella Amazon Elastic Compute Cloud User Guide.

Riduci i colli di bottiglia causati dai dischi lenti

Ti consigliamo di monitorare la `IoWaitPercent` CloudWatch metrica per identificare i rallentamenti nelle prestazioni che possono derivare dalla lentezza dei dischi di archiviazione sul tuo S3 File Gateway. Quando tenti di ottimizzare i problemi di prestazioni relativi al disco, considera quanto segue:

- `IoWaitPercent`riporta la percentuale di tempo in cui la CPU è in attesa di una risposta dai dischi root o cache.

- Quando `IoWaitPercent` è superiore al 5-10%, in genere indica un rallentamento delle prestazioni del gateway causato da dischi con prestazioni insufficienti. Questa metrica dovrebbe avvicinarsi il più possibile allo 0%, il che significa che il gateway non è mai in attesa sul disco, il che aiuta a ottimizzare le risorse della CPU.
- Puoi controllare `IoWaitPercent` nella scheda Monitoraggio della console Storage Gateway o configurare gli CloudWatch allarmi consigliati per avvisarti automaticamente se la metrica supera una soglia specifica. Per ulteriori informazioni, consulta Creazione di CloudWatch allarmi consigliati per il gateway.
- Per ridurre al minimo i dischi root e cache del gateway, consigliamo di utilizzare uno NVMe o l'SSD. `IoWaitPercent`

Modifica l'allocazione delle risorse delle macchine virtuali per CPU, RAM e dischi cache

Quando si tenta di ottimizzare il throughput per S3 File Gateway, è importante allocare risorse sufficienti alla macchina virtuale del gateway, inclusi CPU, RAM e dischi di cache. I requisiti minimi di risorse virtuali di CPUs 4,16 GB di RAM e 150 GB di storage nella cache sono in genere adatti solo per carichi di lavoro più piccoli. Quando si allocano risorse virtuali per carichi di lavoro più grandi, si consiglia quanto segue:

- Aumenta il numero allocato tra 16 e 48, CPUs a seconda dell'utilizzo tipico della CPU generato da S3 File Gateway. Puoi monitorare l'utilizzo della CPU utilizzando la `UserCpuPercent` metrica. Per ulteriori informazioni, consulta Comprendere le metriche del gateway.
- Aumenta la RAM allocata tra 32 e 64 GB.

> **Note**
>
> S3 File Gateway non può utilizzare più di 64 GB di RAM.

- NVMe Utilizzate il nostro SSD per i dischi root e il disco di cache e dimensionate i dischi di cache in modo da allinearli al set di dati di picco che intendete scrivere sul gateway. Per ulteriori informazioni, consulta le best practice di dimensionamento della cache di S3 File Gateway sul canale ufficiale Amazon Web Services YouTube .
- Aggiungi almeno 4 dischi di cache virtuale al gateway, anziché utilizzare un unico disco di grandi dimensioni. Più dischi virtuali possono migliorare le prestazioni anche se condividono lo stesso

disco fisico sottostante, ma i miglioramenti sono in genere maggiori quando i dischi virtuali si trovano su dischi fisici sottostanti diversi.

Ad esempio, se desideri distribuire 12 TB di cache, puoi utilizzare una delle seguenti configurazioni:

- 4 dischi cache da 3 TB
- 8 dischi cache da 1,5 TB
- 12 dischi cache da 1 TB

Oltre alle prestazioni, ciò consente una gestione più efficiente della macchina virtuale nel tempo. Man mano che il carico di lavoro cambia, è possibile aumentare in modo incrementale il numero di dischi di cache e la capacità complessiva della cache, mantenendo al contempo le dimensioni originali di ogni singolo disco virtuale per preservare l'integrità del gateway.

Per ulteriori informazioni, vedere Decidere la quantità di storage su disco locale.

Quando distribuisci S3 File Gateway come istanza Amazon EC2, considera quanto segue:

- Il tipo di istanza scelto può influire in modo significativo sulle prestazioni del gateway. Amazon EC2 offre un'ampia flessibilità per regolare l'allocazione delle risorse per l'istanza S3 File Gateway.
- Per i tipi di istanze Amazon EC2 consigliati per S3 File Gateway, consulta Requisiti per i tipi di istanze Amazon EC2.
- Puoi modificare il tipo di istanza Amazon EC2 che ospita un S3 File Gateway attivo. Ciò consente di regolare facilmente la generazione di hardware Amazon EC2 e l'allocazione delle risorse per trovare un rapporto ideale. price-to-performance Per modificare il tipo di istanza, utilizza la seguente procedura nella console Amazon EC2:

  1. Arresta l'istanza Amazon EC2.
  2. Cambia il tipo di istanza Amazon EC2.
  3. Accendi l'istanza Amazon EC2.

> **Note**
>
> L'arresto di un'istanza che ospita un S3 File Gateway interromperà temporaneamente l'accesso alla condivisione dei file. Assicurati di pianificare una finestra di manutenzione, se necessario.

- Il price-to-performance rapporto di un'istanza Amazon EC2 si riferisce alla potenza di calcolo ottenuta al prezzo pagato. In genere, le istanze Amazon EC2 di nuova generazione offrono il rapporto price-to-performance migliore, con hardware più recente e prestazioni migliorate a un costo relativamente inferiore rispetto alle generazioni precedenti. Fattori come il tipo di istanza, la regione e i modelli di utilizzo influiscono su questo rapporto, quindi è importante selezionare l'istanza giusta per il carico di lavoro specifico per ottimizzare il rapporto costo/efficacia.

Regola il livello di sicurezza delle PMI

Il SMBv3 protocollo consente sia la firma SMB che la crittografia SMB, con alcuni compromessi in termini di prestazioni e sicurezza. Per ottimizzare il throughput, è possibile regolare il livello di sicurezza SMB del gateway per specificare quali di queste funzionalità di sicurezza vengono applicate alle connessioni client. Per ulteriori informazioni, consulta Impostare un livello di sicurezza per il gateway.

Quando regolate il livello di sicurezza SMB, tenete presente quanto segue:

- Il livello di sicurezza predefinito per S3 File Gateway è Enforce encryption. Questa impostazione applica sia la crittografia che la firma per le connessioni client SMB alle condivisioni di file del gateway, il che significa che tutto il traffico dal client al gateway è crittografato. Questa impostazione non influisce sul traffico dal gateway a AWS, che è sempre crittografato.

  Il gateway limita ogni connessione client crittografata a una singola vCPU. Ad esempio, se si dispone di un solo client crittografato, tale client sarà limitato a una sola vCPU, anche se 4 o più v CPUs sono allocate al gateway. Per questo motivo, la velocità effettiva per le connessioni crittografate da un singolo client a S3 File Gateway è in genere limitata tra 40-60 MB/s.
- Se i requisiti di sicurezza consentono un approccio più rilassato, è possibile modificare il livello di sicurezza impostandolo su Client negotiated, che disabiliterà la crittografia SMB e applicherà solo la firma SMB. Con questa impostazione, le connessioni client al gateway possono utilizzare più v, il che in genere si traduce in un aumento delle CPUs prestazioni di throughput.

> **Note**
>
> Dopo aver modificato il livello di sicurezza SMB per S3 File Gateway, è necessario attendere che lo stato della condivisione dei file passi da Aggiornamento a Disponibile nella console Storage Gateway, quindi disconnettere e ricollegare i client SMB affinché la nuova impostazione abbia effetto.

Utilizza più thread e client per parallelizzare le operazioni di scrittura

È difficile ottenere le massime prestazioni di throughput con un S3 File Gateway che utilizza un solo client NFS o SMB per scrivere un file alla volta, perché la scrittura sequenziale da un singolo client è un'operazione a thread singolo. Consigliamo invece di utilizzare più thread di ogni client NFS o SMB per scrivere più file in parallelo e di utilizzare più client NFS o SMB contemporaneamente sul tuo S3 File Gateway per massimizzare il throughput del gateway.

L'utilizzo di più thread può migliorare significativamente le prestazioni. Tuttavia, l'utilizzo di più thread richiede più risorse di sistema, il che può influire negativamente sulle prestazioni se il gateway non è dimensionato per soddisfare l'aumento del carico. In un'implementazione tipica, ci si può aspettare di ottenere migliori prestazioni di throughput aggiungendo più thread e client, fino a raggiungere i limiti massimi di hardware e larghezza di banda per il gateway. Ti consigliamo di sperimentare diversi numeri di thread per trovare l'equilibrio ottimale tra velocità e utilizzo delle risorse di sistema per la tua specifica configurazione hardware e di rete.

Considerate le seguenti informazioni sugli strumenti più comuni che possono aiutarvi a testare la configurazione del thread e del client:

- Puoi testare le prestazioni di scrittura multithread utilizzando strumenti come robocopy per copiare un set di file in una condivisione di file sul tuo gateway. Per impostazione predefinita, robocopy utilizza 8 thread per copiare i file, ma è possibile specificare fino a 128 thread.

  Per usare più thread con robocopy, aggiungi lo `/MT:n` switch al tuo comando, n dov'è il numero di thread che vuoi usare. Esempio:

  ```
  robocopy C:\source D:\destination /MT:64
  ```

  Questo comando utilizzerà 64 thread per l'operazione di copia.

  > **Note**
  >
  > Si sconsiglia di utilizzare Windows Explorer per trascinare e rilasciare i file durante il test della velocità effettiva massima, poiché questo metodo è limitato a un singolo thread e copia i file in sequenza.

  Per ulteriori informazioni, consulta robocopy sul sito Web Microsoft Learn.

- Puoi anche eseguire test utilizzando strumenti comuni di benchmarking dello storage come DISKSPD o FIO. Questi strumenti offrono opzioni per regolare il numero di thread, la profondità di I/O e altri parametri in base ai requisiti specifici del carico di lavoro.

  DiskSpd consente di controllare il numero di thread utilizzando il parametro. `-t` Esempio:

  ```
  diskspd -c10G -d300 -r -w50 -t64 -o32 -b1M -h -L C:\testfile.dat
  ```

  Questo comando di esempio esegue le seguenti operazioni:

  - Crea un file di test da 10 GB () `-c1G`
  - Funziona per 300 secondi () `-d300`
  - Esegue un I/O test casuale con il 50% di letture e 50% di scrittura () `-r -w50`
  - Utilizza 64 thread () `-t64`
  - Imposta la profondità della coda a 32 per thread () `-o32`
  - Utilizza una dimensione del blocco di 1 MB () `-b1M`
  - Disattiva la memorizzazione nella cache hardware e software () `-h -L`

  Per ulteriori informazioni, consulta Utilizzare DISKSPD per testare le prestazioni di archiviazione del carico di lavoro sul sito Web Microsoft Learn.

- FIO utilizza il `numjobs` parametro per controllare il numero di thread paralleli. Esempio:

  ```
  fio --name=mixed_test --rw=randrw --rwmixread=70 --bs=1M -- iodepth=64
  --size=10G --runtime=300 --numjobs=64 --ioengine=libaio --direct=1 --
  group_reporting
  ```

  Questo comando di esempio esegue le seguenti operazioni:

  - Esegue un I/O test casuale (`--rw=randrw`)
  - Esegue il 70% di letture e il 30% di scrittura () `--rwmixread=70`
  - Utilizza una dimensione del blocco di 1 MB () `--bs=1M`
  - Imposta la I/O profondità su 64 () `--iodepth=64`
  - Test su un file da 10 GB (`--size=10G`)
  - Funziona per 5 minuti (`--runtime=300`)
  - Crea 64 lavori paralleli (thread) (`--numjobs=64`)
  - Utilizza un motore asincrono I/O () `--ioengine=libaio`
  - Raggruppa i risultati per un'analisi più semplice () `--group_reporting`

Per ulteriori informazioni, consultate la pagina man di fio Linux.

•

Disattiva l'aggiornamento automatico della cache

La funzionalità di aggiornamento automatico della cache consente a S3 File Gateway di aggiornare automaticamente i metadati, il che può aiutare a catturare eventuali modifiche apportate da utenti o applicazioni al set di file scrivendo direttamente nel bucket Amazon S3, anziché tramite il gateway. Per ulteriori informazioni, consulta Refreshing Amazon S3 bucket Object Cache.

Per ottimizzare il throughput del gateway, consigliamo di disattivare questa funzionalità nelle distribuzioni in cui tutte le letture e le scritture sul bucket Amazon S3 verranno eseguite tramite il tuo S3 File Gateway.

Quando configuri l'aggiornamento automatico della cache, considera quanto segue:

- Se devi utilizzare l'aggiornamento automatico della cache perché gli utenti o le applicazioni della tua distribuzione scrivono occasionalmente direttamente su Amazon S3, ti consigliamo di configurare l'intervallo di tempo più lungo possibile tra gli aggiornamenti, in modo che sia comunque pratico per le tue esigenze aziendali. Un intervallo di aggiornamento della cache più lungo aiuta a ridurre il numero di operazioni sui metadati che il gateway deve eseguire durante la navigazione nelle directory o la modifica dei file.

  Ad esempio: imposta l'aggiornamento automatico della cache su 24 ore, anziché 5 minuti, se ciò è tollerabile per il carico di lavoro.
- L'intervallo di tempo minimo è di 5 minuti. L'intervallo massimo è di 30 giorni.
- Se scegli di impostare un intervallo di aggiornamento della cache molto breve, ti consigliamo di testare l'esperienza di navigazione nelle directory per i tuoi client NFS e SMB. Il tempo necessario per aggiornare la cache del gateway può aumentare notevolmente a seconda del numero di file e sottodirectory nel bucket Amazon S3.

Aumenta il numero di thread di caricamento di Amazon S3

Per impostazione predefinita, S3 File Gateway apre 8 thread per il caricamento dei dati di Amazon S3, che fornisce una capacità di caricamento sufficiente per le distribuzioni più comuni. Tuttavia, è possibile che un gateway riceva dati dai client NFS e SMB a una velocità superiore a quella che può

caricare su Amazon S3 con la capacità standard di 8 thread, il che può far sì che la cache locale raggiunga il limite di archiviazione.

In circostanze specifiche, Supporto puoi aumentare il numero di thread di caricamento di Amazon S3 per il tuo gateway da 8 a 40, il che consente di caricare più dati in parallelo. A seconda della larghezza di banda e di altri fattori specifici della distribuzione, ciò può aumentare in modo significativo le prestazioni di caricamento e contribuire a ridurre la quantità di storage nella cache necessaria per supportare il carico di lavoro.

Ti consigliamo di utilizzare la `CachePercentDirty` CloudWatch metrica per monitorare la quantità di dati archiviati sui dischi di cache del gateway locale che non sono ancora stati caricati su Amazon S3 e di Supporto contattarci per determinare se l'aumento del numero del pool di thread di caricamento possa migliorare il throughput per il tuo S3 File Gateway. Per ulteriori informazioni, consulta Understanding gateway metrics.

> **Note**
>
> Questa impostazione consuma risorse aggiuntive della CPU del gateway. Si consiglia di monitorare l'utilizzo della CPU del gateway e di aumentare le risorse CPU allocate, se necessario.

Aumenta le impostazioni di timeout SMB

Quando S3 File Gateway copia file di grandi dimensioni in una condivisione di file SMB, la connessione client SMB può scadere dopo un periodo di tempo prolungato.

Consigliamo di estendere l'impostazione del timeout della sessione SMB per i client SMB a 20 minuti o più, a seconda delle dimensioni dei file e della velocità di scrittura del gateway. L'impostazione predefinita è 300 secondi o 5 minuti. Per ulteriori informazioni, vedi Il processo di backup del gateway non riesce o si verificano errori durante la scrittura sul gateway.

Attiva il blocco opportunistico per le applicazioni compatibili

Il blocco opportunistico, o «oplocks», è abilitato di default per ogni nuovo S3 File Gateway. Quando si utilizzano oplock con applicazioni compatibili, il client raggruppa più operazioni più piccole in operazioni più grandi, il che è più efficiente per il client, il gateway e la rete. Ti consigliamo di mantenere attivo il blocco opportunistico se utilizzi applicazioni che sfruttano la memorizzazione

nella cache locale lato client, come Microsoft Office, Adobe Suite e molte altre, perché può migliorare significativamente le prestazioni.

Se disattivi il blocco opportunistico, le applicazioni che supportano gli oplock in genere aprono file di grandi dimensioni (50 MB o più) molto più lentamente. Questo ritardo si verifica perché il gateway invia i dati in parti da 4 KB, il che si traduce in una velocità effettiva elevata I/O e bassa.

Regola la capacità del gateway in base alla dimensione del set di file di lavoro

Il parametro di capacità del gateway specifica il numero massimo di file per i quali il gateway memorizzerà i metadati nella cache locale. Per impostazione predefinita, la capacità del gateway è impostata su Small, il che significa che il gateway archivia i metadati per un massimo di 5 milioni di file. L'impostazione predefinita funziona bene per la maggior parte dei carichi di lavoro, anche se ci sono centinaia di milioni o addirittura miliardi di oggetti in Amazon S3, perché in una distribuzione tipica si accede attivamente solo a un piccolo sottoinsieme di file alla volta. Questo gruppo di file viene definito «set di lavoro».

Se il carico di lavoro accede regolarmente a un set di lavoro superiore a 5 milioni di file, il gateway dovrà eliminare frequentemente la cache, ossia piccole operazioni di I/O archiviate nella RAM e mantenute sul disco principale. Ciò può influire negativamente sulle prestazioni del gateway poiché il gateway recupera nuovi dati da Amazon S3.

Puoi monitorare la `IndexEvictions` metrica per determinare il numero di file i cui metadati sono stati rimossi dalla cache per fare spazio a nuove voci. Per ulteriori informazioni, consulta Understanding gateway metrics.

Si consiglia di utilizzare l'azione `UpdateGatewayInformation` API per aumentare la capacità del gateway in modo che corrisponda al numero di file del set di lavoro tipico. Per ulteriori informazioni, consulta UpdateGatewayInformation.

> **Note**
>
> L'aumento della capacità del gateway richiede RAM e capacità del disco root aggiuntive.
>
> - Le dimensioni ridotte (5 milioni di file) richiedono almeno 16 GB di RAM e 80 GB di disco root.
> - Medium (10 milioni di file) richiede almeno 32 GB di RAM e 160 GB di disco root.

- Le dimensioni grandi (20 milioni di file) richiedono 64 GB di RAM e 240 GB di disco root.

Important

La capacità del gateway non può essere ridotta.

Implementa più gateway per carichi di lavoro più grandi

Quando possibile, consigliamo di suddividere il carico di lavoro su più gateway, anziché consolidare molte condivisioni di file su un unico gateway di grandi dimensioni. Ad esempio, è possibile isolare una condivisione di file molto utilizzata su un gateway, raggruppando le condivisioni di file utilizzate meno frequentemente su un altro gateway.

Quando pianifichi una distribuzione con più gateway e condivisioni di file, considera quanto segue:

- Il numero massimo di condivisioni di file su un singolo gateway è 50, ma il numero di condivisioni di file gestite da un gateway può influire sulle prestazioni del gateway. Per ulteriori informazioni, vedere Guida alle prestazioni per gateway con più condivisioni di file.
- Le risorse su ogni S3 File Gateway sono condivise tra tutte le condivisioni di file, senza partizionamento.
- Una singola condivisione di file con un utilizzo intenso può influire sulle prestazioni di altre condivisioni di file sul gateway.

Note

Non è consigliabile creare più condivisioni di file mappate sulla stessa posizione Amazon S3 da più gateway, a meno che almeno una di esse non sia di sola lettura.
Le scritture simultanee sullo stesso file da più gateway sono considerate uno scenario di scrittura multipla, che può causare problemi di integrità dei dati.

Ottimizzazione di S3 File Gateway per i backup dei database SQL Server

I backup dei database sono un caso d'uso comune e consigliato per S3 File Gateway, che offre una conservazione conveniente a breve e lungo termine archiviando i backup del database in Amazon S3, con la possibilità di eseguire il ciclo di vita su livelli di storage più bassi, se necessario. Con questa soluzione, puoi ridurre la necessità di applicazioni di backup aziendali utilizzando strumenti integrati come SQL Server Management Studio e Oracle RMAN.

Le sezioni seguenti descrivono le migliori pratiche per ottimizzare l'implementazione di S3 File Gateway per prestazioni ottimizzate e un supporto conveniente per centinaia di terabyte di backup di database SQL. Le linee guida fornite in ogni sezione contribuiscono in modo incrementale a migliorare il throughput complessivo. Sebbene nessuna di queste raccomandazioni sia obbligatoria e non siano interdipendenti, sono state selezionate e ordinate in modo logico che consente di testare e ottimizzare le implementazioni Supporto di S3 File Gateway. Durante l'implementazione e il test di questi suggerimenti, tieni presente che ogni implementazione di S3 File Gateway è unica, quindi i risultati possono variare.

S3 File Gateway fornisce un'interfaccia di file per archiviare e recuperare oggetti Amazon S3 utilizzando i protocolli di file NFS o SMB standard del settore, con una mappatura 1:1 nativa tra file e oggetto. Implementa S3 File Gateway come macchina virtuale in locale nel tuo ambiente KVM VMware Microsoft Hyper-V o Linux o nel cloud come AWS istanza Amazon EC2. S3 File Gateway non è progettato per fungere da sostituto completo del NAS aziendale. S3 File Gateway emula un file system, ma non è un file system. L'utilizzo di Amazon S3 come storage backend durevole crea un sovraccarico aggiuntivo per ogni I/O operazione, quindi la valutazione delle prestazioni di S3 File Gateway rispetto a un NAS o un file server esistente non è un confronto equivalente.

Implementa il gateway nella stessa posizione dei server SQL

Ti consigliamo di implementare l'appliance virtuale S3 File Gateway in una posizione fisica con la minore latenza di rete possibile tra l'appliance e i server SQL. Quando scegli una posizione per il gateway, considera quanto segue:

- Una latenza di rete inferiore rispetto al gateway può contribuire a migliorare le prestazioni dei client SMB, come i server SQL.
- S3 File Gateway è progettato per tollerare una latenza di rete più elevata tra il gateway e Amazon S3 rispetto a quella tra il gateway e i client.

- Per le istanze S3 File Gateway distribuite in Amazon EC2, consigliamo di mantenere il gateway e i server SQL nello stesso gruppo di collocamento. Per ulteriori informazioni, consulta i gruppi di posizionamento per le tue istanze Amazon EC2 nella Amazon Elastic Compute Cloud User Guide.

Riduci i colli di bottiglia causati dai dischi lenti

Ti consigliamo di monitorare la `IoWaitPercent` CloudWatch metrica per identificare i rallentamenti nelle prestazioni che possono derivare dalla lentezza dei dischi di archiviazione sul tuo S3 File Gateway. Quando tenti di ottimizzare i problemi di prestazioni relativi al disco, considera quanto segue:

- `IoWaitPercent`riporta la percentuale di tempo in cui la CPU è in attesa di una risposta dai dischi root o cache.
- Quando `IoWaitPercent` è superiore al 5-10%, in genere indica un rallentamento delle prestazioni del gateway causato da dischi con prestazioni insufficienti. Questa metrica dovrebbe avvicinarsi il più possibile allo 0%, il che significa che il gateway non è mai in attesa sul disco, il che aiuta a ottimizzare le risorse della CPU.
- Puoi controllare `IoWaitPercent` nella scheda Monitoraggio della console Storage Gateway o configurare gli CloudWatch allarmi consigliati per avvisarti automaticamente se la metrica supera una soglia specifica. Per ulteriori informazioni, consulta Creazione di CloudWatch allarmi consigliati per il gateway.
- Per ridurre al minimo i dischi root e cache del gateway, consigliamo di utilizzare uno NVMe o l'SSD. `IoWaitPercent`

Regola l'allocazione delle risorse della macchina virtuale S3 File Gateway per CPU, RAM e dischi cache

Quando si tenta di ottimizzare il throughput per S3 File Gateway, è importante allocare risorse sufficienti alla macchina virtuale del gateway, inclusi CPU, RAM e dischi di cache. I requisiti minimi di risorse virtuali di CPUs 4,16 GB di RAM e 150 GB di storage nella cache sono in genere adatti solo per carichi di lavoro più piccoli. Quando si allocano risorse virtuali per carichi di lavoro più grandi, si consiglia quanto segue:

- Aumenta il numero allocato tra 16 e 48, CPUs a seconda dell'utilizzo tipico della CPU generato da S3 File Gateway. Puoi monitorare l'utilizzo della CPU utilizzando la `UserCpuPercent` metrica. Per ulteriori informazioni, consulta Comprendere le metriche del gateway.

- Aumenta la RAM allocata tra 32 e 64 GB.

  > **Note**
  >
  > S3 File Gateway non può utilizzare più di 64 GB di RAM.

- NVMe Utilizzate il nostro SSD per i dischi root e il disco di cache e dimensionate i dischi di cache in modo da allinearli al set di dati di picco che intendete scrivere sul gateway. Per ulteriori informazioni, consulta le best practice di dimensionamento della cache di S3 File Gateway sul canale ufficiale Amazon Web Services YouTube .
- Aggiungi almeno 4 dischi di cache virtuale al gateway, anziché utilizzare un unico disco di grandi dimensioni. Più dischi virtuali possono migliorare le prestazioni anche se condividono lo stesso disco fisico sottostante, ma i miglioramenti sono in genere maggiori quando i dischi virtuali si trovano su dischi fisici sottostanti diversi.

  Ad esempio, se desideri distribuire 12 TB di cache, puoi utilizzare una delle seguenti configurazioni:

  - 4 dischi cache da 3 TB
  - 8 dischi cache da 1,5 TB
  - 12 dischi cache da 1 TB

  Oltre alle prestazioni, ciò consente una gestione più efficiente della macchina virtuale nel tempo. Man mano che il carico di lavoro cambia, è possibile aumentare in modo incrementale il numero di dischi di cache e la capacità complessiva della cache, mantenendo al contempo le dimensioni originali di ogni singolo disco virtuale per preservare l'integrità del gateway.

  Per ulteriori informazioni, vedere Decidere la quantità di storage su disco locale.

Quando distribuisci S3 File Gateway come istanza Amazon EC2, considera quanto segue:

- Il tipo di istanza scelto può influire in modo significativo sulle prestazioni del gateway. Amazon EC2 offre un'ampia flessibilità per regolare l'allocazione delle risorse per l'istanza S3 File Gateway.
- Per i tipi di istanze Amazon EC2 consigliati per S3 File Gateway, consulta Requisiti per i tipi di istanze Amazon EC2.
- Puoi modificare il tipo di istanza Amazon EC2 che ospita un S3 File Gateway attivo. Ciò consente di regolare facilmente la generazione di hardware Amazon EC2 e l'allocazione delle risorse per trovare un rapporto ideale. price-to-performance Per modificare il tipo di istanza, utilizza la seguente procedura nella console Amazon EC2:

1. Arresta l'istanza Amazon EC2.
2. Cambia il tipo di istanza Amazon EC2.
3. Accendi l'istanza Amazon EC2.

> **Note**
>
> L'arresto di un'istanza che ospita un S3 File Gateway interromperà temporaneamente l'accesso alla condivisione dei file. Assicurati di pianificare una finestra di manutenzione, se necessario.

- Il price-to-performance rapporto di un'istanza Amazon EC2 si riferisce alla potenza di calcolo ottenuta al prezzo pagato. In genere, le istanze Amazon EC2 di nuova generazione offrono il rapporto price-to-performance migliore, con hardware più recente e prestazioni migliorate a un costo relativamente inferiore rispetto alle generazioni precedenti. Fattori come il tipo di istanza, la regione e i modelli di utilizzo influiscono su questo rapporto, quindi è importante selezionare l'istanza giusta per il carico di lavoro specifico per ottimizzare il rapporto costo/efficacia.

Migliora la produttività dei client SMB regolando il livello di sicurezza del tuo S3 File Gateway

Il SMBv3 protocollo consente sia la firma SMB che la crittografia SMB, con alcuni compromessi in termini di prestazioni e sicurezza. Per ottimizzare il throughput, è possibile regolare il livello di sicurezza SMB del gateway per specificare quali di queste funzionalità di sicurezza vengono applicate alle connessioni client. Per ulteriori informazioni, consulta Impostare un livello di sicurezza per il gateway.

Quando regolate il livello di sicurezza SMB, tenete presente quanto segue:

- Il livello di sicurezza predefinito per S3 File Gateway è Enforce encryption. Questa impostazione applica sia la crittografia che la firma per le connessioni client SMB alle condivisioni di file del gateway, il che significa che tutto il traffico dal client al gateway è crittografato. Questa impostazione non influisce sul traffico dal gateway a AWS, che è sempre crittografato.

  Il gateway limita ogni connessione client crittografata a una singola vCPU. Ad esempio, se si dispone di un solo client crittografato, tale client sarà limitato a una sola vCPU, anche se 4 o più v CPUs sono allocate al gateway. Per questo motivo, la velocità effettiva per le connessioni crittografate da un singolo client a S3 File Gateway è in genere limitata tra 40-60 MB/s.

- Se i requisiti di sicurezza consentono un approccio più rilassato, è possibile modificare il livello di sicurezza impostandolo su Client negotiated, che disabiliterà la crittografia SMB e applicherà solo la firma SMB. Con questa impostazione, le connessioni client al gateway possono utilizzare più v, il che in genere si traduce in un aumento delle CPUs prestazioni di throughput.

> **Note**
>
> Dopo aver modificato il livello di sicurezza SMB per S3 File Gateway, è necessario attendere che lo stato della condivisione dei file passi da Aggiornamento a Disponibile nella console Storage Gateway, quindi disconnettere e ricollegare i client SMB affinché la nuova impostazione abbia effetto.

Migliora la produttività dei client SMB suddividendo i backup SQL in più file

- È difficile ottenere le massime prestazioni di throughput con un S3 File Gateway: solo un server SQL scrive un file alla volta, perché la scrittura sequenziale da un singolo server SQL è un'operazione a thread singolo. Si consiglia invece di utilizzare più thread da ciascun server SQL per scrivere più file in parallelo e di utilizzare più server SQL contemporaneamente su S3 File Gateway per massimizzare il throughput del gateway. Con i backup SQL, la suddivisione dei backup in più file consente a ciascun file di utilizzare un thread separato, che scriverà più file contemporaneamente nella condivisione di file S3 File Gateway. Maggiore è il numero di thread, maggiore è la velocità effettiva che è possibile ottenere, fino ai limiti del gateway.
- SQL Server supporta la scrittura su più file contemporaneamente durante una singola operazione di backup. Ad esempio, è possibile specificare più destinazioni di file utilizzando i comandi T-SQL o SQL Server Management Studio (SSMS). Ogni file utilizza un thread separato per inviare dati dal server SQL alla condivisione di file del gateway. Questo approccio consente una migliore I/O velocità di trasmissione, che può migliorare in modo significativo la velocità e l'efficienza del backup.

Quando configuri i backup del server SQL, considera quanto segue:

- Suddividendo i backup in più file, gli amministratori di SQL Server possono ottimizzare i tempi di backup e gestire i backup di database di grandi dimensioni in modo più efficace.

- Il numero di file utilizzati dipende dalla configurazione dello storage e dai requisiti prestazionali del server. Per i database di grandi dimensioni, si consiglia di suddividere i backup in diversi file più piccoli tra 10 GB e 20 GB ciascuno.
- Non esiste un limite rigoroso al numero di file su cui SQL Server può scrivere durante un backup, ma considerazioni pratiche come l'architettura di archiviazione e la larghezza di banda della rete dovrebbero guidare questa scelta.

Per ulteriori informazioni, consulta:

- Esegui il backup di SQL Server il 43-67% più velocemente scrivendo su più file
- Archivia facilmente i tuoi backup di SQL Server in Amazon S3 utilizzando File Gateway

Previeni errori di copia di file di grandi dimensioni aumentando le impostazioni di timeout SMB

Quando S3 File Gateway copia file di backup SQL di grandi dimensioni in una condivisione di file SMB, la connessione client SMB può scadere dopo un periodo di tempo prolungato. Consigliamo di estendere l'impostazione del timeout della sessione SMB per i client SMB di SQL Server a 20 minuti o più, a seconda delle dimensioni dei file e della velocità di scrittura del gateway. L'impostazione predefinita è 300 secondi o 5 minuti. Per ulteriori informazioni, vedi Il processo di backup del gateway non riesce o si verificano errori durante la scrittura sul gateway.

Aumenta il numero di thread di caricamento di Amazon S3

Per impostazione predefinita, S3 File Gateway apre 8 thread per il caricamento dei dati di Amazon S3, che fornisce una capacità di caricamento sufficiente per le distribuzioni più comuni. Tuttavia, è possibile che un gateway riceva dati dai server SQL a una velocità superiore a quella che può caricare su Amazon S3 con la capacità standard di 8 thread, il che può far sì che la cache locale raggiunga il limite di archiviazione.

In circostanze specifiche, Supporto puoi aumentare il numero di thread di caricamento di Amazon S3 per il tuo gateway da 8 a 40, il che consente di caricare più dati in parallelo. A seconda della larghezza di banda e di altri fattori specifici della distribuzione, ciò può aumentare in modo significativo le prestazioni di caricamento e contribuire a ridurre la quantità di storage nella cache necessaria per supportare il carico di lavoro.

Ti consigliamo di utilizzare la `CachePercentDirty` CloudWatch metrica per monitorare la quantità di dati archiviati sui dischi di cache del gateway locale che non sono ancora stati caricati su Amazon S3 e di Supporto contattarci per determinare se l'aumento del numero del pool di thread di caricamento possa migliorare il throughput per il tuo S3 File Gateway. Per ulteriori informazioni, consulta Understanding gateway metrics.

> **Note**
>
> Questa impostazione consuma risorse aggiuntive della CPU del gateway. Si consiglia di monitorare l'utilizzo della CPU del gateway e di aumentare le risorse CPU allocate, se necessario.

Disattiva l'aggiornamento automatico della cache

La funzionalità di aggiornamento automatico della cache consente a S3 File Gateway di aggiornare automaticamente i metadati, il che può aiutare a catturare eventuali modifiche apportate da utenti o applicazioni al set di file scrivendo direttamente nel bucket Amazon S3, anziché tramite il gateway. Per ulteriori informazioni, consulta Refreshing Amazon S3 bucket Object Cache.

Per ottimizzare il throughput del gateway, consigliamo di disattivare questa funzionalità nelle distribuzioni in cui tutte le letture e le scritture sul bucket Amazon S3 verranno eseguite tramite il tuo S3 File Gateway.

Quando configuri l'aggiornamento automatico della cache, considera quanto segue:

- Se devi utilizzare l'aggiornamento automatico della cache perché gli utenti o le applicazioni della tua distribuzione scrivono occasionalmente direttamente su Amazon S3, ti consigliamo di configurare l'intervallo di tempo più lungo possibile tra gli aggiornamenti, in modo che sia comunque pratico per le tue esigenze aziendali. Un intervallo di aggiornamento della cache più lungo aiuta a ridurre il numero di operazioni sui metadati che il gateway deve eseguire durante la navigazione nelle directory o la modifica dei file.

  Ad esempio: imposta l'aggiornamento automatico della cache su 24 ore, anziché 5 minuti, se ciò è tollerabile per il carico di lavoro.
- L'intervallo di tempo minimo è di 5 minuti. L'intervallo massimo è di 30 giorni.
- Se scegli di impostare un intervallo di aggiornamento della cache molto breve, ti consigliamo di testare l'esperienza di navigazione nelle directory per i tuoi server SQL. Il tempo necessario per

aggiornare la cache del gateway può aumentare notevolmente a seconda del numero di file e sottodirectory nel bucket Amazon S3.

Implementa più gateway per supportare il carico di lavoro

Storage Gateway può supportare backup SQL per ambienti di grandi dimensioni con centinaia di database SQL, più SQL Server e centinaia di terabyte di dati di backup suddividendo il carico di lavoro su più gateway.

Quando pianifichi una distribuzione con più gateway e server SQL, considera quanto segue:

- Un singolo gateway può in genere caricare fino a 20 TB al giorno, con risorse hardware e larghezza di banda sufficienti. Puoi aumentare questo limite fino a 40 TB al giorno aumentando il numero di thread di caricamento di Amazon S3.
- Ti consigliamo di eseguire un proof-of-concept test per misurare le prestazioni e tenere conto di tutte le variabili della distribuzione. Dopo aver determinato il throughput di picco del carico di lavoro di backup SQL, puoi scalare il numero di gateway per soddisfare i tuoi requisiti.
- Consigliamo di progettare la soluzione pensando alla crescita, poiché il numero di database e le dimensioni dei database possono aumentare nel tempo. Per continuare a scalare e supportare un carico di lavoro crescente, puoi implementare gateway aggiuntivi in base alle esigenze.

Risorse aggiuntive per i carichi di lavoro di backup del database

- Archivia i backup di SQL Server in Amazon S3 utilizzando Gateway di archiviazione AWS
- Archivia facilmente i tuoi backup di SQL Server in Amazon S3 utilizzando File Gateway
- Utilizzo Gateway di archiviazione AWS per archiviare i backup dei database Oracle in Amazon S3
- Backup dei database Oracle su Amazon S3 su larga scala
- Integra un database SAP ASE in Amazon S3 utilizzando Gateway di archiviazione AWS
- Come viene utilizzato One AWS Hero Gateway di archiviazione AWS per il backup nel cloud
- Migliori pratiche per il dimensionamento della cache di S3 File Gateway

Sicurezza nello AWS Storage Gateway

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di un data center e di un'architettura di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra AWS te e te. Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi nel AWS cloud. AWS ti fornisce anche servizi che puoi utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità che si applicano a AWS Storage Gateway, vedere AWS Services in Scope by Compliance Program AWS .
- Sicurezza nel cloud: la responsabilità dell'utente è determinata dal AWS servizio utilizzato. 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 aiuta a comprendere come applicare il modello di responsabilità condivisa quando si usa Storage Gateway. Gli argomenti seguenti illustrano come configurare Storage Gateway per soddisfare gli obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le risorse dello Storage Gateway.

Protezione dei dati in AWS Storage Gateway

Il modello di responsabilità AWS condivisa modello di di si applica alla protezione dei dati in AWS Storage Gateway. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per maggiori informazioni sulla privacy dei dati, consulta le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al AWS Modello di responsabilità condivisa e GDPR nel AWS Blog sulla sicurezza.

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal

modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando si lavora con Storage Gateway o altro Servizi AWS utilizzando la console AWS CLI, l'API o AWS SDKs. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando si fornisce un URL a un server esterno, suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la richiesta al server.

Crittografia dei dati utilizzando AWS KMS

Amazon FSx File Gateway supporta la crittografia SMB fino alle più recenti specifiche SMB v3.1.1, tra cui AES 128 CCM e AES 128 GCM. I client compatibili si connetteranno automaticamente utilizzando la crittografia. Inoltre, FSx File Gateway utilizza la crittografia SMB quando comunica con FSx Windows File Server in. AWSÈ necessario configurare un Direct Connect collegamento e impostare politiche appropriate per consentire il passaggio del traffico SMB e del traffico di gestione verso. AWS AWS

Crittografia di un file system

Per informazioni, consulta la sezione Crittografia dei dati FSx in Amazon nella Guida FSx per l'utente di Amazon per Windows File Server.

Quando lo utilizzi AWS KMS per crittografare i tuoi dati, tieni presente quanto segue:

- I dati vengono crittografati nel cloud mentre sono inattivi. Cioè, i dati sono crittografati in . FSx
- Gli utenti IAM devono disporre delle autorizzazioni necessarie per chiamare le operazioni AWS KMS API. Per ulteriori informazioni, consulta Utilizzo delle policy IAM con AWS KMS nella Guida per gli sviluppatori di AWS Key Management Service .

> **Important**
>
> Quando usi una AWS KMS chiave per la crittografia lato server, devi scegliere una chiave simmetrica. Storage Gateway non supporta le chiavi asimmetriche. Per ulteriori informazioni, consulta Utilizzo di chiavi simmetriche e asimmetriche nella Guida per gli sviluppatori di AWS Key Management Service .

Per ulteriori informazioni su AWS KMS, consulta Cos'è? AWS Key Management Service

Gestione delle identità e degli accessi per AWS Storage Gateway

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse SGW. AWS IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell’accesso tramite policy
- Come funziona AWS Storage Gateway con IAM
- Esempi di policy basate sull'identità per Storage Gateway AWS
- Risoluzione dei problemi relativi all'identità e all'accesso AWS allo Storage Gateway
- Utilizzo dei tag per controllare l'accesso al gateway e alle risorse

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 AWS allo Storage Gateway)
- Amministratore del servizio: determina l'accesso degli utenti e invia le richieste di autorizzazione (consulta Come funziona AWS Storage Gateway con IAM)
- Amministratore IAM: scrivi policy per gestire l'accesso (consulta Esempi di policy basate sull'identità per Storage Gateway AWS)

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 AWS Storage Gateway con IAM

Prima di utilizzare IAM per gestire l'accesso a AWS SGW, scopri quali funzionalità IAM sono disponibili per l'uso con AWS SGW.

Funzionalità IAM che puoi utilizzare con AWS Storage Gateway

Funzionalità IAM	AWS Supporto SGW
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

Funzionalità IAM	AWS Supporto SGW
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
Ruoli di servizio	Sì
Ruoli collegati al servizio	Sì

Per avere una visione di alto livello di come AWS SGW 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 SGW AWS

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 SGW AWS

Per visualizzare esempi di politiche basate sull'identità di AWS SGW, vedere. Esempi di policy basate sull'identità per Storage Gateway AWS

Politiche basate sulle risorse all'interno di SGW AWS

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 SGW AWS

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale entità principale può eseguire operazioni su quali risorse e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso in una policy. Includere le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni AWS SGW, vedere Actions Defined by AWS Storage Gateway nel Service Authorization Reference.

Le azioni politiche in AWS SGW utilizzano il seguente prefisso prima dell'azione:

```
sgw
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

Per visualizzare esempi di politiche basate sull'identità di AWS SGW, vedere. Esempi di policy basate sull'identità per Storage Gateway AWS

Risorse politiche per SGW AWS

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 risorse AWS SGW e relativi ARNs, vedere Resources Defined by AWS Storage Gateway nel Service Authorization Reference. Per sapere con quali azioni è possibile specificare l'ARN di ogni risorsa, vedere Azioni definite da AWS Storage Gateway.

Per visualizzare esempi di politiche AWS SGW basate sull'identità, vedere. Esempi di policy basate sull'identità per Storage Gateway AWS

Chiavi relative alle condizioni delle politiche per SGW AWS

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 delle chiavi di condizione AWS SGW, vedere Condition Keys for AWS Storage Gateway nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, vedere Azioni definite da AWS Storage Gateway.

Per visualizzare esempi di politiche AWS SGW basate sull'identità, vedere. Esempi di policy basate sull'identità per Storage Gateway AWS

ACLs AWS in SGW

Supporti ACLs: no

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 SGW AWS

Supporta ABAC (tag nelle policy): parzialmente

Il controllo degli accessi basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi, chiamati tag. Puoi allegare tag a entità e AWS risorse IAM, quindi progettare politiche ABAC per consentire le 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 SGW AWS

Supporta le credenziali temporanee: sì

Le credenziali temporanee forniscono un 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 SGW AWS

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Le sessioni di accesso inoltrato (FAS) utilizzano le autorizzazioni del principale chiamante e Servizio AWS, in combinazione con la richiesta, di effettuare richieste Servizio AWS ai servizi downstream. Per i dettagli delle policy relative alle richieste FAS, consulta Forward access sessions.

Ruoli di servizio per SGW AWS

Supporta i ruoli di servizio: sì

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 interrompere la funzionalità AWS SGW. Modificate i ruoli di servizio solo quando AWS SGW fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per SGW AWS

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 ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Storage Gateway AWS

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare AWS risorse SGW. 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 i dettagli sulle azioni e sui tipi di risorse definiti da AWS SGW, incluso il formato di ARNs per ogni tipo di risorsa, vedere Actions, Resources and Condition Keys for AWS Storage Gateway nel Service Authorization Reference.

Argomenti

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare AWS risorse SGW 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 SGW AWS

Per accedere alla console AWS Storage Gateway, è necessario disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentire all'utente di elencare e visualizzare i dettagli sulle risorse AWS SGW presenti nel proprio. 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'API. AWS Al contrario, è opportuno concedere l'accesso solo alle azioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che gli utenti e i ruoli possano ancora utilizzare la console AWS SGW, collega anche la AWS SGW `ConsoleAccess` o la policy `ReadOnly` 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": "*"
        }
    ]
}
```

Risoluzione dei problemi relativi all'identità e all'accesso AWS allo Storage Gateway

Utilizzate le seguenti informazioni per aiutarvi a diagnosticare e risolvere i problemi più comuni che potreste riscontrare quando lavorate con AWS SGW e IAM.

Argomenti

Non sono autorizzato a eseguire un'azione in SGW AWS

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 `sgw:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw: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 `sgw:`*`GetWidget`*.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a AWS SGW.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS SGW. 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.

> **Important**
>
> Storage Gateway può assumere ruoli di servizio esistenti che vengono passati utilizzando l'azione delle `iam:PassRole` policy, ma non supporta le policy IAM che utilizzano la chiave di `iam:PassedToService` contesto per limitare l'azione a servizi specifici.
> Per ulteriori informazioni, consulta gli argomenti seguenti nella Guida per l'utente AWS Identity and Access Management :
>
> - IAM: passa un ruolo IAM a un AWS servizio specifico
> - Concessione a un utente delle autorizzazioni per trasferire un ruolo a un servizio AWS
> - Chiavi disponibili per IAM

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse AWS SGW

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 AWS SGW supporta queste funzionalità, consulta. Come funziona AWS Storage Gateway con IAM

- Per scoprire come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (federazione delle identità) nella Guida per l'utente IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente di IAM.

Utilizzo dei tag per controllare l'accesso al gateway e alle risorse

Per controllare l'accesso alle risorse e alle azioni del gateway, puoi utilizzare policy AWS Identity and Access Management (IAM) basate su tag. È possibile fornire il controllo in due modi:

1. Controllare l'accesso alle risorse di gateway in base ai tag di queste risorse.
2. Controllare quali tag possono essere trasferiti in una condizione di richiesta IAM.

Per informazioni su come usare i tag per controllare l'accesso, consulta Controllo degli accessi tramite tag.

Controllo dell'accesso in base ai tag di una risorsa

Per controllare le operazioni che un utente o un ruolo può eseguire su una risorsa di gateway, è possibile usare 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.

L'esempio seguente consente a un utente o un ruolo di eseguire le operazioni `ListTagsForResource`, `ListFileShares` e `DescribeNFSFileShares` su tutte le risorse. La policy si applica solo se il tag nella risorsa ha la chiave impostata su `allowListAndDescribe` e il valore impostato su `yes`.

JSON

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

```
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListTagsForResource",
                "storagegateway:ListFileShares",
                "storagegateway:DescribeNFSFileShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allowListAndDescribe": "yes"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:*"
            ],
            "Resource": "arn:aws:storagegateway:us-east-1:111122223333:*/*"
        }
    ]
}
```

Controllo dell'accesso in base ai tag in una richiesta IAM

Per controllare cosa può fare un utente su una risorsa gateway, puoi utilizzare le condizioni di una policy IAM basata sui tag. Ad esempio, puoi scrivere una policy che consenta o neghi a un utente la possibilità di eseguire operazioni API specifiche in base al tag fornito al momento della creazione della risorsa.

In questo esempio, la prima istruzione consente all'utente di creare un gateway solo se la coppia chiave-valore del tag fornito al momento della creazione del gateway è **`Department`** e **`Finance`**. Quando si utilizza l'operazione API, si aggiunge questo tag alla richiesta di attivazione.

La seconda istruzione consente all'utente di creare una condivisione file NFS (Network File System) o Server Message Block (SMB) su un gateway solo se la coppia chiave-valore del tag sul gateway corrisponde a **`Department`**e **`Finance`**. Inoltre, l'utente deve aggiungere un tag alla condivisione file e la coppia chiave-valore del tag deve essere **`Department`** e **`Finance`**. Puoi aggiungere i tag a una condivisione file nel momento in cui la crei. Non ci sono autorizzazioni per le operazioni

`AddTagsToResource` o `RemoveTagsFromResource`, quindi l'utente non è in grado di eseguire queste operazioni sul gateway o sulla condivisione file.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:CreateNFSFileShare",
            "storagegateway:CreateSMBFileShare"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/Department":"Finance",
               "aws:RequestTag/Department":"Finance"
            }
         }
      }
   ]
}
```

Convalida della conformità per AWS Storage Gateway

I revisori di terze parti valutano la sicurezza e la conformità di AWS Storage Gateway nell'ambito di più programmi di AWS conformità. Questi includono SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR e HITRUST CSF.

Per informazioni generali, vedere 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 responsabilità per la conformità quando utilizzi Storage Gateway è determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. AWS fornisce le risorse seguenti per semplificare la conformità:

- Guide rapide su sicurezza e conformità Guide introduttive implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla sicurezza e sulla conformità. AWS
- Whitepaper sull'architettura per la sicurezza e la conformità HIPAA: questo white paper descrive in che modo le aziende possono utilizzare per creare applicazioni conformi all'HIPAA. AWS
- AWS Risorse per la conformità Risorse per la conformità: questa raccolta di potrebbe riguardare il settore e la località in cui operate.
- Valutazione delle risorse in base alle regole contenute nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida del settore e alle normative.
- AWS Security Hub CSPM— Questo AWS servizio offre una visione completa dello stato di sicurezza dell'utente, AWS che consente di verificare la conformità agli standard e alle best practice del settore della sicurezza.

Resilienza nello AWS Storage Gateway

L'infrastruttura AWS globale è costruita attorno a Regioni AWS zone di disponibilità.

An Regione AWS è un luogo fisico in tutto il mondo in cui i data center sono raggruppati. Ogni gruppo di data center logici è denominato zona di disponibilità (AZ). Ciascuno Regione AWS è composto da un minimo di tre isolati e fisicamente separati AZs all'interno di un'area geografica. A differenza di altri provider di servizi cloud, che spesso definiscono una regione come un unico data center, il design

multiplo di AZ di ognuno Regione AWS offre vantaggi distinti. Ogni AZ dispone di alimentazione, raffreddamento e sicurezza fisica indipendenti ed è connessa tramite reti ridondanti ultra-low-latency. Se l'implementazione richiede un'attenzione particolare all'elevata disponibilità, è possibile configurare servizi e risorse in modo multiplo per ottenere una maggiore tolleranza AZs ai guasti.

Regioni AWS soddisfano i massimi livelli di sicurezza, conformità e protezione dei dati dell'infrastruttura. Tutto il traffico intercorrente AZs è crittografato. Le prestazioni di rete sono sufficienti per eseguire la replica sincrona tra. AZs AZs semplificano il partizionamento di servizi e risorse per un'elevata disponibilità. Se la distribuzione è partizionata AZs, le risorse sono meglio isolate e protette da problemi come interruzioni di corrente, fulmini, tornado, terremoti e altro ancora. AZs sono fisicamente separate da una distanza significativa da qualsiasi altra AZ, sebbene si trovino tutte nel raggio di 100 km (60 miglia) l'una dall'altra.

Per ulteriori informazioni sulle zone Regioni AWS di disponibilità, vedere AWS Global Infrastructure.

Oltre all'infrastruttura AWS globale, Storage Gateway supporta VMware vSphere High Availability (VMware HA) per proteggere i carichi di lavoro di storage da guasti hardware, hypervisor o di rete. Per ulteriori informazioni, vedere Utilizzo di VMware vSphere High Availability with Storage Gateway Using Gateway.

Sicurezza dell'infrastruttura in AWS Storage Gateway

In quanto servizio gestito, AWS Storage Gateway è protetto dalle procedure di sicurezza di rete AWS globali descritte in Security Pillar - AWS Well-Architected Framework.

Si utilizzano chiamate API AWS pubblicate per accedere a Storage Gateway attraverso la rete. I client devono supportare Transport Layer Security (TLS) 1.2. I client devono, inoltre, supportare le suite di crittografia con PFS (Perfect Forward Secrecy), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa è possibile utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

> **Note**
>
> È necessario trattare l'appliance AWS Storage Gateway come una macchina virtuale gestita e non tentare di accedere o modificare in alcun modo la sua installazione. Il tentativo di installare il software di scansione o di aggiornare qualsiasi pacchetto software utilizzando metodi diversi dal normale meccanismo di aggiornamento del gateway può causare il malfunzionamento del gateway e influire sulla nostra capacità di supportare o correggere il gateway.
>
> AWS esamina, analizza e corregge CVEs regolarmente. Incorporiamo le correzioni di questi problemi in Storage Gateway come parte del nostro normale ciclo di rilascio del software. Queste correzioni vengono in genere applicate come parte del normale processo di aggiornamento del gateway durante le finestre di manutenzione programmata. Per ulteriori informazioni sugli aggiornamenti del gateway, vedere Gestione degli aggiornamenti del gateway tramite la Gateway di archiviazione AWS console.

AWS Best practice per la sicurezza

AWS fornisce una serie di funzionalità di sicurezza da prendere in considerazione durante lo sviluppo e l'implementazione delle proprie politiche di sicurezza. Le seguenti best practice sono linee guida generali e non rappresentano una soluzione di sicurezza completa. Poiché queste pratiche potrebbero non essere appropriate o sufficienti per l'ambiente, gestiscile come considerazioni utili anziché prescrizioni. Per ulteriori informazioni, consulta Best practice di sicurezza AWS.

Registrazione e monitoraggio Gateway di archiviazione AWS

Storage Gateway è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Storage Gateway. CloudTrail acquisisce tutte le chiamate API per Storage Gateway come eventi. Le chiamate acquisite includono le chiamate dalla console di Storage Gateway e le chiamate di codice alle operazioni delle API Storage Gateway. Se crei un trail, puoi attivare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Storage Gateway. 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, è possibile determinare la richiesta effettuata a Storage Gateway, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e ulteriori dettagli.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni sullo Storage Gateway in CloudTrail

CloudTrail viene attivato sul tuo AWS account al momento della creazione dell'account. Quando si verifica un'attività in Storage Gateway, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nel proprio AWS account. Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi nel tuo AWS account, inclusi gli eventi per Storage Gateway, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un percorso nella console, il percorso si applica a tutte le AWS regioni. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, è possibile configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Panoramica della creazione di un trail
- CloudTrail Servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più regioni e ricezione di file di CloudTrail registro da più account

Tutte le operazioni di Storage Gateway sono registrate e documentate nell'argomento Operazioni. Ad esempio, le chiamate a `ActivateGateway`, `ListGateways`, e `ShutdownGateway` le azioni generano voci nei file di CloudTrail registro.

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con credenziali utente root o AWS Identity and Access Management (IAM).
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro AWS servizio.

Per ulteriori informazioni, consulta Elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di registro di Storage Gateway

Un trail è una configurazione che consente la consegna 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 illustra l'azione.


```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                        "gatewayTimezone": "GMT-5:00",
                                        "gatewayName": "cloudtrailgatewayvtl",
                                        "gatewayRegion": "us-east-2",
                                        "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                        "gatewayType": "VTL"
                                             },
                                             "responseElements": {
                                                                    "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                             },
                                             "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
```

```
                                                    "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                                    "eventType": "AwsApiCall",
                                                    "apiVersion": "20130630",
                                                    "recipientAccountId": "444455556666"
             }]
}
```

L'esempio seguente mostra una voce di CloudTrail registro che illustra l' ListGatewaysazione.

```
{
 "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
                                "type": "IAMUser",
                                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                                "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                " userName ":" JohnDoe "
                                },

                                " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                " eventSource ":" storagegateway.amazonaws.com ",
                                " eventName ":" ListGateways ",
                                " awsRegion ":" us-east-2 ",
                                " sourceIPAddress ":" 192.0.2.0 ",
                                " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                                " requestParameters ":null,
                                " responseElements ":null,
                                "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
              }]
}
```

Risoluzione dei problemi relativi all'implementazione dello Storage Gateway

Di seguito, sono disponibili informazioni sulle best practice e sulla risoluzione dei problemi relativi a gateway, piattaforme host, file system, alta disponibilità, ripristino dei dati e istantanee. Le informazioni sulla risoluzione dei problemi dei gateway locali riguardano i gateway distribuiti sulle piattaforme di virtualizzazione supportate. Le informazioni sulla risoluzione dei problemi di alta disponibilità riguardano i gateway in esecuzione sulla piattaforma VMware vSphere High Availability (HA).

Argomenti

- Risoluzione dei problemi: problemi relativi al gateway offline- Scopri come diagnosticare i problemi che possono far apparire il gateway offline nella console Storage Gateway.
- Risoluzione dei problemi: problemi relativi ad Active Directory- Scopri cosa fare se ricevi messaggi di errore come `NETWORK_ERRORTIMEOUT`, o `ACCESS_DENIED` quando tenti di aggiungere File Gateway a un dominio Microsoft Active Directory.
- Risoluzione dei problemi: problemi di attivazione del gateway- Scopri cosa fare se ricevi un messaggio di errore interno quando tenti di attivare lo Storage Gateway.
- Risoluzione dei problemi: problemi relativi al gateway locale- Scopri i problemi tipici che potresti riscontrare lavorando con i gateway locali e come consentire la connessione al gateway Supporto per facilitare la risoluzione dei problemi.
- Risoluzione dei problemi: problemi di configurazione di Microsoft Hyper-V- Scopri i problemi tipici che potresti riscontrare durante l'implementazione di Storage Gateway sulla piattaforma Microsoft Hyper-V.
- Risoluzione dei problemi: problemi relativi al gateway Amazon EC2- Trova informazioni sui problemi tipici che potresti riscontrare quando lavori con i gateway distribuiti su Amazon EC2.
- Risoluzione dei problemi: problemi relativi alle apparecchiature hardware- Scopri come risolvere i problemi che potresti riscontrare con l'appliance hardware AWS Storage Gateway.
- Risoluzione dei problemi: problemi relativi a File Gateway- Trova informazioni che possano aiutarti a comprendere la causa degli errori e delle notifiche di integrità che appaiono nei CloudWatch log di File Gateway.
- Risoluzione dei problemi: problemi di elevata disponibilità- Scopri cosa fare in caso di problemi con i gateway distribuiti in un ambiente VMware HA.

Risoluzione dei problemi: gateway offline nella console Storage Gateway

Utilizza le seguenti informazioni per la risoluzione dei problemi per determinare cosa fare se la Gateway di archiviazione AWS console mostra che il gateway è offline.

È possibile che il gateway venga visualizzato come offline per uno o più dei seguenti motivi:

- Il gateway non può raggiungere gli endpoint del servizio Storage Gateway.
- Il gateway si è spento in modo imprevisto.
- Un disco di cache associato al gateway è stato disconnesso o modificato oppure è guasto.

Per riportare il gateway online, identificate e risolvete il problema che ha causato la disconnessione del gateway.

Controlla il firewall o il proxy associato

Se hai configurato il gateway per utilizzare un proxy o hai posizionato il gateway protetto da un firewall, consulta le regole di accesso del proxy o del firewall. Il proxy o il firewall devono consentire il traffico da e verso le porte di rete e gli endpoint di servizio richiesti da Storage Gateway. Per ulteriori informazioni, vedere di rete e firewall Requisiti di .

Verifica la presenza di un'ispezione continua tramite SSL o deep packet del traffico del tuo gateway

Se è attualmente in corso un'ispezione SSL o deep-packet sul traffico di rete tra il gateway e il gateway AWS, il gateway potrebbe non essere in grado di comunicare con gli endpoint di servizio richiesti. Per riportare il gateway online, è necessario disattivare l'ispezione.

Controlla la metrica IOWait Percentuale dopo un riavvio o un aggiornamento del software

Dopo un riavvio o un aggiornamento del software, controlla se la `IOWaitPercent` metrica per File Gateway è 10 o superiore. Ciò potrebbe rallentare la risposta del gateway durante la ricostruzione della cache dell'indice in RAM. Per ulteriori informazioni, consulta . CloudWatch

Verificare la presenza di un'interruzione dell'alimentazione o di un guasto hardware sull'host dell'hypervisor

Un'interruzione dell'alimentazione o un guasto hardware sull'host hypervisor del gateway può causare lo spegnimento imprevisto del gateway e renderlo irraggiungibile. Dopo aver ripristinato l'alimentazione e la connettività di rete, il gateway sarà nuovamente raggiungibile.

Dopo che il gateway sarà tornato online, assicurati di adottare le misure necessarie per ripristinare i dati. Per ulteriori informazioni, consulta Best practice: recovery your data .

Verifica la presenza di problemi con un disco di cache associato

Il gateway può andare offline se almeno uno dei dischi di cache associati al gateway è stato rimosso, modificato o ridimensionato o se è danneggiato.

Se un disco cache funzionante è stato rimosso dall'host dell'hypervisor:

1. Arresta il gateway.
2. Aggiungere nuovamente il disco.

   > **Note**
   >
   > Assicurati di aggiungere il disco allo stesso nodo del disco.

3. Riavviare il gateway.

Se un disco cache è danneggiato, è stato sostituito o è stato ridimensionato:

- Segui la procedura del Metodo 2 descritta in Sostituzione del tuo S3 File Gateway esistente con una nuova istanza per configurare un nuovo gateway e scaricare nuovamente le informazioni sul disco di cache dal cloud. AWS

Risoluzione dei problemi: problemi di connessione del gateway ad Active Directory

Utilizza le seguenti informazioni per la risoluzione dei problemi per determinare cosa fare se ricevi messaggi di errore come `NETWORK_ERRORTIMEOUT`, o `ACCESS_DENIED` quando tenti di aggiungere il tuo File Gateway a un dominio Microsoft Active Directory.

Per risolvere questi errori, esegui i controlli e le configurazioni seguenti.

Verifica che il gateway sia in grado di raggiungere il controller di dominio eseguendo un test nping

Per eseguire un test nping:

1. Connect alla console locale del gateway utilizzando il software di gestione dell'hypervisor (VMware, Hyper-V o KVM) per i gateway locali o utilizzando ssh per i gateway Amazon EC2.
2. Inserisci il numero corrispondente per selezionare Gateway Console, quindi inserisci per elencare tutti i comandi disponibili. h Per testare la connettività tra la macchina virtuale Storage Gateway e il dominio, eseguire il comando seguente:

   ```
   nping -d corp.domain.com -p 389 -c 1 -t tcp
   ```

   > **Note**
   >
   > `corp.domain.com`Sostituiscilo con il nome DNS del dominio Active Directory e sostituiscilo `389` con la porta LDAP per il tuo ambiente.
   > Verifica di aver aperto le porte richieste all'interno del firewall.

Di seguito è riportato un esempio di test nping riuscito in cui il gateway è riuscito a raggiungere il controller di dominio:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
 seq=2597195024 win=1480
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
 seq=4170716243 win=8192 <mss 8961>
```

```
Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

Di seguito è riportato un esempio di test nping in cui non c'è connettività o risposta dalla `corp.domain.com` destinazione:

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389  S ttl=64 id=30318 iplen=40
 seq=1762671338 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
```

Verifica le opzioni DHCP impostate per il VPC della tua istanza gateway Amazon EC2

Se File Gateway è in esecuzione su un'istanza Amazon EC2, devi assicurarti che un set di opzioni DHCP sia configurato e collegato correttamente all'Amazon Virtual Private Cloud (VPC) che contiene l'istanza del gateway. Per ulteriori informazioni, consulta Set di opzioni DHCP in Amazon VPC.

Verifica che il gateway sia in grado di risolvere il dominio eseguendo una query dig

Se il dominio non è risolvibile dal gateway, il gateway non può entrare a far parte del dominio.

Per eseguire una dig query:

1. Connect alla console locale del gateway utilizzando il software di gestione dell'hypervisor (VMware, Hyper-V o KVM) per i gateway locali o utilizzando ssh per i gateway Amazon EC2.
2. Inserisci il numero corrispondente per selezionare Gateway Console, quindi inserisci per elencare tutti i comandi disponibili. h Per verificare se il gateway è in grado di risolvere il dominio, esegui il comando seguente:

   ```
   dig -d corp.domain.com
   ```

> **Note**
>
> `corp.domain.com`Sostituiscilo con il nome DNS del dominio Active Directory.

Di seguito è riportato un esempio di risposta riuscita:

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.        IN    A

;; ANSWER SECTION:
corp.domain.com.    600    IN    A    10.10.10.10
corp.domain.com.    600    IN    A    10.10.20.10

;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE  rcvd: 78
```

Controlla le impostazioni e i ruoli del controller di dominio

Verifica che il controller di dominio non sia impostato in modalità di sola lettura e che disponga di ruoli sufficienti per consentire l'accesso ai computer. Per verificarlo, prova a collegare altri server dalla stessa sottorete VPC della macchina virtuale gateway al dominio.

Verifica che il gateway sia aggiunto al controller di dominio più vicino

Come procedura ottimale, si consiglia di collegare il gateway a un controller di dominio geograficamente vicino all'appliance gateway. Se l'appliance gateway non è in grado di comunicare con il controller di dominio entro 20 secondi a causa della latenza di rete, il processo di aggiunta al dominio può scadere. Ad esempio, il processo potrebbe scadere se l'appliance gateway si trova negli

Stati Uniti orientali (Virginia settentrionale) Regione AWS e il controller di dominio si trova nell'Asia Pacifico (Singapore). Regione AWS

> **Note**
>
> Per aumentare il valore di timeout predefinito di 20 secondi, è possibile eseguire il comando join-domain in AWS Command Line Interface (AWS CLI) e includere l'`--timeout-in-seconds`opzione per aumentare il tempo. Puoi anche utilizzare la chiamata JoinDomain API e includere il `TimeoutInSeconds` parametro per aumentare il tempo. Il valore di timeout massimo è 3.600 secondi.
> Se ricevi errori durante l'esecuzione dei AWS CLI comandi, assicurati di utilizzare la versione più recente. AWS CLI

Verifica che Active Directory crei nuovi oggetti informatici nell'unità organizzativa (OU) predefinita

Accertarsi che Microsoft Active Directory non disponga di oggetti di criteri di gruppo che creino nuovi oggetti computer in posizioni diverse dall'unità organizzativa predefinita. Prima di poter aggiungere il gateway al dominio Active Directory, è necessario che nell'unità organizzativa predefinita esista un nuovo oggetto computer. Alcuni ambienti Active Directory sono personalizzati in modo da avere oggetti diversi OUs per quelli appena creati. Per garantire che nell'unità organizzativa predefinita esista un nuovo oggetto computer per la macchina virtuale gateway, provate a creare l'oggetto computer manualmente sul controller di dominio prima di aggiungere il gateway al dominio. È inoltre possibile eseguire il comando join-domain utilizzando. AWS CLI Quindi, specifica l'opzione per. `--organizational-unit`

> **Note**
>
> Il processo di creazione dell'oggetto informatico è denominato preallestimento.

Controlla i registri degli eventi del controller di dominio

Se non riesci ad aggiungere il gateway al dominio dopo aver provato tutti gli altri controlli e configurazioni descritti nelle sezioni precedenti, ti consigliamo di esaminare i registri degli eventi del controller di dominio. Verifica la presenza di eventuali errori nel visualizzatore eventi del controller di dominio. Verifica che le query del gateway abbiano raggiunto il controller di dominio.

Risoluzione dei problemi: errore interno durante l'attivazione del gateway

Le richieste di attivazione dello Storage Gateway attraversano due percorsi di rete. Le richieste di attivazione in entrata inviate da un client si connettono alla macchina virtuale (VM) o all'istanza Amazon Elastic Compute Cloud (Amazon EC2) del gateway tramite la porta 80. Se il gateway riceve correttamente la richiesta di attivazione, comunica con gli endpoint Storage Gateway per ricevere una chiave di attivazione. Se il gateway non riesce a raggiungere gli endpoint Storage Gateway, risponde al client con un messaggio di errore interno.

Utilizza le seguenti informazioni per la risoluzione dei problemi per determinare cosa fare se ricevi un messaggio di errore interno quando tenti di attivare il. Gateway di archiviazione AWS

> **Note**
>
> - Assicurati di distribuire nuovi gateway utilizzando l'ultimo file di immagine della macchina virtuale o la versione di Amazon Machine Image (AMI). Riceverai un errore interno se tenti di attivare un gateway che utilizza un'AMI obsoleta.
> - Assicurati di selezionare il tipo di gateway corretto che intendi implementare prima di scaricare l'AMI. I file.ova e AMIs per ogni tipo di gateway sono diversi e non sono intercambiabili.

Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico

Per risolvere gli errori di attivazione durante l'attivazione del gateway utilizzando un endpoint pubblico, esegui i seguenti controlli e configurazioni.

Controlla le porte richieste

Per i gateway distribuiti in locale, verifica che le porte sul firewall locale siano aperte. Per i gateway distribuiti su un'istanza Amazon EC2, verifica che le porte siano aperte nel gruppo di sicurezza dell'istanza. Per confermare che le porte siano aperte, esegui un comando telnet sull'endpoint pubblico da un server. Questo server deve trovarsi nella stessa sottorete del gateway. Ad esempio, i seguenti comandi telnet testano la connessione alla porta 443:

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

Per confermare che il gateway stesso possa raggiungere l'endpoint, accedi alla console VM locale del gateway (per i gateway distribuiti in locale). In alternativa, puoi accedere tramite SSH all'istanza del gateway (per i gateway distribuiti su Amazon EC2). Quindi, esegui un test di connettività di rete. Conferma che il test ritorni`[PASSED]`. Per ulteriori informazioni, vedi Test della connettività di rete del .

> **Note**
>
> Il nome utente di accesso predefinito per la console del gateway è`admin`, e la password predefinita è`password`.

Assicurati che la sicurezza del firewall non modifichi i pacchetti inviati dal gateway agli endpoint pubblici

Le ispezioni SSL, le ispezioni approfondite dei pacchetti o altre forme di sicurezza del firewall possono interferire con i pacchetti inviati dal gateway. L'handshake SSL fallisce se il certificato SSL viene modificato rispetto a quanto previsto dall'endpoint di attivazione. Per confermare che non è in corso alcuna ispezione SSL, esegui un comando OpenSSL sull'endpoint `anon-cp.storagegateway.region.amazonaws.com` di attivazione principale () sulla porta 443. È necessario eseguire questo comando da un computer che si trova nella stessa sottorete del gateway:

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> Sostituisci *`region`* con il tuo. Regione AWS

Se non è in corso alcuna ispezione SSL, il comando restituisce una risposta simile alla seguente:

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

Se è in corso un'ispezione SSL, la risposta mostra una catena di certificati alterata, simile alla seguente:

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

L'endpoint di attivazione accetta gli handshake SSL solo se riconosce il certificato SSL. Ciò significa che il traffico in uscita del gateway verso gli endpoint deve essere esente dalle ispezioni eseguite dai firewall della rete. Queste ispezioni possono essere un'ispezione SSL o un'ispezione approfondita dei pacchetti.

Controlla la sincronizzazione dell'ora del gateway

Scostamenti temporali eccessivi possono causare errori di handshake SSL. Per i gateway locali, è possibile utilizzare la console VM locale del gateway per controllare la sincronizzazione dell'ora del gateway. L'inclinazione temporale non deve superare i 60 secondi.

L'opzione System Time Management non è disponibile sui gateway ospitati su istanze Amazon EC2. Per assicurarti che i gateway Amazon EC2 possano sincronizzare correttamente l'ora, verifica che l'istanza Amazon EC2 possa connettersi al seguente elenco di pool di server NTP tramite le porte UDP e TCP 123:

- time.aws.com
- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint Amazon VPC

Per risolvere gli errori di attivazione durante l'attivazione del gateway utilizzando un endpoint Amazon Virtual Private Cloud (Amazon VPC), esegui i seguenti controlli e configurazioni.

Controlla le porte richieste

Assicurati che le porte richieste all'interno del firewall locale (per i gateway distribuiti in locale) o del gruppo di sicurezza (per i gateway distribuiti in Amazon EC2) siano aperte. Le porte necessarie per connettere un gateway a un endpoint VPC Storage Gateway sono diverse da quelle richieste per la connessione di un gateway a endpoint pubblici. Le seguenti porte sono necessarie per la connessione a un endpoint VPC Storage Gateway:

- TCP 443

- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Inoltre, controlla il gruppo di sicurezza collegato all'endpoint VPC dello Storage Gateway. Il gruppo di sicurezza predefinito collegato all'endpoint potrebbe non consentire le porte richieste. Crea un nuovo gruppo di sicurezza che consenta il traffico proveniente dall'intervallo di indirizzi IP del gateway sulle porte richieste. Quindi, collega quel gruppo di sicurezza all'endpoint VPC.

> **Note**
>
> Utilizza la console Amazon VPC per verificare il gruppo di sicurezza collegato all'endpoint VPC. Visualizza l'endpoint VPC Storage Gateway dalla console, quindi scegli la scheda Security Groups.

Per confermare che le porte richieste siano aperte, è possibile eseguire i comandi telnet sull'endpoint VPC Storage Gateway. È necessario eseguire questi comandi da un server che si trova nella stessa sottorete del gateway. È possibile eseguire i test sul primo nome DNS che non specifica una zona di disponibilità. Ad esempio, i seguenti comandi telnet testano le connessioni alle porte richieste utilizzando il nome DNS vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

Assicurati che la sicurezza del firewall non modifichi i pacchetti inviati dal gateway all'endpoint Amazon VPC di Storage Gateway

Le ispezioni SSL, le ispezioni approfondite dei pacchetti o altre forme di sicurezza del firewall possono interferire con i pacchetti inviati dal gateway. L'handshake SSL fallisce se il certificato SSL

viene modificato rispetto a quanto previsto dall'endpoint di attivazione. Per confermare che non è in corso alcuna ispezione SSL, esegui un comando OpenSSL sull'endpoint VPC Storage Gateway. È necessario eseguire questo comando da un computer che si trova nella stessa sottorete del gateway. Esegui il comando per ogni porta richiesta:

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

Se non è in corso alcuna ispezione SSL, il comando restituisce una risposta simile alla seguente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
```

```
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

Se è in corso un'ispezione SSL, la risposta mostra una catena di certificati alterata, simile alla seguente:

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

L'endpoint di attivazione accetta gli handshake SSL solo se riconosce il certificato SSL. Ciò significa che il traffico in uscita del gateway verso l'endpoint VPC sulle porte richieste è esente dalle ispezioni eseguite dai firewall di rete. Queste ispezioni potrebbero essere ispezioni SSL o ispezioni approfondite dei pacchetti.

Controlla la sincronizzazione dell'ora del gateway

Scostamenti temporali eccessivi possono causare errori di handshake SSL. Per i gateway locali, è possibile utilizzare la console VM locale del gateway per controllare la sincronizzazione dell'ora del gateway. L'inclinazione temporale non deve superare i 60 secondi.

L'opzione System Time Management non è disponibile sui gateway ospitati su istanze Amazon EC2. Per assicurarti che i gateway Amazon EC2 possano sincronizzare correttamente l'ora, verifica che l'istanza Amazon EC2 possa connettersi al seguente elenco di pool di server NTP tramite le porte UDP e TCP 123:

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Verifica la presenza di un proxy HTTP e conferma le impostazioni del gruppo di sicurezza associato

Prima dell'attivazione, verifica se disponi di un proxy HTTP su Amazon EC2 configurato sulla macchina virtuale gateway locale come proxy Squid sulla porta 3128. In questo caso, conferma quanto segue:

- Il gruppo di sicurezza collegato al proxy HTTP su Amazon EC2 deve avere una regola in entrata. Questa regola in entrata deve consentire il traffico proxy Squid sulla porta 3128 dall'indirizzo IP della macchina virtuale del gateway.
- Il gruppo di sicurezza collegato all'endpoint VPC di Amazon EC2 deve avere regole in entrata. Queste regole in entrata devono consentire il traffico sulle porte 1026-1028, 1031, 2222 e 443 dall'indirizzo IP del proxy HTTP su Amazon EC2.

Risolvi gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico e nello stesso VPC è presente un endpoint VPC Storage Gateway

Per risolvere gli errori durante l'attivazione del gateway utilizzando un endpoint pubblico quando è presente un enpoint Amazon Virtual Private Cloud (Amazon VPC) nello stesso VPC, esegui i seguenti controlli e configurazioni.

Verificare che l'impostazione Enable Private DNS Name non sia abilitata sull'endpoint VPC Storage Gateway

Se l'opzione Abilita nome DNS privato è abilitata, non è possibile attivare alcun gateway da quel VPC all'endpoint pubblico.

Per disabilitare l'opzione del nome DNS privato:

1. Apri la Console Amazon VPC.
2. Nel pannello di navigazione, seleziona Endpoint.
3. Scegli il tuo endpoint VPC Storage Gateway.
4. Scegli Azioni.
5. Scegli Gestisci nomi DNS privati.
6. Per Abilita nome DNS privato, deseleziona Abilita per questo endpoint.
7. Scegli Modifica nomi DNS privati per salvare l'impostazione.

Risoluzione dei problemi: problemi relativi al gateway locale

Di seguito sono riportate informazioni sui problemi tipici che potresti riscontrare lavorando con i gateway locali e su come consentire la connessione Supporto al gateway per facilitare la risoluzione dei problemi.

Nella tabella seguente sono elencati i più comuni problemi che potrebbero verificarsi utilizzando gateway distribuiti in locale.

Problema	Operazione da eseguire
Non è possibile reperire l'indirizzo IP del gateway.	Utilizzare il client dell'hypervisor per connettersi all'host e trovare l'indirizzo IP del gateway. • Infatti VMware ESXi, l'indirizzo IP della macchina virtuale è disponibile nel client vSphere nella scheda Riepilogo. • Per Microsoft Hyper-V, l'indirizzo IP della VM può essere reperito accedendo alla console locale. Se comunque non si trova l'indirizzo IP del gateway:

Problema	Operazione da eseguire
	• Controllare che la VM sia attiva. Solo una VM attiva, infatti, consente l'assegnazione di un indirizzo IP al gateway. • Attendere la conclusione della procedura di avvio della VM. Con la VM appena attivata, la sequenza di avvio del gateway potrebbe richiedere qualche minuto per terminare.
Si verificano problemi di firewall o rete.	• Abilitare le porte necessarie per il gateway. • Se si utilizza un firewall o un router per filtrare o limitare il traffico di rete, è necessario configurare il firewall e/o il router affinché consentano questi endpoint di servizio per le comunicazioni in uscita ad AWS. Per ulteriori informazioni sui requisiti di rete e del firewall, consulta Requisiti di rete e firewall.
L'attivazione del gateway non riesce se si fa clic sul pulsante Continua con l'attivazione nella console di gestione Storage Gateway.	• Verificare l'accessibilità della VM del gateway eseguendone il ping dal client. • Verificare la connettività di rete a Internet della VM, senza la quale occorrerà configurare un proxy SOCKS. Per ulteriori informazioni in merito, consulta Verifica della connettività di rete del gateway. • Verificare che gli orari dell'host e della VM del gateway siano corretti e che l'host sia configurato per la sincronizzazione automatica di data e ora con un server NTP (Network Time Protocol). Per informazioni sulla sincronizzazione dell'ora degli host dell'hypervisor e, vedere. VMs Configurazione di un server Network Time Protocol (NTP) per il gateway • Dopo queste fasi, è possibile riprovare l'implementazione del gateway con la console Storage Gateway e la procedura guidata Configura e attiva il gateway. • Verifica che la tua macchina virtuale abbia almeno 16 GB di RAM. L'allocazione del gateway fallisce se la RAM è inferiore a 16 GB. Per ulteriori informazioni, consulta Requisiti di configurazione di File Gate.

Problema	Operazione da eseguire
Occorre aumentare la larghezza di banda tra il gateway e AWS.	È possibile migliorare la larghezza di banda dal gateway al AWS configurando la connessione Internet AWS su un adattatore di rete (NIC) separato da quello che collega le applicazioni e la macchina virtuale del gateway. Questo approccio è utile se si dispone di una connessione a larghezza di banda elevata AWS e si desidera evitare conflitti in termini di larghezza di banda, specialmente durante il ripristino di un'istantanea. Utilizzando Direct Connect si può stabilire una connessione di rete dedicata tra il gateway on-premise e AWS, perfetta per i carichi di lavoro con elevata velocità di trasmissione effettiva. Per misurare la larghezza di banda della connessione dal gateway a AWS, utilizza le metriche e del `CloudBytesDownloaded` gateway. `CloudBytesUploaded` Per ulteriori informazioni su questo argomento, consulta Prestazioni e ottimizzazione. Ottimizzando la connettività a Internet si evita il riempimento del buffer di caricamento.

Problema	Operazione da eseguire

Il throughput da o verso il gateway si azzera.	• Nella scheda Gateway della console Storage Gateway, verifica che gli indirizzi IP per la macchina virtuale gateway siano gli stessi visualizzati utilizzando il software client hypervisor (ovvero il client VMware vSphere o Microsoft Hyper-V Manager). In caso di mancata corrispondenza, riavviare il gateway dalla console Storage Gateway, come illustrato in Spegnimento della macchina virtuale gateway. Dopo il riavvio, gli indirizzi dell'elenco Indirizzi IP nella scheda Gateway della console Storage Gateway dovrebber o corrispondere agli indirizzi IP del gateway, determinati dal client dell'hypervisor.
	  • Infatti VMware ESXi, l'indirizzo IP della macchina virtuale è disponibile nel client vSphere nella scheda Riepilogo.
	  • Per Microsoft Hyper-V, l'indirizzo IP della VM può essere reperito accedendo alla console locale.
	• Verifica la connettività del gateway a AWS come descritto in. Verifica della connettività di rete del gateway
	• Controlla la configurazione dell'adattatore di rete del gateway nel client di gestione dell'hypervisor e assicurati che tutte le interfacc e che intendi utilizzare per il gateway siano attivate.
	• Controlla la configurazione dell'adattatore di rete del gateway nella console locale del gateway. Per istruzioni, consulta Configurazione delle impostazioni di rete del gateway.
	
	Puoi visualizzare la velocità effettiva da e verso il gateway dalla CloudWatch console Amazon. Per ulteriori informazioni sulla misurazione della velocità effettiva da e verso il gateway di destinazi one AWS, consulta. Prestazioni e ottimizzazione

Si sono verificati problemi durante l'importazione (distribuzione) di Storage Gateway su Microsoft Hyper-V.	Consultare Risoluzione dei problemi: configurazione di Microsoft Hyper-V, documento dedicato ai problemi che più comunemente possono verificarsi distribuendo un gateway su Microsoft Hyper-V.

Problema	Operazione da eseguire
Viene visualizzato il seguente messaggio: "I dati scritti sul volume del gateway non sono archiviati in modo sicuro su AWS".	Questo messaggio viene ricevuto se la VM del gateway è stata creata da un clone o uno snapshot di un'altra VM di gateway. Se così non fosse, rivolgersi a Supporto.

Attivazione dell' Supporto accesso per facilitare la risoluzione dei problemi relativi al gateway ospitato in locale

Storage Gateway fornisce una console locale che può essere utilizzata per eseguire diverse attività di manutenzione, tra cui consentire l'accesso Supporto al gateway per facilitare la risoluzione dei problemi relativi al gateway. Per impostazione predefinita, Supporto l'accesso al gateway è disattivato. È possibile attivare questo accesso tramite la console locale dell'host. Per Supporto consentire l'accesso al gateway, è necessario innanzitutto accedere alla console locale dell'host, accedere alla console di Storage Gateway e quindi connettersi al server di supporto.

Per attivare Supporto l'accesso al gateway

1. Accedere alla console locale dell'host.
   - VMware ESXi — per ulteriori informazioni, vedereAccesso alla console locale del gateway con VMware ESXi.
   - Microsoft Hyper-V: per ulteriori informazioni, consulta Accesso alla console locale del gateway con Microsoft Hyper-V.
2. Quando richiesto, immetti il numero corrispondente per selezionare Console gateway.
3. Immetti **h** per aprire la finestra dei comandi disponibili.
4. Esegui una delle seguenti operazioni:
   - Se il gateway utilizza un endpoint pubblico, nella finestra COMANDI DISPONIBILI, immettere **`open-support-channel`** per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

- Se il gateway utilizza un endpoint VPC, nella finestra COMANDI DISPONIBILI, inserisci **`open-support-channel`**. Se il gateway non è attivato, fornire l'endpoint VPC o l'indirizzo IP per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

> **Note**
>
> Il numero del canale non è un numero di porta Protocol/User Datagram Protocol (TCP/UDP (Transmission Control). Al contrario, il gateway crea una connessione Secure Shell (SSH) (TCP 22) ai server di Storage Gateway e su questa mette a disposizione il canale di supporto.

5. Dopo aver stabilito il canale di supporto, fornisci il numero del servizio di supporto Supporto in modo da Supporto poter fornire assistenza per la risoluzione dei problemi.
6. Alla conclusione della sessione di supporto, immettere **`q`** per terminare. Non chiudere la sessione finché il supporto di Amazon Web Services non comunica che la sessione di supporto è completa.
7. Immettere **`exit`** per disconnettersi dalla console Storage Gateway.
8. Seguire le istruzioni per uscire dalla console locale.

Risoluzione dei problemi: configurazione di Microsoft Hyper-V

Nella tabella seguente sono elencati i problemi che più comunemente possono verificarsi quando si implementa Storage Gateway sulla piattaforma Microsoft Hyper-V.

Problema	Operazione da eseguire
Si tenta di importare un gateway e si riceve il seguente messaggio di errore: «Si è verificato un errore del server durante il tentativo di importare	Ci si può imbattere in questo errore per i seguenti motivi: • Se non si specifica l'origine dei file sorgente decompressi del gateway. L'ultima parte della posizione specificata nella finestra di dialogo Importa macchina virtuale dovrebbe essere. `AWS-Storage-Gateway` Esempio:

Problema	Operazione da eseguire
la macchina virtuale. Importazione non riuscita. Impossibile trovare i file di importazione della macchina virtuale nella posizione [...]. Puoi importare una macchina virtuale solo se hai usato Hyper-V per crearla ed esportarla.»	`C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • Se è già stato distribuito un gateway senza selezionare le opzioni Copy the virtual machine (Copia la macchina virtuale) e Duplicate all files (Duplica tutti i file) nella finestra di dialogo Import Virtual Machine (Importa macchina virtuale), la VM è stata già creata nella sede dove si trovano i file di gateway decompressi, dalla quale non è possibile importare nuovamente. Per risolvere il problema, copiare ex novo i file sorgente del gateway decompres si in una nuova sede, da utilizzare come origine d'importazione. Se si prevede di creare più gateway da un'unica posizione di file di origine decompressi, è necessario selezionare Copia la macchina virtuale e selezionare la casella Duplica tutti i file nella finestra di dialogo Importa macchina virtuale.
Si tenta di importare un gateway e si riceve il seguente messaggio di errore: «Si è verificato un errore del server durante il tentativo di importare la macchina virtuale. Importazione non riuscita. L'operazione di importazi one non è riuscita a copiare il file da [...]: il file esiste. (0x80070050)»	Questo errore si verifica quando, con un gateway già distribui to, si tenta di riutilizzare le cartelle predefinite che includono i file del disco rigido virtuale e quelli di configurazione della macchina virtuale. Per risolvere questo problema, specifica nuove posizioni in Server nel pannello sul lato sinistro della finestra di dialogo Impostazioni Hyper-V.

Problema	Operazione da eseguire
Si tenta di importare un gateway e si riceve il seguente messaggio di errore: «Si è verificato un errore del server durante il tentativo di importare la macchina virtuale. Importazione non riuscita. Per importare, assegna alla macchina virtuale un nuovo identificatore. Seleziona il nuovo identificatore e riprova."	Quando importi il gateway, assicurati di selezionare Copia la macchina virtuale e di selezionare la casella Duplica tutti i file nella finestra di dialogo Importa macchina virtuale per creare un nuovo ID univoco per la macchina virtuale.
Si tenta di avviare una macchina virtuale gateway e si riceve il seguente messaggio di errore: «Si è verificato un errore durante il tentativo di avviare le macchine virtuali selezionate. L'imposta zione del processore di partizione secondario non è compatibile con la partizione principale. Impossibile inizializzare 'AWS-Storage-Gateway'. (ID macchina virtuale [...])»	Questo errore è probabilmente causato da una discrepanza della CPU tra quella richiesta CPUs per il gateway e quella disponibi le CPUs sull'host. Accertarsi che il conteggio di CPU della VM sia supportato dall'hypervisor sottostante. Per ulteriori informazioni sui requisiti per Storage Gateway, consulta Requisiti di configurazione di File Gate.

Problema	Operazione da eseguire
Si tenta di avviare una macchina virtuale gateway e si riceve il seguente messaggio di errore: «Si è verificato un errore durante il tentativo di avviare le macchine virtuali selezionate. Impossibile inizializzare 'AWS-Storage-Gateway'. (ID macchina virtuale [...]) Impossibile creare la partizione: le risorse di sistema sono insufficienti per completar e il servizio richiesto. (0x800705AA)»	Questo errore potrebbe essere causato da una discrepanza tra la RAM necessaria per il gateway e quella disponibile sull'host. Per ulteriori informazioni sui requisiti per Storage Gateway, consulta Requisiti di configurazione di File Gate.
Gli aggiornamenti di software di gateway e snapshot si verificano con tempistiche leggermente diverse da quelle previste.	L'orologio della VM del gateway potrebbe essere soggetto allo scostamento del clock, cioè differire dall'orario effettivo. Controlla re e correggere l'orario della VM utilizzando l'opzione di sincroniz zazione oraria della console del gateway locale. Per ulteriori informazioni, consulta Configurazione di un server Network Time Protocol (NTP) per il gateway.
Bisogna inserire i file decompressi di Storage Gateway con Microsoft Hyper-V nel file system dell'host.	Accedere all'host come si fa generalmente con un server Microsoft Windows. Ad esempio, se il nome dell'host dell'hypervisor è `hyperv-server` , si può utilizzare il percorso UNC `\\hyperv-server\c$` , presupponendo che il nome `hyperv-server` possa essere risolto o sia definito nel file degli host in locale.
Nel connettersi all'hyper visor viene richiesto di immettere le credenziali.	Aggiungere le credenziali utente da amministratore locale per l'host dell'hypervisor, avvalendosi dello strumento Sconfig.cmd.

Problema	Operazione da eseguire
È possibile notare prestazioni di rete scadenti se si attiva la coda di macchine virtuali (VMQ) per un host Hyper-V che utilizza una scheda di rete Broadcom.	Per informazioni su una soluzione alternativa, consulta la documentazione Microsoft, vedi Scarse prestazioni di rete sulle macchine virtuali su un host Hyper-V Windows Server 2012 se VMQ è acceso.

Risoluzione dei problemi: problemi relativi al gateway Amazon EC2

Nelle sezioni seguenti, sono elencati i classici problemi che potrebbero verificarsi utilizzando gateway distribuiti su Amazon EC2. Per ulteriori informazioni sulla differenza tra un gateway on-premise e uno distribuito su Amazon EC2, consulta Implementa un host FSx Amazon EC2 predefinito per File Gateway.

Argomenti

Dopo qualche secondo, il gateway ancora non si attiva

Nella console Amazon EC2 accertati di quanto segue:

- La porta 80 è aperta nel gruppo di sicurezza associato all'istanza. Per ulteriori informazioni sull'aggiunta di una regola del gruppo di sicurezza, consulta Adding a security group rule nella Amazon EC2 User Guide.
- L'istanza del gateway è contrassegnata come in esecuzione. Lo Stato dell'istanza nella console Amazon EC2 dovrebbe essere IN ESECUZIONE.
- Il tipo di istanza Amazon EC2 soddisfa i requisiti minimi, come descritto in Requisiti di storage.

Dopo aver risolto il problema, provare di nuovo ad attivare il gateway. A tale scopo, aprire la console Storage Gateway, scegliere Distribuisci un nuovo gateway su Amazon EC2 e inserire nuovamente l'indirizzo IP dell'istanza.

L'istanza del gateway EC2 non è inclusa nell'elenco delle istanze

Se non si assegna all'istanza un tag di risorsa e si dispone di molte istanze in esecuzione, può risultare difficile stabilire quale istanza è stata avviata. Per individuare l'istanza del gateway, in tal caso, occorre procedere come di seguito:

- Controllare il nome dell'Amazon Machine Image (AMI) nella scheda Description (Descrizione) dell'istanza. Il nome di un'istanza basata sull'AMI di Storage Gateway dovrebbe iniziare con il testo **`aws-storage-gateway-ami`**.
- Se si dispone di più istanze basate sull'AMI di Storage Gateway, controllarne l'orario di avvio per trovare quella giusta.

Vuoi connetterti a un'istanza gateway tramite la Console seriale Amazon EC2

Puoi utilizzare la Console seriale Amazon EC2 per la risoluzione dei problemi di avvio, di configurazione di rete e di altro tipo. Per istruzioni e suggerimenti per la risoluzione dei problemi, consulta Console seriale Amazon EC2 nella Guida per l'utente di Amazon Elastic Compute Cloud.

Vuoi aiutarci Supporto a risolvere i problemi del tuo gateway Amazon EC2

Storage Gateway fornisce una console locale che può essere utilizzata per eseguire diverse attività di manutenzione, tra cui consentire l'accesso Supporto al gateway per facilitare la risoluzione dei problemi relativi al gateway. Per impostazione predefinita, Supporto l'accesso al gateway è disattivato. Attivi questo accesso tramite la console locale di Amazon EC2. È possibile effettuare l'accesso alla console locale Amazon EC2 attraverso Secure Shell (SSH). Per effettuare l'accesso tramite SSH, il gruppo di sicurezza dell'istanza deve contenere una regola che apra la porta TCP 22.

> **Note**
>
> Se si aggiunge una nuova regola a un gruppo di sicurezza, la nuova regola si applica a tutte le istanze che utilizzano quel gruppo di sicurezza. Per ulteriori informazioni sui gruppi di

sicurezza e su come aggiungere una regola del gruppo di sicurezza, consulta la sezione Gruppi di sicurezza Amazon EC2 nella Guida per l'utente di Amazon EC2.

Per consentire la Supporto connessione al gateway, devi prima accedere alla console locale dell'istanza Amazon EC2, accedere alla console di Storage Gateway e quindi fornire l'accesso.

Per attivare Supporto l'accesso per un gateway distribuito su un'istanza Amazon EC2

1. Accedere alla console locale dell'istanza Amazon EC2. Per le istruzioni, consultare la sezione Connettersi all'istanza nella Guida per l'utente di Amazon EC2.

   Per accedere alla console locale dell´istanza EC2, è possibile utilizzare il seguente comando.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > *PRIVATE-KEY*È il `.pem` file contenente il certificato privato della coppia di chiavi EC2 che hai usato per avviare l'istanza Amazon EC2. Per ulteriori informazioni, consulta Recuperare la chiave pubblica della propria coppia di chiavi nella Guida per l'utente di Amazon EC2.
   > *INSTANCE-PUBLIC-DNS-NAME*È il nome DNS (Domain Name System) pubblico dell'istanza Amazon EC2 su cui è in esecuzione il gateway. È possibile ottenere questo nome pubblico DNS selezionando l'istanza Amazon EC2 nella console EC2 e facendo clic sulla scheda Descrizione.

2. Quando richiesto, immettere **`6 - Command Prompt`** per aprire la console del canale Supporto .
3. Immettere **h** per aprire la finestra AVAILABLE COMMANDS (COMANDI DISPONIBILI).
4. Esegui una delle seguenti operazioni:

   - Se il gateway utilizza un endpoint pubblico, nella finestra COMANDI DISPONIBILI, immettere **`open-support-channel`** per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

- Se il gateway utilizza un endpoint VPC, nella finestra COMANDI DISPONIBILI, inserisci **`open-support-channel`**. Se il gateway non è attivato, fornire l'endpoint VPC o l'indirizzo IP per connettersi al supporto clienti per Storage Gateway. Consentire la porta TCP 22 in modo da poter aprire un canale di supporto ad AWS. Quando ci si connette al servizio di assistenza clienti, Storage Gateway assegna un numero di supporto che è bene annotare.

> **Note**
>
> Il numero di canale non è un numero di porta Protocol/User Datagram Protocol (TCP/UDP (Transmission Control). Al contrario, il gateway crea una connessione Secure Shell (SSH) (TCP 22) ai server di Storage Gateway e su questa mette a disposizione il canale di supporto.

5. Dopo aver stabilito il canale di supporto, fornisci il numero del servizio di supporto Supporto in modo da Supporto poter fornire assistenza per la risoluzione dei problemi.
6. Alla conclusione della sessione di supporto, immettere **`q`** per terminare. Non chiudere la sessione finché il supporto di Amazon Web Services non comunica che la sessione di supporto è completa.
7. Inserisci **`exit`** per uscire dalla console Storage Gateway.
8. Segui i menu della console per uscire dall'istanza Storage Gateway.

Risoluzione dei problemi: problemi relativi alle apparecchiature hardware

> **Note**
>
> Avviso di fine della disponibilità: a partire dal 12 maggio 2025, l'appliance Gateway di archiviazione AWS hardware non sarà più disponibile. I clienti esistenti con l'appliance Gateway di archiviazione AWS hardware possono continuare a utilizzare e ricevere assistenza fino a maggio 2028. In alternativa, puoi utilizzare il Gateway di archiviazione AWS servizio per fornire alle tue applicazioni in locale e nel cloud l'accesso a uno spazio di archiviazione cloud praticamente illimitato.

Negli argomenti seguenti vengono descritti i problemi che potrebbero verificarsi con l'appliance hardware AWS Storage Gateway e vengono forniti suggerimenti per la risoluzione di tali problemi.

Argomenti

Impossibile determinare l'indirizzo IP del servizio

Durante il tentativo di connessione al servizio, assicurarsi di utilizzare l'indirizzo IP del servizio e non l'indirizzo IP dell'host. Configurare l'indirizzo IP del servizio nella console di servizio e l'indirizzo IP dell'host nella console hardware. La console hardware viene visualizzata quando si avvia l'appliance hardware. Per accedere alla console di servizio dalla console hardware, scegliere Open Service Console (Apri console di servizio).

Come si esegue una reimpostazione ai valori di fabbrica?

Se è necessario eseguire un ripristino delle impostazioni di fabbrica sul dispositivo, contattare il team di AWS Storage Gateway Hardware Appliance per ricevere assistenza, come descritto nella sezione Supporto che segue.

Come si esegue il riavvio remoto?

Se è necessario eseguire un riavvio remoto del dispositivo, è possibile farlo utilizzando l'interfaccia di gestione Dell iDRAC. Per ulteriori informazioni, consulta DRAC9 Virtual Power Cycle: accensione remota dei PowerEdge server Dell EMC sul sito Web di Dell Technologies. InfoHub

Dove si ottiene il supporto Dell iDRAC?

Il PowerEdge server Dell è dotato dell'interfaccia di gestione Dell iDRAC. Consigliamo quanto segue:

- Se si utilizza l'interfaccia di gestione iDRAC, è necessario modificare la password predefinita. Per ulteriori informazioni sulle credenziali iDRAC, vedere PowerEdge Dell - Quali sono le credenziali di accesso predefinite per iDRAC? .

- Assicurati che il firmware up-to-date serva a prevenire violazioni della sicurezza.
- Spostare l'interfaccia di rete iDRAC su una porta normale (`em`) può causare problemi di prestazioni o prevenire il normale funzionamento dell'appliance.

Impossibile trovare il numero di serie dell'appliance hardware

È possibile trovare il numero di serie dell'appliance hardware AWS Storage Gateway utilizzando la console Storage Gateway.

Per trovare il numero di serie del dispositivo hardware:

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Dal menu di navigazione a sinistra della pagina, scegli Hardware.
3. Seleziona il tuo dispositivo hardware dall'elenco.
4. Individua il campo Numero di serie nella scheda Dettagli del tuo dispositivo.

Dove ottenere supporto per l'appliance hardware

Per contattare il supporto tecnico AWS relativo al dispositivo hardware, vedere. Supporto

Il Supporto team potrebbe chiederti di attivare il canale di supporto per risolvere i problemi relativi al gateway da remoto. Non è necessario che questa porta sia aperta per il normale funzionamento del gateway, ma è necessario per la risoluzione dei problemi. È possibile attivare il canale di supporto dalla console hardware, come illustrato nella procedura seguente.

Per aprire un canale di supporto per AWS

1. Aprire la console hardware.
2. Scegli Open Support Channel nella parte inferiore della pagina principale della console hardware, quindi premi`Enter`.

   Il numero di porta assegnato dovrebbe apparire entro 30 secondi se non ci sono problemi di connettività di rete o firewall. Esempio:

   Stato: Aperto sulla porta 19599
3. Annota il numero di porta e forniscilo a Supporto.

Risoluzione dei problemi: problemi relativi a File Gateway

Puoi configurare File Gateway per scrivere voci di registro in un gruppo di CloudWatch log Amazon. In tal caso, riceverai notifiche sullo stato di integrità del gateway e su eventuali errori riscontrati dal gateway. È possibile trovare informazioni su queste notifiche di errore e di integrità in CloudWatch Logs.

Nelle sezioni seguenti sono disponibili informazioni che consentono di comprendere la causa di ogni errore e notifica di integrità e come risolvere i problemi.

Argomenti

Errore: FileMissing

L'`FileMissing`errore è simile all'`ObjectMissing`errore e i passaggi per risolverlo sono identici. Puoi ricevere un `FileMissing` errore quando un writer diverso dal File Gateway specificato elimina il file specificato da Amazon FSx. Eventuali caricamenti successivi su Amazon FSx o i recuperi dell'oggetto da Amazon hanno FSx esito negativo.

Per risolvere un errore FileMissing

1. Salva la copia più recente del file nel file system locale del tuo client SMB (questa copia del file è necessaria nel passaggio 3).

2. Elimina il file dal File Gateway utilizzando il client SMB.
3. Copia la versione più recente del file che hai salvato nella fase 1 Amazon FSx utilizzando il tuo client SMB. Fatelo tramite il vostro File Gateway.

Errore: FsxFileSystemAuthenticationFailure

È possibile che venga visualizzato un `FsxFileSystemAuthenticationFailure` errore quando le credenziali fornite durante il collegamento del file system sono scadute o i relativi privilegi sono stati revocati.

Per risolvere FsxFileSystemAuthenticationFailure un errore

1. Assicurati che le credenziali fornite al momento del collegamento al FSx file system Amazon siano ancora valide.
2. Assicurati che l'utente disponga di tutte le autorizzazioni necessarie, come descritto in Allega un file system Amazon FSx for Windows File Server.

Errore: FsxFileSystemConnectionFailure

È possibile che si `FsxFileSystemConnectionFailure` verifichi un errore quando il FSx server Amazon è inaccessibile dal computer gateway.

Per risolvere un errore FsxFileSystemConnectionFailure

1. Assicurati che tutte le regole del firewall e del VPC consentano la connessione tra la macchina gateway e il server Amazon FSx .
2. Assicurati che il FSx server Amazon sia in esecuzione.

Errore: FsxFileSystemFull

Puoi ricevere un `FsxFileSystemFull` errore quando non c'è abbastanza spazio libero su disco nel FSx file system Amazon.

Per risolvere un FsxFileSystemFull errore

- Aumenta lo spazio di archiviazione per il FSx file system Amazon.

Errore: GatewayClockOutOfSync

È possibile che venga `GatewayClockOutOfSync` visualizzato un errore quando il gateway rileva una differenza di almeno 5 minuti tra l'ora del sistema locale e l'ora riportata dai server AWS Storage Gateway. I problemi di sincronizzazione dell'orologio possono influire negativamente sulla connettività tra il gateway e. AWS Se l'orologio del gateway non è sincronizzato, potrebbero verificarsi errori di I/O per le connessioni NFS e SMB e gli utenti SMB potrebbero riscontrare errori di autenticazione.

Per risolvere un errore GatewayClockOutOfSync

- Verificare la configurazione di rete tra il gateway e il server NTP. Per ulteriori informazioni sulla sincronizzazione dell'ora della macchina virtuale del gateway e sull'aggiornamento della configurazione del server NTP, vedere Network Time Protocol (NTP) per il gateway.

Errore: InvalidFileState

È possibile che venga `InvalidFileState` visualizzato un errore quando un writer diverso dal gateway specificato modifica il file specificato nella condivisione di file specificata. Di conseguenza, lo stato del file sul gateway non corrisponde allo stato in Amazon FSx. Eventuali caricamenti o recuperi successivi del file da Amazon FSx potrebbero non riuscire.

Per risolvere un errore InvalidFileState

1. Salva la copia più recente del file nel file system locale del tuo client SMB (devi copiare questo file nel passaggio 4). Se la versione del file in Amazon FSx è la più recente, scarica quella versione. Puoi farlo accedendo direttamente alla FSx condivisione Amazon utilizzando qualsiasi client SMB.
2. Elimina il file FSx direttamente in Amazon.
3. Elimina il file dal gateway utilizzando il tuo client SMB.
4. Utilizzando il tuo client SMB, copia la versione più recente del file salvato nella fase 1, tramite File Gateway, su Amazon FSx.

Errore: ObjectMissing

Puoi ricevere un `ObjectMissing` errore quando un writer diverso dal File Gateway specificato elimina il file specificato da Amazon FSx. Eventuali caricamenti successivi su Amazon FSx o i recuperi dell'oggetto da Amazon hanno FSx esito negativo.

Per risolvere un errore ObjectMissing

1. Salva la copia più recente del file nel file system locale del tuo client SMB (questa copia del file è necessaria nel passaggio 3).
2. Elimina il file dal File Gateway utilizzando il client SMB.
3. Copia la versione più recente del file che hai salvato nella fase 1 Amazon FSx utilizzando il tuo client SMB. Fatelo tramite il vostro File Gateway.

Errore: DroppedNotifications

È possibile che venga visualizzato un `DroppedNotifications` errore anziché altri tipi di voci di CloudWatch registro previsti quando lo spazio di archiviazione libero sul disco principale del gateway è inferiore a 1 GB o se vengono generate più di 100 notifiche sanitarie entro un intervallo di 1 minuto. In queste circostanze, il gateway interrompe la generazione di notifiche di CloudWatch registro dettagliate come misura precauzionale.

Per risolvere un DroppedNotifications errore

1. Controlla la `Root Disk Usage` metrica nella scheda Monitoraggio del gateway nella console di Storage Gateway per determinare se lo spazio disponibile su disco root si sta esaurendo.
2. Aumenta le dimensioni del disco di archiviazione principale del gateway se lo spazio disponibile è inferiore a 1 GB. Per istruzioni, consulta la documentazione dell'hypervisor della macchina virtuale.

   Per aumentare le dimensioni del disco root per i gateway Amazon EC2, consulta Richiedere modifiche ai volumi EBS nella Guida per l'utente di Amazon Elastic Compute Cloud.

   > **Note**
   >
   > Non è possibile aumentare la dimensione del disco root per lo AWS Storage Gateway Hardware Appliance.

3. Riavviare il gateway.

Notifica: HardReboot

Puoi ricevere una notifica `HardReboot` quando la VM del gateway viene riavviata in modo imprevisto. Questo riavvio può essere dovuto a mancanza di alimentazione, a un guasto hardware o a un altro evento. Per i VMware gateway, un ripristino da parte di vSphere High Availability Application Monitoring può causare questo evento.

Quando il gateway funziona in un ambiente di questo tipo, verifica la presenza della `HealthCheckFailure` notifica e consulta il registro VMware degli eventi per la macchina virtuale.

Notifica: riavvio

Puoi ricevere una notifica di riavvio quando la VM del gateway viene riavviata. Puoi riavviare una macchina virtuale gateway utilizzando la console di gestione VM Hypervisor o la console Storage Gateway. È inoltre possibile riavviare utilizzando il software del gateway durante il ciclo di manutenzione del gateway.

Se il riavvio viene eseguito entro 10 minuti dall'ora di avvio della manutenzione configurata del gateway, probabilmente è un evento normale e non un'indicazione di problema. Se il riavvio è stato eseguito al di fuori della finestra di manutenzione in modo significativo, verifica se il gateway è stato riavviato manualmente.

Risoluzione dei problemi: problemi relativi al dominio Active Directory

FSx File Gateway non genera messaggi di registro specifici per problemi relativi al dominio Active Directory. Se hai problemi ad aggiungere il gateway al tuo dominio Active Directory, procedi come segue:

- Verifica che il gateway non stia tentando di utilizzare un controller di dominio di sola lettura (RODC) per accedere al dominio.
- Verificare che il gateway sia configurato per utilizzare i server DNS corretti.

  Ad esempio, se stai cercando di unire un'istanza gateway Amazon EC2 a un Active Directory AWS gestito, verifica che l'opzione DHCP impostata per il tuo VPC EC2 specifichi i server DNS di Active Directory gestiti. AWS

  I server DNS configurati tramite il set di opzioni DHCP VPC vengono forniti a tutte le istanze EC2 nel VPC. Se desideri specificare un server DNS per un singolo gateway, puoi farlo utilizzando la console locale EC2 di quel gateway.

Per i gateway locali, è necessario specificare un server DNS utilizzando la console locale della macchina virtuale.

- Verifica la connettività di rete del gateway eseguendo i seguenti comandi dal prompt dei comandi nella console locale del gateway. Sostituisci le variabili evidenziate con il nome di dominio e gli indirizzi IP effettivi della tua distribuzione.

```
dig -d ExampleDomainName
ncport -d ExampleDomainControllerIPAddress -p 445
ncport -d ExampleDomainControllerIPAddress -p 389
```

- Verifica che il tuo account del servizio Active Directory disponga delle autorizzazioni necessarie. Per ulteriori informazioni, consulta Requisiti di dell'account del servizio Active Directory.
- Verifica che il gateway si unisca all'unità organizzativa (OU) corretta.

  L'aggiunta a un dominio crea un account computer Active Directory nel contenitore predefinito dei computer (che non è un'unità organizzativa), utilizzando l'ID gateway del gateway come nome dell'account (ad esempio, SGW-1234ADE). Non è possibile personalizzare il nome di questo account.

  Se l'ambiente Active Directory dispone di un'unità organizzativa designata per i nuovi oggetti del computer, è necessario specificare tale unità organizzativa al momento dell'accesso al dominio.

  Se si verificano errori di accesso negato durante il tentativo di accedere all'unità organizzativa designata, rivolgiti all'amministratore di dominio Active Directory. L'amministratore potrebbe aver bisogno di preconfigurare l'account del computer del gateway prima di poter accedere al dominio. Per ulteriori informazioni, vedi Come posso risolvere i problemi relativi all'aggiunta del mio gateway di file Storage Gateway a un dominio per l'autenticazione Microsoft Active Directory? .
- Verifica che il nome host del gateway sia risolvibile in DNS eseguendo il comando seguente dal prompt dei comandi nella console locale del gateway. Sostituisci la variabile evidenziata con il nome host effettivo del gateway.

```
dig -d ExampleHostName -r A
```

  Se hai configurato un nome host personalizzato per il gateway, devi aggiungere manualmente un record DNS A che punti al relativo indirizzo IP.

- Verifica che la latenza di rete tra il gateway e il controller di dominio sia ragionevolmente bassa. La richiesta di aggiunta a un dominio può scadere se il gateway non riceve una risposta dal controller di dominio entro 20 secondi.

  Se si aggiunge il gateway al dominio utilizzando il comando JoinDomainCLI, è possibile aggiungere il `--timeout-in-seconds` flag per aumentare il timeout fino a un massimo di 3.600 secondi.
- Verifica che l'utente di Active Directory che stai utilizzando per aggiungere il gateway al dominio disponga dei privilegi necessari per farlo.

Risoluzione dei problemi: utilizzo CloudWatch delle metriche

Di seguito puoi trovare informazioni sulle azioni per risolvere i problemi utilizzando i CloudWatch parametri di Amazon con Storage Gateway.

Argomenti

Il gateway reagisce lentamente durante la navigazione nelle directory

Se File Gateway reagisce lentamente quando esegui il ls comando o sfogli le directory, controlla le `IndexFetch` metriche and: `IndexEviction` CloudWatch

- Se la `IndexFetch` metrica è maggiore di 0 quando esegui un `ls` comando o sfogli le directory, File Gateway si è avviato senza informazioni sul contenuto della directory interessata e ha dovuto accedere ad per Windows File Server. Gli sforzi successivi per elencare i contenuti di tale directory dovrebbero avvenire più velocemente.
- Se la `IndexEviction` metrica è maggiore di 0, significa che File Gateway ha raggiunto il limite di ciò che può gestire nella cache in quel momento. In questo caso, File Gateway deve liberare dello spazio di archiviazione dalla directory a cui si accede meno di recente per elencare una nuova directory. Se ciò si verifica frequentemente e si verifica un impatto sulle prestazioni, contattateci Supporto.

Supporto Parla dei contenuti del relativo FSx file system Amazon e dei consigli per migliorare le prestazioni in base al tuo caso d'uso.

Il tuo gateway non risponde

Se il File Gateway non risponde, procedi come segue:

- Se di recente è stato eseguito un riavvio o aggiornamento software, controlla il parametro `IOWaitPercent`. Questa metrica mostra la percentuale di tempo in cui la CPU è inattiva quando c'è una richiesta di disco in sospeso. I/O In alcuni casi, questo valore potrebbe essere elevato (10 o maggiore) e potrebbe essere aumentato dopo il riavvio o l'aggiornamento del server. In questi casi, File Gateway potrebbe essere bloccato da un disco root lento mentre ricostruisce la cache degli indici in RAM. Puoi risolvere questo problema utilizzando un disco fisico più veloce per il disco root.
- Se la `MemUsedBytes` metrica è uguale o quasi uguale alla `MemTotalBytes` metrica, significa che File Gateway sta esaurendo la RAM disponibile. Assicurati che File Gateway disponga almeno della RAM minima richiesta. Se lo è già, valuta la possibilità di aggiungere più RAM al File Gateway in base al carico di lavoro e al caso d'uso.

  Se la condivisione file è SMB, il problema potrebbe anche essere dovuto al numero di client SMB connessi alla condivisione file. Controlla il parametro `SMBV(1/2/3)Sessions` per vedere il numero di client connessi in un dato momento. Se ci sono molti client connessi, potrebbe essere necessario aggiungere più RAM al File Gateway.

Non vedi file nel tuo FSx file system Amazon

Se noti che i file sul gateway non si riflettono nel FSx file system Amazon, controlla la `FilesFailingUpload` metrica. Se la metrica riporta che alcuni file non vengono caricati correttamente, controlla le tue notifiche sanitarie. Quando i file non vengono caricati, il gateway genera una notifica sanitaria contenente maggiori dettagli sul problema.

Non vedi istantanee precedenti nel tuo FSx file system Amazon

Alcune operazioni sui file su FSx File Gateway, come la ridenominazione delle cartelle di primo livello o la modifica delle autorizzazioni, possono comportare più operazioni sui file che comportano un I/O carico elevato sul file system FSx per Windows File Server. Se il file system non dispone di risorse prestazionali sufficienti per il carico di lavoro, il file system potrebbe eliminare le copie shadow perché

dà priorità alla disponibilità per la conservazione continua I/O rispetto alla conservazione delle copie shadow storiche.

Nella FSx console Amazon, consulta la pagina Monitoraggio e prestazioni per verificare se il provisioning del file system è insufficiente. In tal caso, puoi passare allo storage SSD, aumentare la capacità di throughput o aumentare gli IOPS SSD per gestire il tuo carico di lavoro.

Il tuo gateway è lento nel trasferimento dei dati su Amazon FSx

Se il tuo File Gateway trasferisce lentamente i dati su Amazon FSx for Windows File Server, procedi come segue:

- Se la `CachePercentDirty` metrica è pari o superiore a 80, File Gateway sta scrivendo i dati su disco più velocemente di quanto possa caricare i dati su Amazon FSx for Windows File Server. Valuta la possibilità di aumentare la larghezza di banda per il caricamento dal tuo File Gateway, di aggiungere uno o più dischi di cache, di rallentare le scritture dei client o di aumentare la capacità di throughput per Amazon FSx for Windows File Server associato.
- Se la `CachePercentDirty` metrica è bassa, controlla la metrica. `IoWaitPercent` Se `IoWaitPercent` è maggiore di 10, il File Gateway potrebbe essere ostacolato dalla velocità del disco di cache locale. Consigliamo dischi SSD (Solid State Drive) locali per la cache, preferibilmente NVM Express (). NVMe Se questi dischi non sono disponibili, prova a utilizzare più dischi di cache da dischi fisici separati per migliorare le prestazioni.

Il processo di backup del gateway non riesce o si verificano errori durante la scrittura sul gateway

Se il processo di backup di File Gateway non riesce o si verificano errori durante la scrittura su File Gateway, effettuate le seguenti operazioni:

- Se la `CachePercentDirty` metrica è pari o superiore al 90 percento, File Gateway non può accettare nuove scritture su disco perché lo spazio disponibile sul disco della cache non è sufficiente. Per vedere la velocità di caricamento di File Gateway S3 per Windows File Server, visualizza `CloudBytesUploaded` la metrica. Confronta questa metrica con la `WriteBytes` metrica, che mostra la velocità con cui il client scrive file sul tuo File Gateway. Se il client SMB sta scrivendo sul tuo File Gateway più velocemente di quanto possa caricare S3 per Windows File Server, aggiungi altri dischi di cache per coprire al minimo le dimensioni del processo di backup. In alternativa, aumenta la larghezza di banda di caricamento.

- Se una copia di file di grandi dimensioni, ad esempio un processo di backup, fallisce ma la `CachePercentDirty` metrica è inferiore all'80%, File Gateway potrebbe raggiungere un timeout della sessione lato client. Per SMB, è possibile aumentare questo timeout utilizzando il comando. PowerShell `Set-SmbClientConfiguration -SessionTimeout 300` L'esecuzione di questo comando imposta il timeout su 300 secondi.

Notifiche di stato della disponibilità elevata

Quando si esegue il gateway sulla piattaforma VMware vSphere High Availability (HA), è possibile ricevere notifiche sullo stato. Per ulteriori informazioni sulle notifiche sullo stato, consulta Risoluzione dei problemi: problemi di alta disponibilità.

Risoluzione dei problemi: problemi di alta disponibilità

Di seguito sono riportate le informazioni sulle azioni da intraprendere in caso di problemi di disponibilità.

Argomenti

Notifiche di stato

Quando esegui il gateway su VMware vSphere HA, tutti i gateway generano le seguenti notifiche di integrità al gruppo di log Amazon CloudWatch configurato. Queste notifiche vengono inserite in un flusso di log chiamato `AvailabilityMonitor`.

Argomenti

Notifica: riavvio

Puoi ricevere una notifica di riavvio quando la VM del gateway viene riavviata. Puoi riavviare una macchina virtuale gateway utilizzando la console di gestione VM Hypervisor o la console Storage Gateway. È inoltre possibile riavviare utilizzando il software del gateway durante il ciclo di manutenzione del gateway.

Operazione da eseguire

Se il riavvio viene eseguito entro 10 minuti dall'ora di avvio della manutenzione configurata del gateway, probabilmente si tratta di un evento normale e non un'indicazione di problema. Se il riavvio è stato eseguito al di fuori della finestra di manutenzione in modo significativo, verifica se il gateway è stato riavviato manualmente.

Notifica: HardReboot

Puoi ricevere una notifica `HardReboot` quando la VM del gateway viene riavviata in modo imprevisto. Questo riavvio può essere dovuto a mancanza di alimentazione, a un guasto hardware o a un altro evento. Per i VMware gateway, un ripristino da parte di vSphere High Availability Application Monitoring può causare questo evento.

Operazione da eseguire

Quando il gateway funziona in un ambiente di questo tipo, verifica la presenza della `HealthCheckFailure` notifica e consulta il registro VMware degli eventi per la macchina virtuale.

Notifica: HealthCheckFailure

Per un gateway su VMware vSphere HA, è possibile ricevere una `HealthCheckFailure` notifica quando un controllo di integrità fallisce e viene richiesto il riavvio della macchina virtuale. Questo evento si verifica anche durante un test per monitorare la disponibilità, indicato da una notifica `AvailabilityMonitorTest`. In questo caso, la notifica `HealthCheckFailure` è prevista.

> **Note**
>
> Questa notifica è valida solo per i VMware gateway.

Operazione da eseguire

Se questo evento si verifica ripetutamente senza notifica `AvailabilityMonitorTest`, verifica la presenza di problemi nell'infrastruttura VM (storage, memoria e così via). Se hai bisogno di ulteriore assistenza, contatta Supporto.

Notifica: AvailabilityMonitorTest

Per un gateway su VMware vSphere HA, è possibile ricevere una `AvailabilityMonitorTest` notifica quando si esegue un test del sistema di monitoraggio della disponibilità e delle applicazioni in. VMware

Metriche

Il parametro `AvailabilityNotifications` è disponibile in tutti i gateway. Questo parametro è il conteggio del numero di notifiche di stato relative alla disponibilità generate dal gateway. Utilizza la statistica `Sum` per verificare se il gateway sta riscontrando eventi correlati alla disponibilità. Consultate il gruppo di CloudWatch log configurato per i dettagli sugli eventi.

Le migliori pratiche per File Gateway

Questa sezione contiene gli argomenti seguenti, che forniscono informazioni sulle migliori pratiche per lavorare con gateway, condivisioni di file, bucket e dati. Ti consigliamo di acquisire familiarità con le informazioni descritte in questa sezione e di provare a seguire queste linee guida per evitare problemi con il tuo. Gateway di archiviazione AWS Per ulteriori indicazioni sulla diagnosi e la risoluzione dei problemi più comuni che potresti riscontrare durante la distribuzione, consulta. Risoluzione dei problemi relativi all'implementazione dello Storage Gateway

Argomenti

Migliori pratiche: ripristino dei dati

Sebbene improbabile, si potrebbe verificare un errore irreversibile del gateway. Tale errore può verificarsi nella macchina virtuale (VM), nel gateway stesso, nello storage locale o in altre posizioni. Se si verifica un errore, è consigliabile seguire le istruzioni nella sezione appropriata di seguito per ripristinare i dati.

> **Important**
>
> Storage Gateway non supporta il ripristino di una macchina virtuale del gateway da uno snapshot creato dall'hypervisor o dall'Amazon Machine Image (AMI) di Amazon EC2. Se la macchina virtuale del gateway non funziona correttamente, attiva un nuovo gateway e ripristina i dati in tale gateway in base alle istruzioni seguenti.

Ripristino da un arresto imprevisto della macchina virtuale

Se la macchina virtuale si arresta in modo imprevisto, ad esempio in caso di interruzione dell'alimentazione, il gateway diventa irraggiungibile. Quando l'alimentazione e la connettività di rete vengono ripristinate, il gateway diventa raggiungibile e inizia a funzionare normalmente. Di seguito sono elencate alcune fasi da seguire per ripristinare i dati:

- Se un'interruzione provoca problemi di connettività di rete, è possibile risolvere il problema. Per informazioni su come testare la connettività di rete, consulta Verifica della connettività di rete del gateway.

Ripristino dei dati da un disco della cache malfunzionante

Se nel disco della cache si verifica un errore, è consigliabile usare le opzioni seguenti per ripristinare i dati, in base alla situazione:

- Se il malfunzionamento si è verificato perché un disco della cache è stato rimosso dall'host, arresta il gateway, aggiungi di nuovo il disco e riavvia il gateway.

Ripristino dei dati da un data center inaccessibile

Se il gateway o il data center diventa inaccessibile per qualsiasi motivo, è possibile ripristinare i dati in un altro gateway in un data center diverso oppure in un gateway ospitato in un'istanza Amazon EC2. Se non hai accesso a un altro data center, è consigliabile creare il gateway in un'istanza Amazon EC2. Le fasi da seguire dipendono dal tipo di gateway da cui vengono ripristinati i dati.

Per recuperare i dati da un File Gateway in un data center inaccessibile

Per File Gateway, mappi un nuovo file al per Windows File Server che contiene i dati che desideri ripristinare.

1. Crea e attiva un nuovo File Gateway su un host Amazon EC2. Per ulteriori informazioni, consulta Implementa un host FSx Amazon EC2 predefinito per File Gateway.
2. Crea un nuovo di file sul gateway EC2 che hai creato. Per ulteriori informazioni, consulta Creare un file system FSx per Windows File Server.
3. Installa il file sul client e mappalo al per Windows File Server che contiene i dati che desideri ripristinare. Per ulteriori informazioni, consulta Mount e utilizzare la condivisione di file.

Ripristino da backup o istantanee direttamente su Amazon FSx

In alcuni casi, potrebbe essere necessario ripristinare i dati direttamente sul FSx file system Amazon, utilizzando un backup o uno snapshot di un momento precedente. In questi casi, esiste il rischio di creare uno scenario di doppia scrittura tra l'applicazione di backup e il FSx File Gateway, che può

causare file bloccati o non corrispondenti. Per evitare problemi durante il ripristino FSx del file system Amazon da backup o istantanee, utilizza la seguente procedura.

> **Note**
>
> Tutti i dati memorizzati nella cache attualmente archiviati su FSx File Gateway non saranno validi dopo aver ripristinato il FSx file system Amazon da un backup o da uno snapshot utilizzando questa procedura.

Per evitare problemi durante il ripristino del FSx file system Amazon da backup o istantanee

1. Scollega il FSx file system Amazon dal FSx File Gateway utilizzando la console Storage Gateway.
2. Ripristina il backup o lo snapshot direttamente sul tuo FSx file system Amazon.
3. Ricollega il FSx file system Amazon al FSx File Gateway utilizzando la console Storage Gateway.

Pulisci le risorse non necessarie

Come best practice, consigliamo di ripulire le risorse di Storage Gateway per evitare addebiti imprevisti o non necessari. Ad esempio, se hai creato un gateway come esercizio dimostrativo o come test, valuta la possibilità di eliminarlo insieme alla relativa appliance virtuale dalla distribuzione. Utilizzare la procedura seguente per ripulire le risorse.

Per eliminare risorse non necessarie

1. Se non intendi più continuare a utilizzare un gateway, eliminalo. Per ulteriori informazioni, consulta Eliminazione del gateway e rimozione delle risorse associate.
2. Eliminare la macchina virtuale Storage Gateway dall'host on-premise. Se è stato creato un proprio gateway su un'istanza Amazon EC2, terminare l'istanza.

Risorse Storage Gateway aggiuntive

Questa sezione contiene i seguenti argomenti, che forniscono informazioni e risorse aggiuntive relative alla configurazione e all'utilizzo Gateway di archiviazione AWS:

Argomenti

- Configurazione dell'host- Scopri come distribuire e configurare un host di macchina virtuale per il tuo gateway.
- Utilizzo di Storage Gateway con VMware HA- Scopri come configurare Storage Gateway per funzionare con le funzionalità di alta disponibilità di VMware vSphere.
- Ottenere la chiave di attivazione- Scopri dove trovare la chiave di attivazione da fornire quando installi un nuovo gateway.
- Usando Direct Connect- Scopri come creare una connessione di rete dedicata tra il gateway locale e il AWS cloud.
- Autorizzazioni Active Directory- Scopri quali autorizzazioni deve avere il tuo account di servizio per poter aggiungere il gateway al tuo dominio Active Directory.
- Ottenere l'indirizzo IP per il dispositivo gateway- Scopri dove trovare l'indirizzo IP dell'host della macchina virtuale del gateway, che devi fornire quando installi un nuovo gateway.
- Comprendere le risorse e le risorse IDs- Scopri come AWS identifica le risorse e le sottorisorse create da Storage Gateway.
- Tagging delle risorse - Scopri come utilizzare i tag di metadati per classificare le risorse e renderle più facili da gestire.
- Componenti open source- Scopri gli strumenti e le licenze di terze parti utilizzati per fornire la funzionalità Storage Gateway.
- Quote- Scopri i limiti e le quote per File Gateway, incluse le limitazioni minime e massime per le condivisioni di file e i dischi di cache locali.

Implementazione e configurazione dell'host VM gateway

I seguenti argomenti forniscono informazioni sulla configurazione della piattaforma host della macchina virtuale per il gateway.

Argomenti

- Implementa un host FSx Amazon EC2 predefinito per File Gateway

- Implementa un host FSx Amazon EC2 personalizzato per File Gateway
- Modifica le opzioni dei metadati delle istanze Amazon EC2
- Sincronizza l'ora della macchina virtuale con l'ora dell'host KVM Hyper-V o Linux
- Sincronizza l'ora della macchina virtuale con l'ora dell'host VMware
- Configurazione degli adattatori di rete per il gateway
- Utilizzo di VMware vSphere High Availability con Storage Gateway

Implementa un host FSx Amazon EC2 predefinito per File Gateway

Questo argomento elenca i passaggi per implementare un host Amazon EC2 utilizzando le specifiche predefinite.

Puoi distribuire e attivare un su un'istanza Amazon Elastic Compute Cloud (Amazon EC2). L'AMI (Amazon Machine Image) del Gateway di archiviazione AWS è disponibile come AMI della community.

> **Note**
>
> La community AMIs di Storage Gateway è pubblicata e completamente supportata da AWS. Come si può vedere AWS, l'editore è un fornitore verificato.

1. Per configurare l'istanza Amazon EC2, scegli Amazon EC2 come piattaforma host nella sezione Opzioni piattaforma del flusso di lavoro. Per istruzioni sulla configurazione dell'istanza Amazon EC2, . FSx
2. Seleziona Launch instance per aprire il modello Gateway di archiviazione AWS AMI nella console Amazon EC2 e personalizzare impostazioni aggiuntive come tipi di istanza, impostazioni di rete e Configura storage.
3. Facoltativamente, puoi selezionare Usa le impostazioni predefinite nella console Storage Gateway per implementare un'istanza Amazon EC2 con la configurazione predefinita.

   L'istanza Amazon EC2 creata da Usa le impostazioni predefinite ha le seguenti specifiche predefinite:

   - Tipo di istanza: m5.xlarge
   - Impostazioni di rete

- Per VPC, seleziona il VPC nel quale desideri che venga eseguita l'istanza EC2.
- Per Sottorete, specifica la sottorete in cui deve essere avviata l'istanza EC2.

> **Note**
>
> Le sottoreti VPC verranno visualizzate nel menu a discesa solo se hanno l'impostazione di assegnazione automatica dell'indirizzo IP pubblico attivata dalla console di gestione VPC.

- Assegnazione automatica di IP pubblico: attivata
- Un gruppo di sicurezza EC2 viene creato e associato all'istanza EC2. Il gruppo di sicurezza presenta le seguenti regole per la porta in ingresso:

> **Note**
>
> È necessario che la porta 80 sia aperta durante l'attivazione del gateway. La porta viene chiusa immediatamente dopo l'attivazione. Successivamente, è possibile accedere all'istanza EC2 solo tramite le altre porte del VPC selezionato.
> Le condivisioni di file sul gateway sono accessibili solo dagli host nello stesso VPC del gateway. Se è necessario accedere alle condivisioni di file da host esterni al VPC, è necessario aggiornare le regole del gruppo di sicurezza appropriate.
> Puoi modificare i gruppi di sicurezza in qualsiasi momento accedendo alla pagina dei dettagli dell'istanza Amazon EC2, selezionando Sicurezza, accedendo a Dettagli del gruppo di sicurezza e scegliendo l'ID del gruppo di sicurezza.

Porta	Protocollo	Protocollo del file system
80	TCP	Accesso HTTP per l'attivazione
137	UDP	NetBIOS

Porta	Protocollo	Protocollo del file system
138	UDP	NetBIOS
139	TCP, UDP	SMB
389	TCP	LDAP
445	TCP	SMB

- Configurare l'archiviazione

Impostazioni predefinite	Volume root AMI	Cache del volume 2
Nome dispositivo		'/dev/sdb'
Dimensione	80 GiB	165 GiB
Tipo di volume	gp3	gp3
IOPS	3000	3000
Elimina al termine	Sì	Sì
Crittografato	No	No
Throughput	125	125

Implementa un host FSx Amazon EC2 personalizzato per File Gateway

Puoi distribuire e attivare un su un'istanza Amazon Elastic Compute Cloud (Amazon EC2). L'AMI (Amazon Machine Image) del Gateway di archiviazione AWS è disponibile come AMI della community.

> **Note**
>
> La community AMIs di Storage Gateway è pubblicata e completamente supportata da AWS. Come si può vedere AWS, l'editore è un fornitore verificato.
> AMIs utilizza la seguente convenzione di denominazione. Il numero di versione aggiunto al nome AMI cambia con ogni versione rilasciata.
> `aws-storage-gateway-FILE_FSX_SMB-2.2.3`

Per distribuire un'istanza Amazon EC2 per ospitare il tuo Amazon FSx File Gateway

1. Inizia la configurazione di un nuovo gateway utilizzando la console Storage Gateway. Per istruzioni, consulta Configurare un Amazon FSx File Gateway. Quando raggiungi la sezione Opzioni piattaforma, scegli Amazon EC2 come piattaforma host, quindi segui i passaggi seguenti per avviare l'istanza Amazon EC2 che ospiterà il tuo File Gateway.
2. Scegli Launch instance per aprire il modello Gateway di archiviazione AWS AMI nella console Amazon EC2, dove puoi configurare impostazioni aggiuntive.

   Usa Quicklaunch per avviare l'istanza Amazon EC2 con le impostazioni predefinite. Per ulteriori informazioni sulle specifiche predefinite di Amazon EC2 Quicklaunch, consulta Quicklaunch Configuration Specifications for .
3. Per Nome, inserire un nome per l'istanza Amazon EC2. Dopo aver implementato l'istanza, puoi cercare questo nome per trovare l'istanza nelle pagine di elenco nella console Amazon EC2.
4. Nella sezione Tipo di istanza, per Tipo di istanza scegli la configurazione hardware per l'istanza. La configurazione hardware deve soddisfare determinati requisiti minimi per supportare il gateway. Consigliamo di iniziare con il tipo di istanza m5.xlarge, che soddisfa i requisiti minimi di hardware per il funzionamento corretto del gateway. Per ulteriori informazioni, consulta Requisiti per i tipi di istanze Amazon EC2.

   È possibile ridimensionare l'istanza dopo l'avvio, se necessario. Per ulteriori informazioni, consulta Resizing your istance nella Amazon EC2 User Guide.

> **Note**
>
> Alcuni tipi di istanze, in particolare i3 EC2, utilizzano dischi SSD. NVMe Questi possono causare problemi all'avvio o all'arresto di File Gateway; ad esempio, è possibile perdere dati dalla cache. Monitora la CloudWatch metrica di `CachePercentDirty` Amazon e avvia o arresta il sistema solo quando tale parametro lo è`0`. Per ulteriori informazioni sui parametri di monitoraggio per il gateway, consulta Metriche e dimensioni dello Storage Gateway nella CloudWatch documentazione.

5. Nella sezione Coppia di chiavi (accesso), in Nome coppia di chiavi: obbligatorio, seleziona la coppia di chiavi che desideri utilizzare per connetterti in modo sicuro alla tua istanza. Se necessario, è possibile creare una nuova coppia di chiavi. Per ulteriori informazioni, consulta Creazione di una coppia di chiavi nella Guida per l'utente di Amazon Elastic Compute Cloud per istanze Linux.
6. Nella sezione Impostazioni di rete, rivedi le impostazioni preconfigurate e scegli Modifica per apportare modifiche ai seguenti campi:
   a. Per VPC: obbligatorio, scegli il VPC in cui vuoi lanciare l'istanza Amazon EC2. Per ulteriori informazioni, consulta Come funziona Amazon VPC nella Guida per l'utente di Amazon Virtual Private Cloud.
   b. (Facoltativo) Per Sottorete, scegli la sottorete in cui vuoi lanciare l'istanza Amazon EC2.
   c. Per Assegna automaticamente IP pubblico, scegli Abilita.
7. Nella sottosezione Firewall (gruppi di sicurezza), rivedi le impostazioni preconfigurate. Puoi modificare il nome e la descrizione predefiniti del nuovo gruppo di sicurezza da creare per la tua istanza Amazon EC2, se lo desideri, oppure scegliere di applicare le regole firewall di un gruppo di sicurezza esistente.
8. Nella sottosezione Regole dei gruppi di sicurezza in ingresso, aggiungi le regole firewall per aprire le porte che i client utilizzeranno per connettersi alla tua istanza. Per ulteriori informazioni sulle porte richieste per Gateway, consulta Requisiti delle porte. Per ulteriori informazioni sull'aggiunta di regole firewall, consulta Regole del gruppo di sicurezza nella Guida per l'utente di Amazon Elastic Compute Cloud per le istanze Linux.

> **Note**
>
> Amazon FSx File Gateway richiede che la porta TCP 80 sia aperta per il traffico in entrata e l'accesso HTTP una tantum durante l'attivazione del gateway. Dopo l'attivazione, è possibile chiudere questa porta.
> Inoltre, è necessario aprire la porta TCP 445 per l'accesso SMB, la porta UDP 137 per l'accesso NetBIOS, la porta UDP 138 per l'accesso NetBIOS e la porta TCP 389 per l'accesso LDAP.

9. Nella sottosezione Configurazione di rete avanzata, rivedere le impostazioni preconfigurate e, se necessario, apportare modifiche.
10. Nella sezione Configura archiviazione scegliere Aggiungi nuovo volume per aggiungere spazio di archiviazione all'istanza del gateway.

> **Important**
>
> È necessario aggiungere almeno un volume Amazon EBS con almeno 150 GiB di capacità per lo storage della cache oltre al volume root preconfigurato. Per migliorare le prestazioni, consigliamo di allocare più volumi EBS per lo storage della cache con almeno 150 GiB ciascuno.

11. Nella sezione Dettagli avanzati, rivedi le impostazioni preconfigurate e apporta le modifiche se necessario.
12. Scegli Avvia istanza per avviare la nuova istanza gateway Amazon EC2 con le impostazioni configurate.
13. Per verificare che la tua nuova istanza sia stata avviata correttamente, vai alla pagina Istanze nella console Amazon EC2 e cerca la nuova istanza per nome. Assicurati che in Stato dell'istanza sia visualizzato In esecuzione con un segno di spunta verde e che il Controllo dello stato sia completo e mostri un segno di spunta verde.
14. Seleziona l'istanza dalla pagina dei dettagli. Copia l'indirizzo IP pubblico dalla sezione di riepilogo dell'istanza, quindi torna alla pagina Configura gateway nella console Storage Gateway per riprendere la configurazione di Amazon . FSx

È possibile determinare l'ID AMI da utilizzare per avviare un File Gateway utilizzando la console Storage Gateway o interrogando l'archivio AWS Systems Manager dei parametri.

Per determinare l'ID AMI, procedi in uno dei seguenti modi:

- Inizia la configurazione di un nuovo gateway utilizzando la console Storage Gateway. Per istruzioni, consulta Configurare un Amazon FSx File Gateway. Quando raggiungi la sezione Opzioni piattaforma, scegli Amazon EC2 come piattaforma host, quindi scegli Launch instance per aprire il modello Gateway di archiviazione AWS AMI nella console Amazon EC2.

  Verrai reindirizzato alla pagina AMI della community EC2, dove puoi vedere l'ID AMI per la tua AWS regione nell'URL.
- Esegui una query sull'archivio dei parametri Systems Manager. È possibile utilizzare l'API AWS CLI o Storage Gateway per interrogare il parametro pubblico Systems Manager nello spazio dei nomi `/aws/service/storagegateway/ami/FILE_FSX_SMB/latest`. Ad esempio, l'utilizzo del seguente comando CLI restituisce l'ID dell'AMI corrente nel campo Regione AWS specificato.

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
  FILE_FSX_SMB/latest
  ```

  Il comando CLI restituisce un output simile al seguente:

  ```
  {
      "Parameter": {
          "Type": "String",
          "LastModifiedDate": 1561054105.083,
          "Version": 18,
           "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
  FILE_FSX_SMB/latest",
           "Name": "/aws/service/storagegateway/ami/FILE_FSX_SMB/latest",,
          "Value": "ami-033d1edba5606cffb"
      }
  }
  ```

Modifica le opzioni dei metadati delle istanze Amazon EC2

Il servizio di metadati dell'istanza (IMDS) è un componente su istanza che fornisce un accesso sicuro ai metadati delle istanze Amazon EC2. Un'istanza può essere configurata per accettare richieste di metadati in entrata che utilizzano IMDS versione 1 (IMDSv1) o richiedere che tutte le richieste di metadati utilizzino IMDS versione 2 (). IMDSv2 IMDSv2 utilizza richieste orientate alla sessione e mitiga diversi tipi di vulnerabilità che potrebbero essere utilizzate per tentare di accedere all'IMDS.

Per informazioni su IMDSv2, consulta Come funziona Instance Metadata Service versione 2 nella Amazon Elastic Compute Cloud User Guide.

Ti consigliamo di richiedere IMDSv2 per tutte le istanze Amazon EC2 che ospitano Storage Gateway. IMDSv2 è obbligatorio per impostazione predefinita su tutte le istanze gateway appena lanciate. Se disponi di istanze esistenti che sono ancora configurate per accettare richieste di IMDSv1 metadati, consulta Require the use of IMDSv2 nella Amazon Elastic Compute Cloud User Guide per istruzioni su come modificare le opzioni di metadati dell'istanza di cui richiedere l'uso. IMDSv2 L'applicazione di questa modifica non richiede il riavvio dell'istanza.

Sincronizza l'ora della macchina virtuale con l'ora dell'host KVM Hyper-V o Linux

Per un gateway distribuito su VMware ESXi, l'impostazione dell'ora dell'host dell'hypervisor e la sincronizzazione dell'ora della macchina virtuale con l'host sono sufficienti per evitare variazioni di orario. Per ulteriori informazioni, consulta Sincronizza l'ora della macchina virtuale con l'ora dell'host VMware. Per un gateway distribuito su Microsoft Hyper-V o Linux KVM, si consiglia di controllare periodicamente l'ora della macchina virtuale utilizzando la procedura descritta di seguito.

Per visualizzare e sincronizzare l'ora di una macchina virtuale gateway hypervisor con un server Network Time Protocol (NTP)

1. Accedere alla console locale del gateway:

   - Per ulteriori informazioni sull'accesso alla console locale di Microsoft Hyper-V, consultare Accesso alla console locale del gateway con Microsoft Hyper-V.
   - Per ulteriori informazioni sull'accesso alla console locale per una macchina virtuale basata su kernel Linux (KVM), vedere. Accesso alla console locale del gateway con Linux KVM
2. Nella schermata del menu principale di Storage Gateway Configuration, immettere il numero corrispondente per selezionare System Time Management.
3. Nella schermata del menu System Time Management, immettere il numero corrispondente per selezionare Visualizza e sincronizza l'ora del sistema.

   La console locale del gateway visualizza l'ora corrente del sistema e la confronta con l'ora riportata dal server NTP, quindi riporta l'esatta discrepanza tra i due orari in secondi.
4. Se la discrepanza temporale è superiore a 60 secondi, immettere **y** per sincronizzare l'ora del sistema con l'ora NTP. In caso contrario, inserire **n**.

La sincronizzazione dell'ora potrebbe richiedere alcuni minuti.

Sincronizza l'ora della macchina virtuale con l'ora dell'host VMware

Per attivare il gateway, devi assicurarti che la data e l'ora della macchina virtuale siano sincronizzate con quelle dell'host e che queste siano impostate correttamente. In questa sezione devi prima sincronizzare la data e l'ora nella macchina virtuale con quelle dell'host. Devi quindi controllare la data e l'ora dell'host e, se necessario, impostarle e configurare l'host per la sincronizzazione automatica con un server NTP (Network Time Protocol).

> **Important**
>
> La sincronizzazione della data e dell'ora della macchina virtuale con quelle dell'host è necessaria per una corretta attivazione del gateway.

Per sincronizzare la data e l'ora della macchina virtuale con quelle dell'host

1. Configurare la data e l'ora della macchina virtuale.

   a. Nel client vSphere, fare clic con il pulsante destro del mouse sul nome della macchina virtuale gateway nel pannello sul lato sinistro della finestra dell'applicazione per aprire il menu contestuale della macchina virtuale, quindi scegliere Modifica impostazioni.

      Viene visualizzata la finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale).

   b. Scegli la scheda Opzioni, quindi scegli VMware Strumenti dall'elenco delle opzioni.

   c. Seleziona l'opzione Sincronizza l'ora dell'ospite con l'host nella sezione Avanzate sul lato destro della finestra di dialogo Proprietà della macchina virtuale, quindi scegli OK.

      La macchina virtuale sincronizza le proprie data e ora con quelle dell'host.

2. Configurare la data e l'ora dell'host.

   È importante verificare che l'orologio dell'host sia impostato sulla data e sull'ora corrette. Se non hai configurato l'orologio dell'host, completa la procedura seguente per impostarlo e sincronizzarlo con un server NTP.

a. Nel client VMware vSphere, selezionare il nodo host vSphere nel pannello a sinistra, quindi scegliere la scheda Configurazione.

b. Selezionare Time Configuration (Configurazione data e ora) nel pannello Software e quindi scegliere il collegamento Properties (Proprietà).

   Viene visualizzata la finestra di dialogo Time Configuration (Configurazione data e ora).

c. In Data e ora, impostare la data e l'ora per l'host vSphere.

d. Configurare l'host per la sincronizzazione automatica di data e ora con un server NTP.

   i. Scegli Opzioni nella finestra di dialogo Time Configuration, quindi nella finestra di dialogo Opzioni NTP Daemon (ntpd), scegli Impostazioni NTP nel pannello di sinistra.

   ii. Scegliere Add (Aggiungi) per aggiungere un nuovo server NTP.

   iii. Nella finestra di dialogo Add NTP Server (Aggiungi server NTP) digitare l'indirizzo IP o il nome di dominio completo di un server NTP e quindi scegliere OK.

   È possibile utilizzare `pool.ntp.org` come nome di dominio.

   iv. Nella finestra di dialogo Opzioni del demone NTP (ntpd), scegli Generale nel pannello di sinistra.

   v. In Comandi di servizio, scegliete Avvia per avviare il servizio.

   Se si modifica questo riferimento al server NTP o successivamente si aggiunge un altro server, sarà necessario riavviare il servizio per usare il nuovo server.

e. Scegliere OK per chiudere la finestra di dialogo NTP Daemon (ntpd) Options (Opzioni daemon NTP - ntpd).

f. Scegliere OK per chiudere la finestra di dialogo Time Configuration (Configurazione data e ora).

Configurazione degli adattatori di rete per il gateway

Storage Gateway utilizza un singolo adattatore di rete VMXNET3 (10 GbE) per impostazione predefinita, ma è possibile configurare il gateway in modo che utilizzi più di un adattatore di rete in modo che sia accessibile da più indirizzi IP. Tale condizione torna utile nei seguenti casi:

- Massimizzazione del throughput: è possibile massimizzare la velocità di trasmissione verso un gateway quando gli adattatori di rete rappresentano un collo di bottiglia.

- Separazione delle applicazioni: potrebbe essere necessario distinguere le modalità di scrittura delle applicazioni sui volumi di un gateway. Potresti, ad esempio, scegliere di far utilizzare a un'applicazione critica di storage una scheda apposita per il tuo gateway.
- Vincoli di rete: l'ambiente applicativo potrebbe richiedere di mantenere le condivisioni di file e gli iniziatori che si connettono ad esse in una rete isolata. Tale rete è diversa da quella con cui il gateway comunica con AWS.

In un tipico caso di utilizzo con più adattatori, un adattatore è configurato come route con cui il gateway comunica AWS (ovvero come gateway predefinito). Ad eccezione di questo adattatore, gli iniziatori devono trovarsi nella stessa sottorete dell'adattatore che contiene le condivisioni di file a cui si connettono. per non compromettere la comunicazione con le destinazioni programmate. Se una destinazione è configurata sullo stesso adattatore con cui viene utilizzata la comunicazione AWS, il traffico di condivisione di file per quella destinazione e il AWS traffico fluiscono attraverso lo stesso adattatore.

In alcuni casi, è possibile configurare un adattatore per la connessione alla console Storage Gateway e quindi aggiungere un secondo adattatore. In tal caso, Storage Gateway configura automaticamente la tabella di routing per utilizzare il secondo adattatore come route preferita. Per istruzioni su come configurare più adattatori, vedere i seguenti argomenti:

Argomenti

- Configurazione del gateway per più utenti NICs su un host VMware ESXi
- Configurazione del gateway per più utenti NICs in Microsoft Hyper-V Host

Configurazione del gateway per più utenti NICs su un host VMware ESXi

La procedura seguente presuppone che la macchina virtuale gateway disponga già di una scheda di rete definita e descrive come aggiungerne una. VMware ESXi

Per configurare il gateway per l'utilizzo di un adattatore di rete aggiuntivo nell'host VMware ESXi

1. Arresta il gateway.
2. Nel client VMware vSphere, selezionare la macchina virtuale gateway.

   Per questa procedura, la macchina virtuale può rimanere attiva.
3. Nel client, apri il menu contestuale (clic con il pulsante destro del mouse) per la VM del gateway e scegli Edit Settings (Modifica impostazioni).

4. Nella scheda Hardware della finestra di dialogo Virtual Machine Properties (Proprietà macchina virtuale), scegli Add (Aggiungi) per aggiungere un dispositivo.
5. Segui la procedura guidata Add Hardware (Aggiungi hardware) per aggiungere una scheda di rete.

   a. Nel riquadro Device Type (Tipo di dispositivo), scegli Ethernet Adapter (Scheda Ethernet) per aggiungere una scheda, quindi scegli Next (Avanti).

   b. Nel riquadro Network Type (Tipo di rete), assicurati che Connect at power on (Connetti all'accensione) sia selezionato per Type (Tipo), quindi scegli Next (Avanti).

      Si consiglia di utilizzare l'adattatore di VMXNET3 rete con Storage Gateway. Per ulteriori informazioni sui tipi di adattatore che potrebbero apparire nell'elenco degli adattatori, vedere Tipi di adattatori di rete nella ESXi documentazione di vCenter Server.

   c. Nel riquadro Ready to Complete (Pronto al completamento), rivedi le informazioni, quindi scegli Finish (Fine).
6. Scegli la scheda Riepilogo della VM, quindi scegli Visualizza tutto accanto alla casella Indirizzo IP. Nella finestra Indirizzi IP macchina virtuale vengono visualizzati tutti gli indirizzi IP da poter utilizzare per accedere al gateway. Verifica che un secondo indirizzo IP sia elencato per il gateway.

   > **Note**
   >
   > Potrebbero volerci alcuni istanti prima che le modifiche della scheda diventino effettive e che le informazioni di riepilogo della VM si aggiornino.
7. Nella console Storage Gateway, accendere il gateway.
8. Nel riquadro Navigazione della console Storage Gateway, scegliere Gateway, quindi scegliere il gateway a cui aggiungere la scheda. Verificare che il secondo indirizzo IP sia presente nell'elenco nella scheda Details (Dettagli).

Per informazioni sulle attività della console locale comuni agli VMware host Hyper-V e KVM, vedere Esecuzione di attività sulla console locale della macchina virtuale

Configurazione del gateway per più utenti NICs in Microsoft Hyper-V Host

La procedura seguente presuppone che la macchina virtuale del gateway disponga già di una scheda di rete definita e che si aggiunga una seconda scheda. Questa procedura mostra come aggiungere una scheda per un host Microsoft Hyper-V.

Per configurare il gateway per l'uso di una scheda di rete aggiuntiva in un host Microsoft Hyper-V

1. Nella console Storage Gateway, spegnere il gateway.
2. In Microsoft Hyper-V Manager, seleziona la tua macchina virtuale gateway dal pannello Macchine virtuali.
3. Se la macchina virtuale gateway non è già disattivata, fai clic con il pulsante destro del mouse sul nome della macchina virtuale per aprire il menu contestuale, quindi scegli Disattiva.
4. Fai clic con il pulsante destro del mouse sul nome della macchina virtuale del gateway per aprire il menu contestuale, quindi scegli Impostazioni.
5. Nella finestra di dialogo Impostazioni, in Hardware, scegli Aggiungi hardware.
6. Nel pannello Aggiungi hardware sul lato destro della finestra di dialogo Impostazioni, scegli Adattatore di rete, quindi scegli Aggiungi per aggiungere un dispositivo.
7. Configurare la scheda di rete e quindi scegliere Apply (Applica) per applicare le impostazioni.
8. Nella finestra di dialogo Impostazioni, in Hardware, confermate che la nuova scheda di rete è stata aggiunta all'elenco hardware, quindi scegliete OK.
9. Accendere il gateway utilizzando la console Storage Gateway.
10. Nel pannello di navigazione della console Storage Gateway, scegli Gateway, quindi seleziona il gateway a cui hai aggiunto l'adattatore. Conferma che un secondo indirizzo IP sia elencato nella scheda Dettagli.

Per informazioni sulle attività della console locale comuni agli host VMware Hyper-V e KVM, vedere Esecuzione di attività sulla console locale della macchina virtuale

Utilizzo di VMware vSphere High Availability con Storage Gateway

Storage Gateway offre un'elevata disponibilità VMware tramite una serie di controlli di integrità a livello di applicazione integrati con VMware vSphere High Availability (HA). VMware Questo approccio consente di proteggere i carichi di lavoro di storage da errori di hardware, hypervisor o rete. Consente inoltre di proteggere da errori di software, come il timeout di connessione e condivisione file o l'indisponibilità del volume.

Con questa integrazione, un gateway distribuito in un VMware ambiente locale o in un VMware cloud on si ripristina AWS automaticamente dalla maggior parte delle interruzioni del servizio. Generalmente il processo dura meno di 60 secondi senza perdita di dati.

> **Note**
>
> Si consiglia di effettuare le seguenti operazioni se si implementa Storage Gateway in un cluster VMware HA:
>
> - Implementare il pacchetto scaricabile VMware ESX .ova che contiene la macchina virtuale Storage Gateway su un solo host in un cluster.
> - Quando si distribuisce il pacchetto .ova, selezionare un data store che non sia locale su un host. Al contrario, utilizzare un datastore accessibile a tutti gli host del cluster. Se si seleziona un datastore locale per un host e l'host ha esito negativo, l'origine dati potrebbe non essere accessibile ad altri host del cluster e il failover su un altro host potrebbe non riuscire.
> - Con il clustering, se distribuisci il pacchetto .ova nel cluster, seleziona un host quando ti viene richiesto di farlo. In alternativa, puoi distribuire direttamente a un host in un cluster.

I seguenti argomenti descrivono come implementare Storage Gateway in un cluster VMware HA:

Argomenti

Configurazione del cluster vSphere VMware HA

Innanzitutto, se non hai già creato un VMware cluster, creane uno. Per informazioni su come creare un VMware cluster, vedere Create a vSphere HA Cluster nella VMware documentazione.

Successivamente, configura il VMware cluster in modo che funzioni con Storage Gateway.

Per configurare il VMware cluster

1. Nella pagina Modifica impostazioni cluster in VMware vSphere, assicurarsi che il monitoraggio delle macchine virtuali sia configurato per il monitoraggio delle macchine virtuali e delle applicazioni. A tale scopo, imposta i seguenti valori per ciascuna opzione:

   - Risposta all'errore dell'host: riavvio VMs
   - Risposta per l'isolamento dell'host: spegnimento e riavvio VMs
   - Datastore with PDL (Datastore con PDL): Disabled (Disabilitato)
   - Datastore with APD (Datastore con APD): Disabled (Disabilitato)
   - VM Monitoring (Monitoraggio VM) : VM and Application Monitoring (Monitoraggio VM e applicazioni)
2. Ottimizzare la sensibilità del cluster regolando i seguenti valori:

   - Intervallo di errore: dopo questo intervallo, la macchina virtuale viene riavviata se non viene ricevuto un heartbeat VM.
   - Tempo di attività minimo: tempo di attesa del cluster dopo che una macchina virtuale inizia a monitorare gli heartbeat degli strumenti VM.
   - Numero massimo di reimpostazioni per VM: il cluster riavvia la macchina virtuale per un numero massimo di volte all'interno della finestra temporale massima di ripristino.
   - Finestra temporale massima reimpostazioni: la finestra temporale entro cui contare il numero massimo di reimpostazioni per VM.

   Se non si è sicuri di quali valori impostare, utilizzare queste impostazioni di esempio:

   - Failure interval (Intervallo di errore): **30** secondi
   - Minimum uptime (Tempo di attività minimo): **120** secondi
   - Maximum per-VM resets (Numero massimo reimpostazioni VM): **3**
   - Maximum resets time window (Finestra temporale massima reimpostazioni): **1** ora

Se ne hai altri VMs in esecuzione sul cluster, potresti voler impostare questi valori in modo specifico per la tua macchina virtuale. Non è possibile eseguire questa operazione fino a quando non distribuisci la VM dal file .ova. Per ulteriori informazioni sull'impostazione di questi valori, consulta (Facoltativo) Aggiungi opzioni Override for Other VMs sul tuo cluster.

Configura il tipo di gateway

Utilizzare la seguente procedura per configurare il gateway

Per scaricare l'immagine .ova per il tipo di gateway

- Scarica l'immagine .ova per il tipo di gateway di una delle seguenti opzioni:
  - File Gateway — Crea e attiva un Amazon FSx File Gateway

Distribuzione del gateway

Nel cluster configurato distribuisci l'immagine .ova in uno degli host del cluster. Per istruzioni, vedere Distribuire un modello OVF o OVA nella documentazione online di VMware vSphere.

Per distribuire l'immagine .ova del gateway

1. Distribuire l'immagine .ova in uno degli host del cluster.
2. Assicurarsi che i datastore scelti per il disco root e la cache siano disponibili per tutti gli host del cluster.

(Facoltativo) Aggiungi opzioni Override for Other VMs sul tuo cluster

Se ne hai altri VMs in esecuzione sul tuo cluster, potresti voler impostare i valori del cluster in modo specifico per ogni macchina virtuale. Per istruzioni, vedere Personalizzazione di una singola macchina virtuale nella documentazione online di VMware vSphere.

Per aggiungere opzioni di override per altre VMs nel tuo cluster

1. Nella pagina Riepilogo di VMware vSphere, scegliere il cluster per aprire la pagina del cluster, quindi scegliere Configura.
2. Scegliere la scheda Configuration (Configurazione) e quindi scegliere VM Overrides (Sostituzioni VM).
3. Aggiungere una nuova opzione di sostituzione VM per modificare ogni valore.

   Impostare i seguenti valori per ciascuna opzione in vSphere HA - VM Monitoring:

   - Monitoraggio VM: Override Enabled - Monitoraggio di macchine virtuali e applicazioni

- Sensibilità di monitoraggio delle macchine virtuali: Override Enabled - Monitoraggio di macchine virtuali e applicazioni
- Monitoraggio delle VM: personalizzato
- Intervallo di errore: secondi **30**
- Tempo di attività minimo: secondi **120**
- Maximum per-VM resets (Numero massimo reimpostazioni VM): **5**
- Intervallo di tempo massimo di ripristino: entro ore **1**

Attivazione del gateway

Dopo aver implementato il file.ova nell' VMware ambiente, attiva il gateway utilizzando la console Storage Gateway. Per istruzioni, consulta Rivedi le impostazioni e attiva Amazon FSx File Gateway.

Testa la tua configurazione VMware ad alta disponibilità

Dopo aver attivato il gateway, esegui il test della configurazione.

Per testare la tua configurazione VMware HA

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel riquadro di navigazione, scegli Gateway, quindi scegli il gateway che desideri testare per VMware HA.
3. Per Azioni, scegli Verifica VMware HA.
4. Nella casella Verify VMware High Availability Configuration che appare, scegli OK.

   > **Note**
   >
   > Il test della configurazione VMware HA riavvia la macchina virtuale del gateway e interrompe la connettività al gateway. L'esecuzione del test potrebbe richiedere alcuni minuti.

   Se il test ha esito positivo, lo stato Verified (Verificato) viene visualizzato nella scheda dettagli del gateway nella console.
5. Scegliere Exit (Esci).

Puoi trovare informazioni sugli eventi VMware HA nei gruppi di CloudWatch log di Amazon. Per ulteriori informazioni, consulta Ottenere i registri di integrità di File Gateway con CloudWatch gruppi di log.

Ottenimento di una chiave di attivazione per il gateway

Per ricevere una chiave di attivazione per il gateway, effettua una richiesta Web alla macchina virtuale (VM) del gateway. La macchina virtuale restituisce un reindirizzamento che contiene la chiave di attivazione, che viene passata come uno dei parametri dell'opzione `ActivateGateway` API per specificare la configurazione del gateway. Per ulteriori informazioni, vedere ActivateGatewaylo Storage Gateway API Reference.

> **Note**
>
> Le chiavi di attivazione del gateway scadono dopo 30 minuti se non vengono utilizzate.

La richiesta effettuata alla macchina virtuale gateway include la AWS regione in cui avviene l'attivazione. L'URL restituito dal reindirizzamento nella risposta contiene un parametro della stringa di query denominato `activationkey`. Questo parametro della stringa di query è la chiave di attivazione. Il formato della stringa di query ha un aspetto simile a questo: `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*. L'output di questa query restituisce sia la regione che la chiave di attivazione.

L'URL include anche `vpcEndpoint`, l'ID dell'endpoint VPC per i gateway che si connettono utilizzando il tipo di endpoint VPC.

> **Note**
>
> L'appliance hardware AWS Storage Gateway, i modelli di immagini VM e le Amazon Machine Images (AMI) di Amazon EC2 sono preconfigurati con i servizi HTTP necessari per ricevere e rispondere alle richieste Web descritte in questa pagina. Non è richiesta né consigliata l'installazione di servizi aggiuntivi sul gateway.

Argomenti

- Linux (curl)
- Linux (bash/zsh)

- Microsoft Windows PowerShell
- Utilizzo della console locale

Linux (curl)

Gli esempi seguenti mostrano come recuperare una chiave di attivazione utilizzando Linux (curl).

> **Note**
>
> Sostituisci le variabili evidenziate con i valori effettivi per il gateway. I valori accettabili sono i seguenti:
>
> - *`gateway_ip_address`*- L' IPv4 indirizzo del gateway, ad esempio `172.31.29.201`
> - *`gateway_type`*- Il tipo di gateway che desideri attivare, ad esempio `STOREDCACHED`,`VTL`,`FILE_S3`, o`FILE_FSX_SMB`.
> - *`region_code`*- La regione in cui desideri attivare il gateway. Consulta Endpoint regionali nella Guida di riferimento generale.AWS Se questo parametro non è specificato o se il valore fornito è digitato in modo errato o non corrisponde a una regione valida, il comando utilizzerà per impostazione predefinita la `us-east-1` regione.
> - *`vpc_endpoint`*- Il nome dell'endpoint VPC per il gateway, ad esempio. `vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com`

Per ottenere la chiave di attivazione per un endpoint pubblico:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

Per ottenere la chiave di attivazione per un endpoint VPC:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux (bash/zsh)

L'esempio seguente mostra come usare Linux (bash/zsh) per recuperare la risposta HTTP, analizzare le intestazioni HTTP e ottenere la chiave di attivazione.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

L'esempio seguente mostra come utilizzare Microsoft Windows PowerShell per recuperare la risposta HTTP, analizzare le intestazioni HTTP e ottenere la chiave di attivazione.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

Utilizzo della console locale

come utilizzare la console locale per generare e visualizzare una chiave di attivazione.

Come ottenere una chiave di attivazione per il gateway dalla console locale

1. Accedi alla tua console locale come amministratore.
2. Dopo aver effettuato l'accesso e aver visualizzato il menu principale Attivazione dell'AWS appliance: configurazione, seleziona `0` per scegliere Ottieni chiave di attivazione.
3. Seleziona Storage Gateway come opzione di famiglia di gateway.
4. Quando richiesto, inserisci Regione AWS dove desideri attivare il gateway.
5. Immettere 1 per pubblico oppure 2 per endpoint VPC come tipo di rete.
6. Inserire 1 per Standard o 2 per Federal Information Processing Standard (FIPS) come tipo di endpoint.

Utilizzo Direct Connect con Storage Gateway

Direct Connect collega la tua rete interna ad Amazon Web Services Cloud. Utilizzando Direct Connect Storage Gateway, è possibile creare una connessione per esigenze di carichi di lavoro ad alta velocità, fornendo una connessione di rete dedicata tra il gateway locale e. AWS

Storage Gateway utilizza endpoint pubblici. Una volta Direct Connect stabilita una connessione, è possibile creare un'interfaccia virtuale pubblica per consentire il routing del traffico verso gli endpoint Storage Gateway. L'interfaccia virtuale pubblica ignora i provider di servizi Internet nel percorso di rete. L'endpoint pubblico del servizio Storage Gateway può trovarsi nella stessa AWS regione della Direct Connect posizione o in una AWS regione diversa.

La figura seguente mostra un esempio di come Direct Connect funziona con Storage Gateway. architettura di rete che mostra Storage Gateway connesso al cloud tramite connessione AWS diretta.

La procedura seguente presuppone che è stato creato un funzionamento gateway.

Da utilizzare Direct Connect con Storage Gateway

1. Crea e stabilisci una AWS Direct Connect connessione tra il data center locale e l'endpoint Storage Gateway. Per ulteriori informazioni su come creare una connessione, consulta Nozioni di base su Direct Connect nella Guida per l'utente di Direct Connect .

2. Connect l'appliance Storage Gateway locale al Direct Connect router.
3. Creare un'interfaccia virtuale pubblica e configurare il router locale di conseguenza. Per ulteriori informazioni, consulta Creazione di un'interfaccia virtuale nella Guida per l'utente di Direct Connect .

Per ulteriori informazioni Direct Connect, consulta What is? Direct Connect nella Guida Direct Connect per l'utente.

Requisiti di autorizzazione degli account del servizio Active Directory

Se prevedi di utilizzare Microsoft Active Directory per fornire l'accesso autenticato all'utente ai di file sul tuo Gateway di archiviazione AWS, devi assicurarti di disporre di un account del servizio Active Directory e che l'account del servizio disponga delle autorizzazioni delegate per aggiungere computer al tuo dominio. Un account di servizio è un account utente di Active Directory a cui è stata delegata l'autorizzazione per eseguire determinate attività. Fornisci le credenziali di nome utente e password per questo account quando ti colleghi a uno Storage Gateway al tuo dominio Active Directory.

All'account del servizio Active Directory devono essere delegate le seguenti autorizzazioni nell'unità organizzativa a cui si accede al gateway:

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

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

Ottenere l'indirizzo IP per il dispositivo gateway

Dopo aver scelto un host e distribuito la macchina virtuale gateway, è possibile connettere e attivare il gateway. Per eseguire questa operazione, è necessario l'indirizzo IP della macchina virtuale gateway. L'indirizzo IP si ottiene dalla console locale del gateway. È possibile effettuare l'accesso alla console locale e ottenere l'indirizzo IP nella parte superiore della pagina della console.

Per i gateway distribuiti in locale, è anche possibile ottenere l'indirizzo IP dall'hypervisor. Per i gateway Amazon EC2, è anche possibile ottenere l'indirizzo IP dell'istanza Amazon EC2 dalla console di gestione Amazon EC2. Per informazioni su come ottenere l'indirizzo IP del gateway, consulta:

- VMware ospitare: Accesso alla console locale del gateway con VMware ESXi
- Host HyperV: Accesso alla console locale del gateway con Microsoft Hyper-V
- Host di macchina virtuale basata su kernel (KVM) Linux: Accesso alla console locale del gateway con Linux KVM
- Host EC2: Ottenere un indirizzo IP da un host Amazon EC2

Quando individui l'indirizzo IP, annotalo. Quindi torna alla console Storage Gateway e digita l'indirizzo IP nella console.

Ottenere un indirizzo IP da un host Amazon EC2

Per ottenere l'indirizzo IP dell'istanza Amazon EC2 su cui il gateway viene distribuito, collegarsi alla console locale dell'istanza EC2. Quindi ottenere l'indirizzo IP nella parte superiore della pagina della console. Per istruzioni, consulta .

È possibile anche recuperare l'indirizzo IP dalla console di gestione Amazon EC2. Consigliamo di usare l'indirizzo IP pubblico per l'attivazione. Per ottenere l'indirizzo IP pubblico, utilizzare la procedura 1. Se si sceglie invece di utilizzare l'indirizzo IP elastico, consulta la procedura 2.

Procedura 1: per connettersi al gateway utilizzando l'indirizzo IP pubblico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze) e selezionare l'istanza EC2 sulla quale è distribuito il gateway.

3. Scegliere la scheda Description (Descrizione) in basso, quindi annotare l'indirizzo IP pubblico. Utilizzarlo per collegarsi al gateway. Tornare alla console Storage Gateway e digitare l'indirizzo IP.

Per utilizzare l'indirizzo IP elastico per l'attivazione, procedere nel modo seguente.

Procedura 2: per connettersi al gateway utilizzando l'indirizzo IP elastico

1. Apri la console Amazon EC2 all'indirizzo https://console.aws.amazon.com/ec2/.
2. Nel riquadro di navigazione, scegliere Instances (Istanze) e selezionare l'istanza EC2 sulla quale è distribuito il gateway.
3. Scegliere la scheda Description (Descrizione) in basso, quindi annotare il valore Elastic IP (IP elastico). Utilizzarlo per collegarsi al gateway. Tornare alla console Storage Gateway e digitare l'indirizzo IP elastico.

Informazioni sulle risorse e sulle risorse di Storage Gateway IDs

In Storage Gateway, la risorsa principale è un gateway, ma altri tipi di risorse è la condivisione di file. Le condivisioni di file vengono chiamate sottorisorse e non esistono a meno che non siano associate a un gateway.

A queste risorse e sottorisorse sono associati Amazon Resource Names (ARNs) univoci, come mostrato in questa tabella.

Tipo di risorsa	Formato ARN
ARN gateway	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
ARN condivisione file	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

Lavorare con Resource IDs

Quando crei una risorsa, Storage Gateway assegna a tale risorsa un ID risorsa univoco. Questo ID risorsa è parte dell'ARN della risorsa. Un ID risorsa ha il formato di un identificatore di risorsa seguito da un trattino e da una combinazione univoca di otto lettere e numeri. Ad esempio, un ID gateway ID ha il formato `sgw-12A3456B` dove `sgw` è l'identificativo della risorsa per i gateway.

Gli ID delle risorse di Storage Gateway sono in lettere maiuscole. Tuttavia, quando si utilizzano questi ID risorsa con l'API Amazon EC2, Amazon EC2 si aspetta che gli ID risorsa siano costituiti da lettere minuscole. Per utilizzare questo ID risorsa con l'API di EC2, è necessario modificarlo in modo che sia composto solo da lettere minuscole. Ad esempio, in Storage Gateway l'ID per un volume può essere `vol-1122AABB`. Quando usi questo ID con l'API di EC2, devi modificarlo in `vol-1122aabb`. In caso contrario, l'API di EC2 potrebbe non comportarsi come previsto.

> **Important**
>
> IDs per i volumi Storage Gateway e gli snapshot di Amazon EBS creati dai volumi gateway stanno passando a un formato più lungo. A partire da dicembre, tutti i nuovi volumi e istanze verranno creati con una stringa di 17 caratteri. A partire da aprile 2016, potrai utilizzarli più a lungo in IDs modo da poter testare i tuoi sistemi con il nuovo formato. Per ulteriori informazioni, consulta Longer EC2 e EBS Resource. IDs
> Ad esempio, un ARN volume con gli ID volume in formato più lungo sarà come la seguente: `arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG`.
> Un ID snapshot con formato ID più lungo sarà come il seguente: `snap-78e226633445566ee`.
> Per ulteriori informazioni, vedere Annuncio: Heads-up — Longer Storage Gateway volume and snapshot IDs in arrivo nel 2016.

Etichettatura delle risorse di Storage Gateway

In Storage Gateway, puoi usare i tag per gestire le risorse. I tag consentono di aggiungere metadati alle risorse e categorizzarle per facilitarne la gestione. Ogni tag è composto da una coppia chiave-valore definita dall'utente. È possibile aggiungere i tag a gateway, volumi e nastri virtuali. Puoi cercare e filtrare queste risorse in base ai tag aggiunti.

Ad esempio, puoi usare i tag per identificare le risorse Storage Gateway utilizzate da ogni reparto dell'organizzazione. Puoi contrassegnare con i tag i gateway e i volumi utilizzati dal reparto contabile: (`key=department` e `value=accounting`). Puoi quindi filtrare con questo tag per identificare tutti i gateway e i volumi utilizzati dal reparto contabile e usare le informazioni per determinare i costi. Per ulteriori informazioni, consulta Utilizzo dei tag di allocazione dei costi e Utilizzo dell'editor di tag.

Se archivi un nastro virtuale contrassegnato da tag, il nastro mantiene i propri tag nell'archivio. Analogamente, se recuperi un nastro dall'archivio su un altro gateway, i tag sono gestiti nel nuovo gateway.

Per File Gateway, puoi utilizzare i tag per controllare l'accesso alle risorse. Per informazioni su come eseguire questa attività, consultare Utilizzo dei tag per controllare l'accesso al gateway e alle risorse.

I tag non hanno alcun significato semantico ma vengono interpretati rigorosamente come stringhe di caratteri.

Ai tag si applicano le limitazioni seguenti:

- Per le chiavi e i valori dei tag viene fatta la distinzione tra maiuscole e minuscole.
- Il numero massimo di tag per ogni risorsa è 50.
- Le chiavi dei tag non possono iniziare con `aws:`. Questo prefisso è riservato per l'uso di AWS .
- I caratteri validi per la proprietà di chiave sono lettere e numeri UTF-8, spazi e i caratteri speciali + - = . _ : / e @.

Lavorare con i tag

È possibile lavorare con i tag utilizzando la console Storage Gateway, l'API di Storage Gateway o l'interfaccia a riga di comando (CLI) Storage Gateway. Le procedure seguenti illustrano come aggiungere, modificare ed eliminare un tag dalla console.

Per aggiungere un tag

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Nel riquadro di navigazione, scegliere la risorsa a cui vuoi applicare un tag.

   Ad esempio, per applicare tag a un gateway, scegliere Gateways (Gateway), quindi scegliere il gateway che si desidera contrassegnare con dei tag dall'elenco di gateway.
3. Scegliere Tags (Tag), quindi Add tag (Aggiungi tag).

4. Nella finestra di dialogo Add/edit tags (Aggiungi/Modifica tag), selezionare Add New Volume (Aggiungi nuovo volume).
5. Digita una chiave per Key (Chiave) e un valore per Value (Valore). Ad esempio, è possibile digitare **`Department`** per la chiave e **`Accounting`** per il valore.

   > **Note**
   >
   > È possibile lasciare la casella Value (Valore) vuota.

6. Per aggiungere altri tag, scegliere Create Tag (Crea tag). È possibile aggiungere più tag a una risorsa.
7. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

Per modificare un tag

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegliere la risorsa con il tag da modificare.
3. Scegliere Tags (Tag) per aprire la finestra di dialogo Add/edit tags (Aggiungi/modifica tag).
4. Scegli l'icona a forma di matita accanto al tag che desideri modificare, quindi modifica il tag.
5. Al termine della modifica dei tag, scegliere Save (Salva).

Come Per eliminare un tag

1. Apri la console Storage Gateway a https://console.aws.amazon.com/storagegateway/casa.
2. Scegliere la risorsa con il tag da eliminare.
3. Scegliere Tags (Tag), quindi scegliere Add/edit tags (Aggiungi/modifica tag) per aprire la finestra di dialogo Add/edit tags (Aggiungi/modifica tag).
4. Scegliere l'icona X accanto al tag che si desidera eliminare, poi scegliere Save (Salva).

Utilizzo di componenti open source per Gateway di archiviazione AWS

Questa sezione descrive gli strumenti e le licenze di terze parti da cui dipendiamo per fornire Gateway di archiviazione AWS funzionalità.

Argomenti

Componenti open source per Storage Gateway

Vengono utilizzati diversi strumenti e licenze di terze parti per fornire funzionalità per Volume Gateway, Tape Gateway e Amazon S3 File Gateway.

Utilizza i seguenti link per scaricare il codice sorgente di alcuni componenti software open source inclusi nel software: Gateway di archiviazione AWS

- Per i dispositivi Storage Gateway distribuiti su VMware ESXi: sources.tar
- Per i dispositivi Storage Gateway distribuiti su Microsoft Hyper-V: sources_hyperv.tar
- Per le appliance Storage Gateway distribuite su una macchina virtuale (KVM) basata su kernel Linux: sources_KVM.tar

Questo prodotto include software sviluppato dal progetto OpenSSL per l'utilizzo nel kit di strumenti OpenSSL (http://www.openssl.org/). Per le licenze pertinenti per tutti gli strumenti di terze parti dipendenti, consulta Licenze di terze parti.

Componenti open source per Amazon FSx File Gateway

Per fornire la funzionalità di Amazon FSx File Gateway (FSx File Gateway) vengono utilizzati diversi strumenti e licenze di terze parti.

Utilizza i seguenti link per scaricare il codice sorgente di alcuni componenti software open source inclusi nel software FSx File Gateway:

- Per Amazon FSx File Gateway 2021-07-07 versione: -open-source.tgz sgw-file-fsx-smb
- Per Amazon FSx File Gateway 2021-04-06 versione: -20210406-open-source.tgz sgw-file-fsx-smb

Questo prodotto include software sviluppato dal progetto OpenSSL per l'utilizzo nel kit di strumenti OpenSSL (http://www.openssl.org/). Per le licenze pertinenti per tutti gli strumenti di terze parti dipendenti, consulta i seguenti link:

- Per Amazon FSx File Gateway 2021-07-07 release: licenza di terze parti.

- Per Amazon FSx File Gateway 2021-04-06 Release: licenza di terze parti.

Limiti e quote per FSx

Quote per i FSx file system Amazon

La tabella seguente elenca i limiti e le quote minimi e massimi per i FSx file system Amazon.

Risorsa	Limite per FSx file system Amazon
Numero massimo di tag	50 tag
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 richieste
Capacità di archiviazione minima per i file system SSD	32 GiB
Capacità di archiviazione minima per i file system HDD	2.000 GiB
Capacità massima di archiviazione per file system SSD e HDD	64 TiB
Capacità di throughput minima	8 MBps
Capacità di throughput massima	2.048 MBps
Numero massimo di condivisioni di FSx file Amazon	100.000

Dimensioni disco locale consigliate per il gateway

La tabella seguente consiglia le dimensioni per lo storage su disco locale per ciascuna Gateway di archiviazione AWS unità della distribuzione.

Tipo di gateway	Cache (minimo)	Cache (massimo)	
FSx File Gateway	150 GiB	64 TiB	

> **Note**
>
> È possibile configurare una o più unità locali per la cache fino alla capacità massima. Quando si aggiunge la cache a un FSx File Gateway esistente, è importante creare nuovi dischi sull'host virtuale (hypervisor o istanza Amazon EC2). Non modificate le dimensioni dei dischi esistenti se i dischi sono stati precedentemente allocati come cache.

Riferimento API per Storage Gateway

Oltre a utilizzare la console, puoi utilizzare l' Gateway di archiviazione AWS API per configurare e gestire i gateway in modo programmatico. Questa sezione descrive Gateway di archiviazione AWS le operazioni, la richiesta di firma per l'autenticazione e la gestione degli errori. Per ulteriori informazioni sulle regioni e sugli endpoint disponibili per Storage Gateway, consulta Endpoint e quote Gateway di archiviazione AWS nella Riferimenti generali di AWS.

> **Note**
>
> È inoltre possibile utilizzare il AWS SDKs per sviluppare applicazioni con Storage Gateway. AWS SDKs Per Java, .NET e PHP racchiudono l'API Storage Gateway sottostante, semplificando le attività di programmazione. Per ulteriori informazioni sul download delle librerie SDK, consulta Librerie e codice di esempio.

Argomenti

Gateway di archiviazione AWS Intestazioni di richiesta obbligatorie

Questa sezione descrive le intestazioni richieste a cui è necessario inviare con ogni richiesta POST. Gateway di archiviazione AWS Devi includere intestazioni HTTP per identificare le informazioni principali sulla richiesta, tra cui l'operazione che vuoi richiamare, la data della richiesta e le informazioni che indicano la tua autorizzazione come mittente della richiesta. Le intestazioni fanno distinzione tra maiuscole e minuscole, ma l'ordine delle intestazioni non è importante.

L'esempio seguente mostra le intestazioni utilizzate nell'ActivateGatewayoperazione.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
```

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

Le seguenti sono le intestazioni che devono essere incluse nelle richieste POST a. Gateway di archiviazione AWS Le intestazioni mostrate di seguito che iniziano con «x-amz» sono intestazioni specifiche. AWS Tutte le altre intestazioni elencate sono intestazioni comuni usate in transazioni HTTP.

Header	Description

`Authorization`	L'intestazione di autorizzazione contiene diverse informazioni sulla richiesta che consentono di determinare se la richiesta è un'azione valida Gateway di archiviazione AWS per il richiedente. Il formato di questa intestazione è il seguente (con l'aggiunta di interruzioni di riga ai fini della leggibilità):
	
	`Authorization: AWS4-HMAC_SHA456`
	`Credentials= YourAccessKey /yyymmdd/region/storagegateway/aw`
	`s4_request,`
	`SignedHeaders=content-type;host;x-amz-date;x-amz-targ`
	`et,`
	`Signature= CalculatedSignature`
	
	Nella sintassi precedente, si specificano l'anno YourAccessKey, il mese e il giorno (aaaammgg), la regione e il. CalculatedSignature Il formato dell'intestazione di autorizzazione è dettato dai requisiti del processo di firma V4. AWS I dettagli sulla firma vengono approfonditi nell'argomento Firmare le richieste.

`Content-Type`	Utilizza `application/x-amz-json-1.1` come tipo di contenuto per tutte le richieste di. Gateway di archiviazione AWS `Content-Type: application/x-amz-json-1.1`

Header	Description
`Host`	Utilizza l'intestazione host per specificare l' Gateway di archiviazione AWS endpoint a cui inviare la richiesta. Ad esempio, `storagegateway.us-east-2.amazonaws.com` è l'endpoint per la regione Stati Uniti orientali (Ohio). Per ulteriori informazioni sugli endpoint disponibili per Gateway di archiviazione AWS, consulta Gateway di archiviazione AWS Endpoints and Quotas in. Riferimenti generali di AWS `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	È necessario fornire il timestamp nell'intestazione HTTP `Date` o nell'intestazione AWS `x-amz-date` . (Alcune librerie client HTTP non consentono di impostare l'intestazione `Date`) Quando è presente un'`x-amz-date` intestazione, Gateway di archiviazione AWS ignora qualsiasi `Date` intestazione durante l'autenticazione della richiesta. Il `x-amz-date` formato deve essere ISO8601 Basic nel formato YYYYMMDD' T'HHMMSS'Z'. Se vengono utilizzati sia l'intestazione che l'intestazione, non è `Date` necessario che il formato dell'`x-amz-date` intestazione Date sia. ISO8601 `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	Questa intestazione specifica la versione dell'API e l'operazione richiesta . I valori dell'intestazione target sono formati concatenando la versione API con il nome API e usano il formato seguente. `x-amz-target: StorageGateway_ APIversion .operationName` Il valore OperationName (ad esempio ActivateGateway "«) può essere trovato dall'elenco delle API,. Riferimento API per Storage Gateway

Firmare le richieste

Storage Gateway richiede l'autenticazione con firma di ogni richiesta inviata. Per firmare una richiesta, è necessario calcolare una firma digitale utilizzando una funzione hash crittografica. Una funzione hash crittografica è una funzione che restituisce un valore hash univoco basato sull'input. L'input alla funzione hash include il testo della richiesta e la tua chiave di accesso segreta. La funzione hash restituisce un valore hash che includi nella richiesta come firma. La firma è parte dell'intestazione `Authorization` della richiesta.

Dopo aver ricevuto la richiesta, Storage Gateway ricalcola la firma utilizzando la stessa funzione hash e lo stesso input utilizzati per firmare la richiesta. Se la firma risultante corrisponde alla firma nella richiesta, Storage Gateway elabora la richiesta. In caso contrario, la richiesta viene respinta.

Storage Gateway supporta l'autenticazione con AWS Signature Version 4. La procedura per il calcolo di una firma può essere suddivisa in tre fasi:

- Fase 1. Creazione di una richiesta canonica

  Riorganizza la richiesta HTTP in un formato canonico. L'utilizzo di un formato canonico è necessario in quanto Storage Gateway utilizza quel formato quando ricalcola una firma da confrontare con quella che hai inviato.

- Fase 2: creazione di una stringa di firma

  Crea una stringa che utilizzerai come uno dei valori di input per la funzione hash crittografica. La stringa, denominata stringa di firma, è una concatenazione del nome dell'algoritmo hash, della data della richiesta, di una stringa di ambito credenziali e della richiesta in formato canonico creata nella fase precedente. La stringa di ambito credenziali è anch'essa una concatenazione di data, regione e informazioni sul servizio.

- Fase 3. Creazione di una firma

  Crea una firma per la tua richiesta utilizzando una funzione hash crittografica che accetta due stringhe di input: la tua stringa di firma e una chiave derivata. La chiave derivata viene calcolata partendo dalla chiave di accesso segreta e utilizzando la stringa di ambito delle credenziali per creare una serie di codici di autenticazione dei messaggi basati su Hash ()HMACs.

Esempio di calcolo di firma

L'esempio in questa sezione mostra come creare una firma per ListGateways. L'esempio può essere utilizzato come riferimento per verificare il metodo di calcolo della firma.

L'esempio presuppone quanto segue:

- Il timestamp della richiesta è "Mon, 10 Sep 2012 00:00:00" GMT.
- L'endpoint è la regione Stati Uniti orientali (Ohio).

La sintassi generale della richiesta (incluso il corpo JSON) è:

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

Il formato canonico della richiesta calcolata per Fase 1. Creazione di una richiesta canonica è:

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

L'ultima riga della richiesta canonica è l'hash del corpo della richiesta. Nota inoltre la terza riga vuota nella richiesta canonica. Questo perché non esistono parametri di query per questa API (o per alcun Storage Gateway APIs).

La stringa di firma per Fase 2: creazione di una stringa di firma è:

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

La prima riga della stringa di firma è l'algoritmo, la seconda è il timestamp, la terza è l'ambito credenziali e l'ultima è un hash del formato della richiesta canonica in Fase 1.

Per Fase 3. Creazione di una firma, la chiave derivata può essere rappresentata come segue:

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

Se viene utilizzata la chiave di accesso segreta wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY, la firma calcolata è:

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

La fase finale consiste nel creare l'intestazione `Authorization`. Per la chiave di accesso AKIAIOSFODNN7EXAMPLE, l'intestazione (con interruzioni di riga aggiunte per facilitare la lettura) è:

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

Risposte agli errori

Argomenti

- Eccezioni
- Codici di errore delle operazioni
- Risposte agli errori

Questa sezione fornisce informazioni di riferimento sugli Gateway di archiviazione AWS errori. Questi errori sono rappresentati da un'eccezione di errore e da un codice di errore dell'operazione.

L'eccezione di errore `InvalidSignatureException`, ad esempio, viene restituita da qualsiasi risposta API in caso di problema con la firma della richiesta. Tuttavia, il codice di errore dell'operazione `ActivationKeyInvalid` viene restituito solo per l'ActivateGatewayAPI.

A seconda del tipo di errore, Storage Gateway può restituire solo un'eccezione oppure sia un'eccezione che un codice di errore dell'operazione. In Risposte agli errori vengono forniti esempi di risposte di errore.

Eccezioni

La tabella seguente elenca le eccezioni delle Gateway di archiviazione AWS API. Quando un' Gateway di archiviazione AWS operazione restituisce una risposta di errore, il corpo della risposta contiene una di queste eccezioni. `InternalServerError` e `InvalidGatewayRequestException` restituiscono uno dei messaggi Codici di errore delle operazioni dei codici di errore delle operazioni che forniscono il codice di errore dell'operazione specifico.

Eccezione	Messaggio	Codice di stato HTTP
`IncompleteSignatureException`	La firma specificata non è completa.	400 Richiesta non valida
`InternalFailure`	L'elaborazione della richiesta non è riuscita a causa di un errore, un'eccezione o un guasto sconosciuto.	500 - Errore interno del server
`InternalServerError`	Uno dei messaggi dei codici di errore delle operazioni in Codici di errore delle operazioni.	500 - Errore interno del server
`InvalidAction`	L'azione o operazione richiesta non è valida.	400 Richiesta non valida
`InvalidClientTokenId`	Il certificato X.509 o AWS l'ID della chiave di accesso fornito non esiste nei nostri archivi.	403 Non consentito

Eccezione	Messaggio	Codice di stato HTTP
`InvalidGatewayRequestException`	Uno dei messaggi dei codici di errore delle operazioni in Codici di errore delle operazioni.	400 Richiesta non valida
`InvalidSignatureException`	La firma di richiesta che abbiamo calcolato non corrisponde alla firma che hai fornito. Controlla la tua chiave di AWS accesso e il metodo di firma.	400 Richiesta non valida
`MissingAction`	Nella richiesta manca un parametro di un'azione o un'operazione.	400 Richiesta non valida
`MissingAuthenticationToken`	La richiesta deve contenere un ID chiave di AWS accesso valido (registrato) o un certificato X.509.	403 Non consentito
`RequestExpired`	La richiesta ha superato la data di scadenza o la data della richiesta (con margine di 15 minuti) oppure la data della richiesta è oltre 15 minuti nel futuro.	400 Richiesta non valida
`SerializationException`	Si è verificato un errore durante la serializzazione. Controllare che il formato del payload JSON sia corretto.	400 Richiesta non valida
`ServiceUnavailable`	La richiesta non è riuscita a causa di un errore temporaneo del server.	503 Service Unavailable (503 Servizio non disponibile)
`SubscriptionRequiredException`	L' AWS Access Key Id richiede un abbonamento per il servizio.	400 Richiesta non valida

Eccezione	Messaggio	Codice di stato HTTP
`ThrottlingException`	Velocità superata.	400 Richiesta non valida
`TooManyRequests`	Troppe richieste.	429 Troppe richieste
`UnknownOperationException`	È stata specificata un'operazione sconosciuta. Le operazioni valide sono elencate in Azioni dell'API Storage Gateway.	400 Richiesta non valida
`UnrecognizedClientException`	Il token di sicurezza incluso nella richiesta non è valido.	400 Richiesta non valida
`ValidationException`	Il valore di un parametro di input è errato o non compreso nell'intervallo.	400 Richiesta non valida

Codici di errore delle operazioni

La tabella seguente mostra la mappatura tra i codici di errore Gateway di archiviazione AWS operativi e APIs che può restituire i codici. Tutti i codici di errore delle operazioni vengono restituiti con una delle due eccezioni generali `InternalServerError` e `InvalidGatewayRequestException` descritte in Eccezioni.

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`ActivationKeyExpired`	La chiave di attivazione specificata è scaduta.	ActivateGateway
`ActivationKeyInvalid`	La chiave di attivazione specificata non è valida.	ActivateGateway

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`ActivationKeyNotFound`	La chiave di attivazione specificata non è stata trovata.	ActivateGateway
`BandwidthThrottleScheduleNotFound`	La limitazione di larghezza di banda specificata non è stata trovata.	DeleteBandwidthRateLimit
`CannotExportSnapshot`	Lo snapshot specificato non può essere esportato.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`InitiatorNotFound`	L'iniziatore specificato non è stato trovato.	DeleteChapCredentials
`DiskAlreadyAllocated`	Il disco specificato è già allocato.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskDoesNotExist`	Il disco specificato non esiste.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
`DiskSizeNotGigAligned`	Il disco specificato non è allineato ai gigabyte.	CreateStorediSCSIVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`DiskSizeGreaterThanVolumeMaxSize`	La dimensione del disco specificata è superiore alla dimensione massima del volume.	CreateStorediSCSIVolume
`DiskSizeLessThanVolumeSize`	La dimensione del disco specificata è inferiore alla dimensione del volume.	CreateStorediSCSIVolume
`DuplicateCertificateInfo`	Le informazioni sul certificato specificate sono duplicate.	ActivateGateway
FileSystemAssociationEndpointConfigurationConflict	La configurazione dell'endpoint dell'associazione di file system esistente è in conflitto con la configurazione specificata.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	L'indirizzo IP dell'endpoint specificato è già in uso.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	Manca l'indirizzo IP dell'endpoint di File System Association.	AssociateFileSystem
FileSystemAssociationNotFound	L'associazione di file system specificata non è stata trovata.	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
FileSystemNotFound	Il file system specificato non è stato trovato.	AssociateFileSystem

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`GatewayInternalError`	Si è verificato un errore interno del gateway.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`GatewayNotConnected`	Il gateway specificato non è connesso.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`GatewayNotFound`	Il gateway specificato non è stato trovato.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`GatewayProxyNetworkConnectionBusy`	La connessione di rete proxy gateway specificata è occupata.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`InternalError`	Si è verificato un errore interno.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`InvalidParameters`	La richiesta specificata contiene parametri non validi.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`LocalStorageLimitExceeded`	Il limite di storage locale è stato superato.	AddCache AddUploadBuffer AddWorkingStorage
`LunInvalid`	Il LUN specificato non è valido.	CreateStorediSCSIVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`MaximumVolumeCountExceeded`	Il numero massimo di volumi è stato superato.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
`NetworkConfigurationChanged`	La configurazione di rete del gateway è stata modificata.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`NotSupported`	L'operazione specifica ta non è supportata.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`OutdatedGateway`	Il gateway specificato non è aggiornato.	ActivateGateway
`SnapshotInProgressException`	Lo snapshot specificato è in corso.	DeleteVolume
`SnapshotIdInvalid`	Lo snapshot specificato non è valido.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`StagingAreaFull`	L'area di gestione temporanea è piena.	CreateCachediSCSIVolume CreateStorediSCSIVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`TargetAlreadyExists`	La destinazione specificata esiste già.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`TargetInvalid`	La destinazione specificata non è valida.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
`TargetNotFound`	La destinazione specificata non è stata trovata.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`UnsupportedOperationForGatewayType`	L'operazione specificata non è valida per il tipo di gateway.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
`VolumeAlreadyExists`	Il volume specificato esiste già.	CreateCachediSCSIVolume CreateStorediSCSIVolume
`VolumeIdInvalid`	Il volume specificato non è valido.	DeleteVolume
`VolumeInUse`	Il volume specificato è già in uso.	DeleteVolume

Codice di errore dell'operazione	Messaggio	Operazioni che restituiscono questo codice di errore
`VolumeNotFound`	Il volume specificato non è stato trovato.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
`VolumeNotReady`	Il volume specificato non è pronto.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

Risposte agli errori

Quando si verifica un errore, le informazioni dell'intestazione della risposta contengono:

- Tipo di contenuto: application/ -1.1 x-amz-json
- Un codice di stato HTTP `4xx` o `5xx` appropriato

Il corpo di una risposta di errore contiene informazioni relative all'errore. La risposta di errore di esempio seguente mostra la sintassi di output degli elementi della risposta comuni a tutte le risposte di errore.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
```

```
          "errorDetails": "String"
        }
}
```

La tabella seguente illustra i campi della risposta di errore JSON mostrata nella sintassi precedente.

__type

Una delle eccezioni elencate in Eccezioni.

- Tipo: stringa

error

Contiene dettagli dell'errore specifici dell'API. Negli errori generali, ovvero non specifici di un'API, queste informazioni sull'errore non vengono visualizzate.

Tipo: raccolta

errorCode

Uno dei codici di errore delle operazioni .

- Tipo: stringa

errorDetails

Questo campo non viene usato nella versione corrente dell'API.

- Tipo: stringa

message

Uno dei messaggi dei codici di errore delle operazioni.

- Tipo: stringa

Esempi di risposta di errore

Il seguente corpo JSON viene restituito se si utilizza l' DescribeStorediSCSIVolumesAPI e si specifica un input di richiesta ARN del gateway che non esiste.

```
{
  "__type": "InvalidGatewayRequestException",
```

```
  "message": "The specified volume was not found.",
  "error": {
    "errorCode": "VolumeNotFound"
  }
}
```

Il corpo JSON seguente viene restituito se Storage Gateway calcola una firma che non corrisponde alla firma inviata con una richiesta.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Azioni dell'API Storage Gateway

Per un elenco delle operazioni di Storage Gateway , consulta Operazioni nel Riferimento API Gateway di archiviazione AWS .

Cronologia dei documenti per la Amazon FSx File Gateway User Guide

La tabella seguente descrive le modifiche importanti apportate in ogni versione di questa guida per l'utente dopo aprile 2018. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile iscriversi a un feed RSS.

Modifica	Descrizione	Data
Avviso di modifica della disponibilità per File Gateway FSx	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.	28 ottobre 2024
Avviso di modifica della disponibilità per FSx File Gateway	Gateway di archiviazione AWS's FSx File Gateway non sarà più disponibile per i nuovi clienti a partire dal 28/10/24. Per utilizzare il servizio, è necessario registrar si prima di tale data. I clienti esistenti di FSx File Gateway possono continuare a utilizzar e il servizio normalmente. Per funzionalità simili a FSx File Gateway, consulta questo post del blog.	26 settembre 2024
È stata aggiunta l'opzione per attivare o disattivare gli	Storage Gateway riceve aggiornamenti di manutenzi one regolari che possono	6 giugno 2024

aggiornamenti di manutenzione	includere aggiornamenti del sistema operativo e del software, correzioni per la stabilità, le prestazioni e la sicurezza e l'accesso a nuove funzionalità. È ora possibile configurare un'impostazione per attivare o disattivare questi aggiornamenti per ogni singolo gateway della distribuzione. Per ulteriori informazioni, vedere Gestione degli aggiornamenti del gateway tramite la Gateway di archiviazione AWS console.	
Allarmi consigliati CloudWatch aggiornati	L' CloudWatch `HealthNotifications` allarme ora si applica ed è consigliato per tutti i tipi di gateway e piattaforme host. Le impostazioni di configurazione consigliate sono state aggiornate anche per `HealthNotifications` e `AvailabilityNotifications` . Per ulteriori informazioni, vedere gli CloudWatch allarmi.	2 ottobre 2023

Suggerimenti per la GatewayClockOutOfSync risoluzione dei problemi aggiunti	La sezione Risoluzione dei problemi relativi al File Gateway include ora linee guida per la risoluzione dei problemi che possono verificar si se l'orologio del sistema gateway non è sincronizzato con l'ora del server AWS Storage Gateway. Per ulteriori informazioni, vedere Errore:. GatewayClockOutOfSync	19 ottobre 2022
Aggiunti suggerimenti per la risoluzione dei problemi relativi all'accesso al dominio Active	La sezione Risoluzione dei problemi relativi al File Gateway include ora linee guida per la risoluzione dei problemi che possono verificar si quando si tenta di aggiunger e il gateway a un dominio Active Directory. Per ulteriori informazioni, vedere Risoluzio ne dei problemi relativi al dominio Active Directory.	19 ottobre 2022
Procedure di creazione del gateway aggiornate	La procedura per la creazione di un nuovo gateway è stata aggiornata per riflettere le modifiche nella console Storage Gateway. Per ulteriori informazioni, consulta Creare e attivare un Amazon S3 File Gateway.	12 ottobre 2021

Supporto per più file system	Amazon FSx File Gateway ora supporta fino a cinque FSx file system Amazon collegati. Per ulteriori informazioni, consulta Collegare un file system Amazon FSx for Windows File Server.	7 luglio 2021
Supporto per le quote di FSx soft storage di Amazon	Amazon FSx File Gateway ora supporta le quote di soft storage (che avvisano quando gli utenti superano i limiti di dati) quando scrivono su FSx file system Amazon collegati in cui sono configurate le quote di storage. Le quote fisse (che impongono limiti di dati negando l'accesso in scrittura) non sono supportate. Le quote flessibili funzionano per tutti gli utenti tranne l'utente FSx amministratore di Amazon. Per ulteriori informazioni sull'impostazione delle quote di storage, consulta la sezione Quote di storage nella Amazon FSx for Windows File Server User Guide.	7 luglio 2021

Nuova guida	Oltre al File Gateway originale (ora noto come Amazon S3 File Gateway), Storage Gateway fornisce Amazon FSx File Gateway (FSx File Gateway). FSx File Gateway offre una bassa latenza e un accesso efficiente alle condivisioni di file in-cloud FSx per Windows File Server dalla tua struttura locale. Per ulteriori informazioni, consulta Cos'è Amazon FSx File Gateway?	27 aprile 2021
Conformità agli standard FedRAMP	Storage Gateway è ora conforme a FedRAMP. Per ulteriori informazioni, vedere Convalida della conformità per Storage Gateway.	24 novembre 2020
Migrazione File Gateway	File Gateway ora fornisce un processo documenta to per la sostituzione di un File Gateway esistente con un nuovo File Gateway. Per ulteriori informazioni, vedere Sostituzione di un File Gateway con un nuovo File Gateway.	30 ottobre 2020

Le prestazioni di lettura della cache a freddo di File Gateway sono aumentate di 4 volte	Storage Gateway ha aumentato di 4 volte le prestazioni di lettura della cache fredda. Per ulteriori informazioni, vedere Guida alle prestazioni per File Gateways.	31 agosto 2020
Ordinare l'appliance hardware tramite la console	È ora possibile ordinare l'appliance hardware tramite la Gateway di archiviazione AWS console. Per ulteriori informazioni, vedere Utilizzo dell'appliance hardware AWS Storage Gateway.	12 agosto 2020
Support per gli endpoint FIPS (Federal Information Processing Standard) in nuove regioni AWS	È ora possibile attivare un gateway con endpoint FIPS nelle regioni Stati Uniti orientali (Ohio), Stati Uniti orientali (Virginia settentrionale), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon) e Canada (Centrale). Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS nella Riferimenti generali di AWS.	31 luglio 2020

Aumento del quadruplo dello storage nella cache locale di File Gateway	Storage Gateway ora supporta una cache locale fino a 64 TB per File Gateway, migliorando le prestazioni per le applicazioni locali fornendo un accesso a bassa latenza a set di dati di lavoro più grandi. Per ulteriori informazioni, vedere Dimensioni dei dischi locali consigliate per il gateway nella Guida per l'utente di Storage Gateway.	7 luglio 2020
Visualizza gli CloudWatch allarmi Amazon nella console Storage Gateway	È ora possibile visualizzare gli CloudWatch allarmi nella console Storage Gateway. Per ulteriori informazioni, vedere Comprendere gli CloudWatch allarmi.	29 maggio 2020
Supporto per gli endpoint Federal Information Processing Standard (FIPS)	Puoi ora attivare un gateway con endpoint FIPS nelle regioni AWS GovCloud (US) . Per scegliere un endpoint FIPS per un File Gateway, vedi Scelta di un endpoint di servizio.	22 maggio 2020
Nuove regioni AWS	Storage Gateway è ora disponibile nelle regioni Africa (Città del Capo) ed Europa (Milano). Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS nella Riferimenti generali di AWS.	07 maggio 2020

Supporto per classe di storage S3 Intelligent-Tiering	Storage Gateway ora supporta la classe di archiviazione S3 Intelligent-Tiering. La classe di storage S3 Intelligent-Tiering è progettata per ottimizzare i costi dello storage spostando automaticamente i dati sul livello di accesso di storage più conveniente, senza impatto sulle prestazioni o sovraccarico operativo. Per ulteriori informazioni, consulta Classe di archiviazione per l'ottimizzazione automatica degli oggetti a cui si accede frequentemente e raramente nella Guida per l'utente di Amazon Simple Storage Service.	30 aprile 2020
Nuova AWS regione	Storage Gateway è ora disponibile nella regione AWS GovCloud (Stati Uniti orientali). Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS in Riferimenti generali di AWS.	12 marzo 2020

Supporto per hypervisor macchina virtuale basata su kernel (KVM) Linux	Storage Gateway offre ora la possibilità di distribuire un gateway on-premise nella piattaforma di virtualizzazione KVM. I gateway distribuiti in KVM hanno tutte le stesse funzionalità e caratteristiche dei gateway on-premise esistenti. Per ulteriori informazioni, consulta l'argomento relativo agli Hypervisor supportati e requisiti host nella Guida per l'utente di Storage Gateway.	4 febbraio 2020
Support per VMware vSphere High Availability	Storage Gateway ora fornisce supporto per l'alta disponibilità per aiutare VMware a proteggere i carichi di lavoro di storage da guasti hardware, hypervisor o di rete. Per ulteriori informazioni, vedere Using VMware vSphere High Availability with Storage Gateway nella Storage Gateway User Guide. Questa versione include inoltre i miglioramenti delle prestazioni. Per ulteriori informazioni, consulta Prestazioni nella Guida per l'utente di Storage Gateway.	20 novembre 2019

Support per Amazon CloudWatch Logs	Ora puoi configurare File Gateway con Amazon CloudWatch Log Groups per ricevere notifiche sugli errori e sullo stato del gateway e delle sue risorse. Per ulteriori informazioni, consulta Getting Notified About Gateway Health and Errors with Amazon CloudWatch Log Groups nella Storage Gateway User Guide.	4 settembre 2019
Novità Regione AWS	Storage Gateway è ora disponibile nella regione Asia Pacifico (Hong Kong). Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS in Riferimenti generali di AWS.	14 agosto 2019
Novità Regione AWS	Storage Gateway è ora disponibile nella regione Medio Oriente (Bahrein). Per ulteriori informazioni, consulta Endpoint e quote Gateway di archiviazione AWS in Riferimenti generali di AWS.	29 luglio 2019

Supporto per attivare un gateway in un cloud privato virtuale (VPC, Virtual Private Cloud)	È ora possibile attivare un gateway in un cloud privato virtuale. È possibile creare una connessione privata tra l'applicazione software locale e l'infrastruttura di storage basato sul cloud. Per ulteriori informazioni, vedere Activating a Gateway in a Virtual Private Cloud.	20 giugno 2019
Supporto File Gateway per l'autorizzazione basata su tag	File Gateway ora supporta l'autorizzazione basata su tag. È possibile controlla re l'accesso alle risorse File Gateway in base ai tag presenti su tali risorse. È inoltre possibile controllare l'accesso in base ai tag che possono essere trasmessi in una condizione di richiesta IAM. Per ulteriori informazioni, consulta Controllo dell'accesso alle risorse del gateway di file.	4 marzo 2019

Disponibilità dell'appliance hardware AWS Storage Gateway in Europa	L'appliance hardware AWS Storage Gateway è ora disponibile in Europa. Per ulteriori informazioni, consulta Regioni hardware appliance Gateway di archiviazione AWS in Riferimenti generali di AWS. Inoltre, ora è possibile aumentare lo spazio di archiviazione utilizzabile sullo Storage Gateway Hardware Appliance da 5 TB a 12 TB e sostituire la scheda di rete in rame installata con una scheda di rete in fibra ottica da 10 gigabit. AWS Per ulteriori informazioni, consulta Configurazione dell'appliance hardware.	25 febbraio 2019
Supporto per l'appliance hardware AWS Storage Gateway	L'appliance hardware AWS Storage Gateway include il software Storage Gateway preinstallato su un server di terze parti. È possibile gestire l'appliance dalla Console di gestione AWS. L'appliance può ospitare gateway di file, di nastri virtuali e di volumi. Per ulteriori informazioni, consulta Utilizzo dell'appliance hardware Storage Gateway.	18 settembre 2018

Aggiornamenti precedenti

La tabella che segue descrive le modifiche importanti apportate a ogni versione della Gateway di archiviazione AWS Guida per l'utente prima di maggio 2018.

Modifica	Descrizione	Data della modifica
Nuovo Regione AWS	Il gateway di nastri virtuali è ora disponibile nella regione Asia Pacifico (Singapore). Per informazioni dettagliate, consulta Regioni AWS che supportano Storage Gateway.	3 Aprile 2018
Nuovo Regione AWS	Storage Gateway è ora disponibile nella regione Europa (Parigi). Per informazioni dettagliate, consulta Regioni AWS che supportano Storage Gateway.	18 dicembre 2017
Support per la versione VMware ESXi 6.5 di Hypervisor	Gateway di archiviazione AWS ora supporta la versione 6.5 di VMware ESXi Hypervisor. Questa si aggiunge alle versioni 4.1, 5.0, 5.1, 5.5 e 6.0. Per ulteriori informazioni, consulta Hypervisor supportati e requisiti di hosting.	13 settembre 2017
Supporto del gateway di file per l'hypervisor Microsoft Hyper-V	Puoi ora distribuire un gateway di file in un hyperviso r Microsoft Hyper-V. Per informazioni, consulta Hypervisor supportati e requisiti di hosting.	22 giugno 2017
Nuovo Regione AWS	Storage Gateway è ora disponibile nella regione Asia Pacifico (Mumbai). Per informazioni dettaglia te, consulta Regioni AWS che supportano Storage Gateway.	02 maggio 2017
Supporto per i gateway di file in Amazon EC2	Gateway di archiviazione AWS ora offre la possibili tà di implementare un File Gateway in Amazon EC2. Puoi avviare un gateway di file in Amazon EC2 usando l'Amazon Machine Image (AMI) Storage Gateway ora disponibile come AMI della community. Per informazi	08 febbraio 2017

Modifica	Descrizione	Data della modifica
	oni su come creare un File Gateway e distribuirlo su un'istanza EC2, consulta. Crea e attiva un Amazon FSx File Gateway Per informazioni su come avviare un'AMI File Gateway, vedereImplementa un host FSx Amazon EC2 predefinito per File Gateway. Inoltre, File Gateway ora supporta la configurazione del proxy HTTP. Per ulteriori informazioni, consulta Routing del gateway distribuito su Amazon EC2 tramite un proxy HTTP.	
Nuovo Regione AWS	Storage Gateway è ora disponibile nella regione Europa (Londra). Per informazioni dettagliate, consulta Regioni AWS che supportano Storage Gateway.	13 dicembre 2016
Nuovo Regione AWS	Storage Gateway è ora disponibile nella regione Canada (Centrale). Per informazioni dettagliate, consulta Regioni AWS che supportano Storage Gateway.	08 dicembre 2016
Supporto per il gateway di file	Oltre ai gateway di volumi e ai gateway di nastri virtuali, Storage Gateway offre ora gateway di file. Un gateway di file combina un servizio e un'applia nce software virtuale, permettendoti di archiviare e recuperare oggetti in Amazon S3 tramite protocolli di file standard del settore, come NFS (Network File System). Il gateway permette l'accesso a oggetti in Amazon S3 come file in un punto di montaggio NFS.	29 Novembre 2016